OCCAMSEC E-BRIEF // AUGUST 27 2018

TABLE OF CONTENTS

Foreign Economic Espionage in Cyberspace

The Office of the National Counterintelligence Executive provided congress the 2011 report on Foreign Spies Stealing U.S. Economic Secrets in Cyberspace. In a new 2018 report, the counterintelligence agency describes ongoing efforts by China, Iran, and Russia to steal sensitive US information and trade secrets.

Key Takeaways

Foreign nation states and the actors working on their behalf represent the most persistent and pervasive cyber intelligence threat. The report states China, Iran, and Russia are "three of the most capable and active cyber actors tied to economic espionage," and will "remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace. All will almost certainly continue to deploy significant resources and a wide array of tactics to acquire intellectual and proprietary information".

Lack of standardization during the current first-generation development of cloud and IoT infrastructure will likely hinder comprehensive security solutions in the near term.

Emerging Threats

- Software Supply Chain Operations - "Software supply chain infiltration has already threatened the critical infrastructure sector and could threaten other sectors as well." The report cites seven significant events reported in the public domain in 2017 compared to only four between 2014 and 2016.

- Foreign Laws That Could Enable Intellectual Property Theft - In 2017 China put into effect a new cyber security law requiring foreign companies to submit information and communication technology (ICT) for government security reviews and companies operating in China store their data in China. "The U.S. Chamber of Commerce has gone on record to explain that if a foreign company is forced to localize a valuable set of data or information in China, whether for research and development purposes or simply to conduct its business, it will have to assume a significant amount of risk."

- Foreign Technology Companies With Links to Host Governments - The report specifically cites Kaspersky Lab however references to Chinese laws include providing Beijing basis to compel technology companies operating in China to cooperate with national security services.

Targeted Technologies

- Energy / Alternative Energy

- Biotechnology

- Defense Technology

- Environmental Protection

- High-End Manufacturing

The report includes the following actions to help mitigate the prevalence of economic espionage in cyberspace:

- Sharing informations about cyberthreats, vulnerabilities, and other risks.
- Promoting best practices, risk assessments, and capability development.
- Improving responses to cyber incidents.
- Building and driving the market towards a more secure cyber ecosystem.
- Partnering to address cyber issues.

::Download the full report here

Related Articles

Corporate spying costs billions, can it be stopped? CNBC

China Is Still Stealing America's Business Secrets, U.S. Officials Say Defense One

GE Engineer Linked to China Stole Power Plant Technology, FBI Says Wall Street Journal

Source: OccamSec

US Intel Chief Warns of Devastating Cyber Threat to US Infrastructure

The US intelligence chief warned that the threat was growing for a devastating cyber assault on critical US infrastructure, saying the "warning lights are blinking red again" nearly two decades after the 11 September 2001 attacks. Russia, China, Iran, and North Korea launch daily cyber strikes on the computer networks of federal, state, and local government agencies, US corporations, and academic institutions, said Director of National Intelligence Dan Coats. Of the four, "Russia has been the most aggressive foreign actor, no question," he said.

Coats spoke at the Hudson Institute think tank shortly after the Department of Justice announced the indictment of 12 Russian military intelligence officers on charges of hacking into the computers of the 2016 US presidential campaign of Hillary Clinton and Democratic Party organizations. The indictment and Coats' comments came three days before US President Donald Trump was to meet Russian President Vladimir Putin for talks in Helsinki, Trump's first formal summit with Putin. Coats warned that the possibility of a "crippling cyber attack on our critical infrastructure" by a foreign actor is growing. He likened daily cyber attacks to the "alarming activities" that US intelligence agencies detected before al Qaeda staged the most devastating extremist attack on the US homeland on 11 September 2001. "The system was blinking red. Here we are nearly two decades later and I'm here to say the warning lights are blinking red again," he said.

Coats said the US government has not yet detected the kinds of cyber attacks and intrusions that officials say Russia launched against state election boards and voter data bases before the 2016 election. “However, we fully realize that we are just one click away of the keyboard from a similar situation repeating itself,” Coats continued. At the same time, he said, some of the same Russian actors who meddled in the 2016 campaign again are using fake social media accounts and other means to spread false information and propaganda to fuel political divisions in the United States, he said. Coats cited unnamed “individuals” affiliated with the Internet Research Agency, the St. Petersburg-based “troll factory” indicted by a federal grand jury in February as part of Special Counsel Robert Mueller’s investigation into alleged Russian election meddling. These individuals have been “creating new social media accounts, masquerading as Americans, and then using these accounts to draw attention to divisive issues,” he said.

Source: Reuters

The Use of Social Media by United States Extremists

Emerging communication technologies, and social media platforms in particular, play an increasingly important role in the radicalization and mobilization processes of violent and non-violent extremists. However, the extent to which extremists utilize social media, and whether it influences terrorist outcomes, is still not well understood. This research brief expands the current knowledge base by leveraging newly collected data on the social media activities of 479 extremists in the PIRUS dataset who radicalized between 2005 and 2016. This includes descriptive analyses of the frequency of social media usage among US extremists, the types of social media platforms used, the differences in the rates of social media use by ideology and group membership, the purposes of social media use, and the impact of social media on foreign fighter travel and domestic terrorism plots. The PIRUS data reveal four key findings on the relationship between social media and the radicalization of US extremists:

- Online social media platforms are playing an increasingly important role in the radicalization processes of US extremists. While US extremists were slow to embrace social media, in recent years, the number of individuals relying on these user-to-user platforms for the dissemination of extremist content and the facilitation of extremist relationships has grown exponentially. In fact, in 2016 alone, social media played a role in the radicalization processes of nearly 90% of the extremists in the PIRUS data.

- Lone actors (i.e. individuals who were operationally alone in their extremist activities) in the PIRUS data were particularly active on social media. From 2005-2016, social media played a role in the radicalization and mobilization processes of 68.12% of the lone actors in the PIRUS data. In 2016 alone, social media factored into the radicalization and mobilization processes of 88.23% of the lone actors in the PIRUS data. By comparison, from 2005 to 2016, social media factored into the radicalization of 50.15% of individuals who were members of extremist groups or radical cliques.

- Despite the increased usage of social media among US extremists, user-to-user communications do not appear to increase the likelihood that extremists will be successful in traveling to foreign conflict zones or committing acts of domestic terrorism. In fact, the extremists who were most active on social media had lower success rates regarding foreign fighter travel and

terrorist plots than individuals who were not as active on social media. Importantly, activity on open social media platforms, such as Facebook and Twitter, played a key role in the identification and interdiction of US foreign fighters and terrorism suspects in several recent cases.

- While social media does not appear to increase the success rates of extremist outcomes, evidence suggests that it contributed to the acceleration of radicalization of US extremists. For example, the average radicalization duration of US foreign fighters in 2005, when social media was first emerging as a factor in the radicalization of US extremists, was approximately 18 months. In 2016, when over 90% of US foreign fighters were active on social media, the duration of radicalization was down to 13 months on average.

Source: START

DOJ's Cyber-Digital Task Force Warns of Foreign Interference in First Report

The Justice Department's new Cyber-Digital Task Force issued its first report highlighting foreign interference in American cyberspace. The report comes three days after President Trump's widely criticized meeting and press conference with Russian President Vladimir Putin and a week after Deputy Attorney General Rod Rosenstein announced the indictment of 12 Russians accused of election meddling. The report also comes the same day Director of National Intelligence Dan Coats reiterated that Russia is the most aggressive state actor continuing to attempt to influence US affairs.

The report covers a range of malign foreign influence operations, including those that target election infrastructure, political organizations, and disinformation operations. The report emphasizes the importance of vigilance against foreign interference in American elections and politics. "Foreign influence operations include covert actions by foreign governments intended to sow division in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve geo-political objectives," the report says. For the report, click HERE.

Source: CBS News

New Office 365 Phishing Attack Uses Malicious Links in SharePoint Documents

Fake emails targeting Office 365 users via malicious links inserted into SharePoint documents are the latest trick phishers employ to bypass the platform's built-in security, Avanan researchers warn.

The cloud security company says that the phishing attack was leveraged against some 10% of its Office 365 customers in the past two weeks and they believe the same percentage applies to Office 365 globally.

About the PhishPoint attack

"The victim receives an email containing a link to a SharePoint document. The body of the message is identical to a standard SharePoint invitation to collaborate," the researchers explained.

“After clicking the hyperlink in the email, the victim’s browser automatically opens a SharePoint file. The SharePoint file content impersonates a standard access request to a OneDrive file, with an ‘Access Document’ hyperlink that is actually a malicious URL.”
As you may guess, the malicious link leads to a spoofed Office 365 login screen, ready to harvest login credentials.

Protection

The company touts its security solution as a good way to catch these types of attacks, since Microsoft doesn’t scan attached files hosted on their other services such as SharePoint and, in any case, wouldn’t be able to blacklist these URLs without blacklisting links to all SharePoint files.

But companies can also implement multi-factor authentication to secure their employees’ Office 365 (and other) accounts and invest in anti-phishing training programs.

“Like many of the more nuanced instances of phishing we analyze, these attacks were designed to be visually indistinguishable from obviously work-related emails that appear safe,” the researchers pointed out, and advised users to be skeptical of emails with URGENT or ACTION REQUIRED in the subject line, be suspicious of URLs in the body of the email and, when presented with a login page, to check whether its URL is actually hosted by the legitimate service.

But, as they noted, if this attack involved links that would trigger a malware download rather than direct to a phishing page, the attack would have caused damage by the time the user clicked and investigated the URL.

Source: HelpNetSecurity

Millions of Android Devices Are Vulnerable Right Out of the Box

Security meltdowns on your smartphone are often self-inflicted: You clicked the wrong link, or installed the wrong app. But for millions of Android devices, the vulnerabilities have been baked in ahead of time, deep in the firmware, just waiting to be exploited. Who put them there? Some combination of the manufacturer that made it, and the carrier that sold it to you.

That’s the key finding of new analysis from mobile security firm Kryptowire, which details troubling bugs preloaded into 10 devices sold across the major US carriers. Kryptowire CEO Angelos Stavrou and director of research Ryan Johnson will present their research, funded by the Department of Homeland Security, at the Black Hat security conference Friday.

The potential outcomes of the vulnerabilities range in severity, from being able to lock someone out of their device to gaining surreptitious access to its microphone and other functions. They all share one common trait, though: They didn’t have to be there.
'The problem is not going to go away.'

Instead, they’re a byproduct of an open Android operating system that lets third-party companies modify code to their own liking. There’s nothing inherently wrong with that; it allows for

differentiation, which gives people more choice. Google will release a vanilla version of Android Pie this fall, but it'll eventually come in all kinds of flavors.

Those modifications lead to headaches, though, including the well-established problem of delays in shipping security updates. They can also, as Stavrou and his team have uncovered, result in firmware bugs that put users at risk.

"The problem is not going to go away, because a lot of the people in the supply chain want to be able to add their own applications, customize, add their own code. That increases the attack surface, and increases the probability of software error," Stavrou says. "They're exposing the end user to exploits that the end user is not able to respond to."

The Black Hat talk focuses largely on devices from Asus, LG, Essential, and ZTE. That last one should pique some interest; DHS has suggested that the China-based company poses a security threat, though the agency hasn't shared any concrete evidence to that effect.

And while DHS-funded, the Kryptowire study doesn't provide that, either. Rather than focusing on manufacturer intent, it looks at the endemic problem of bad code pushed by participants in the broader Android ecosystem.

Take the Asus ZenFone V Live, which Kryptowire found to leave its owners exposed to an entire system takeover, including taking screenshots and video recordings of a user's screen, making phone calls, reading and modifying text messages, and more.

"Asus is aware of the recent ZenFone security concerns raised and is working diligently and swiftly to resolve them with software updates that will be distributed over-the-air to our ZenFone users," the company said in a statement. "Asus is committed to users' security and privacy and we highly encourage all users to update to the latest ZenFone software to ensure a safe and secure user experience."

At this point, pushing an update is the most Asus can do to clean up the mess it made. But Stavrou questions the efficacy of the patching process. "The user has to accept the patch. So even if they send it to the phone, you might not accept the update," he says. He notes also that on some of the models Kryptowire tested, the update process itself was broken, a finding backed up by a recent study from German security firm Security Research Labs.

The attacks Kryptowire details do largely require the user to install an app. But while that's normally a decent limiting factor for potential hacks—stick with the Google Play Store, folks—Stavrou says that what makes these vulnerabilities so pernicious is that those apps don't need to have special privileges when you install them. An app wouldn't, in other words, have to trick you into granting access to your text and call logs. It would take it, simply and silently, thanks to the device's broken firmware.

That scenario could lead to a variety of outcomes, depending on the device. For the ZTE Blade Spark and Blade Vantage, firmware flaws would allow any app to access text messages, call data, and the so-called logcat log, which collects system messages and can include sensitive information like email addresses, GPS coordinates, and more. On the LG G6, the most popular model in the Kryptowire report, vulnerabilities could expose the logcat log, or be used to lock a

user out of their device. And an attacker could factory reset an Essential Phone, wiping both its data and cache.

“Once we were made aware of the vulnerability, it was immediately fixed by our team,” says Essential head of communications Shari Doherty.
There’s nothing you can personally do to fix the problem, or realistically even identify it in the first place.

LG appears to have addressed some but not all of the underlying issues. “LG was made aware of the vulnerabilities and has introduced security updates to address these issues. In fact, most of the reported vulnerabilities have already been patched or have been included in upcoming scheduled maintenance updates not related to security risks,” the company said in a statement.

As for ZTE, the company said in a statement that it has “already delivered and/or is working with carriers today to deliver the maintenance releases that fix these identified issues. ZTE will continue to work with technology partners and carrier customers to deliver future and on-going maintenance releases that continue to protect devices for consumers.”

An AT&T spokesperson confirmed that the carrier had “deployed the manufacturer’s software patches to address this issue.” Verizon and Sprint did not respond to requests for comment. T-Mobile deferred to the CTIA, a wireless industry trade association, which in turn declined to comment until it had a chance to review the Kryptowire findings.

The parade of statements shows progress, but also underscores the key issue. These updates can take months to create and test, Stavrou says, and need to pass through the gauntlet from manufacturer to carrier to customer. While you wait, there’s nothing you can do to fix the problem yourself, or realistically even identify it in the first place.

“One thing that is clear is that there is nobody defending the consumer,” Stavrou says. “It’s so deep in the system that the consumer might not be able to tell that it’s there. Or even if they did, they have no recourse other than waiting for the manufacturer, or the carrier, or whoever is updating the firmware to do so.”

Meanwhile, this batch of findings is just the first in a much longer pipeline that Kryptowire will eventually make public. (It hasn’t yet, in order to give companies enough time to respond.)
“We would like to thank the security researchers at Kryptowire for their efforts to reinforce the security of the Android ecosystem. The issues they have outlined do not affect the Android operating system itself, but rather, third party code and applications on devices,” a Google spokesperson said in a statement.

That third-party code and those apps don’t seem likely to disappear any time soon. And as long as they’re there, expect the deeply hidden headaches to continue.

Source: WIRED

Scammers Targeting Hawaiian Electric Customers Are After New Form of Payment

HONOLULU (HawaiiNewsNow) - Scams to swindle money out of unsuspecting consumers are constantly evolving. And in the latest scam reported by Hawaiian Electric Companies, thieves are going after a new form of electronic currency.

Bitcoins are the form of digital payment scammers are after while targeting Hawaiian Electric customers.
In a news release Tuesday, HECO said scammers are targeting customers on Oahu, Maui and Hawaii Island.

The company says the scammers contact potential victims via phone or email threatening an immediate disconnect of power if payment isn't received. They also send an email with a "disconnection notice" on a letterhead with an outdated Hawaiian Electric logo.

On the email is a QR code to scan at bitcoin machines which will convert cash into digital currency.
But HECO warns not to fall for it — it's all a scam.

“This is simply a new twist on an old scam but our same advice applies: just hang up,” Jim Alberts, senior vice president for customer service of the Hawaiian Electric Companies said. “Whether it’s bitcoin, gift cards or money orders, our companies aren’t going to threaten you or have you running around town to meet unorthodox payment demands.”

On Oahu alone, three businesses reported falling victim to the deception. HECO says they reportedly paid hundreds of dollars at local bitcoin machines.
Adding to the apparent authenticity, HECO says the scammer provide a callback number the leads to an automated recording, similar to the one used by Hawaiian Electric Companies.
HECO provided this advice for customers to avoid being scammed:

- Hang up on calls demanding immediate payment over the phone or via prepaid debit cards or bitcoin.
- If the caller asks to meet you to pick up a payment or provides directions to a bitcoin machine, it’s a scam.
- Don't fall for it if the caller says your account is delinquent and threatens to shut off your power immediately unless payment is made.

For any dealings with electric company payment or billing, check with HECO customer service on their website, or call the number listed on monthly electric bills.
HECO added they do not accept bitcoins as a form of payment, like almost all utilities across the nation.

Source: Hawaii News Now

Hackers Exploit Voicemail Vulnerability to Access Financial Accounts

You already know how important it is to have strong passwords and two-factor authentication on your online accounts — but you may not have considered your voicemail password. Voicemail accounts are startlingly easy for hackers to access, and that can be a problem for your other online accounts.

That's because most of your online accounts let you reset your password by phone. Theoretically, by calling or texting an access code to your phone number, a service can confirm your identity before letting you reset your password. But if a hacker has access to your voicemail, they can request a password reset code by phone and intercept it. Then they change your password and have full access to your account. Websites like PayPal, eBay, LinkedIn and Instagram are all vulnerable — and even secure messaging apps like WhatsApp and Signal can be compromised.

The hack itself is simple. Many voicemail accounts have default passwords or easy to guess passwords, like the last four digits of your phone number. Even if you change the password, you usually only need to provide a weak four-digit code — and most phone providers allow you to guess your code as many times as you want without locking your account. That means a hacker can just go through every possible number combination until they hit the right one. After that, it's easy for them to force your calls to voicemail so they can intercept your password reset code.

Some companies — including PayPal — have protections against this kind of hack, but those can be bypassed, too. PayPal will call you with a password reset code, but requires you to enter that code during the phone call. Hackers can get around this by listening to the code, then changing voicemail greeting to a recording of the code.
In the end, the problem is that our voicemail accounts aren't very secure — and the prevalence of password reset by phone leaves us all vulnerable. The only way to completely prevent such an attack is to shut down your voicemail entirely, which isn't practical for most people. However, you can make it more difficult for hackers by changing your voicemail password. Fortunately, most mobile carriers make it easy. Here are instructions for resetting your password on each carrier:

- AT&T
- Sprint
- T-Mobile
- Verizon

When you reset your password, be sure:

- Make it as long as possible, preferably a random series of numbers.
- Don't include any easily guessable personal information, like addresses, phone numbers or birthdays.
- Save it in your password manager so you don't forget it.

And, of course, you should make sure your other passwords are up to snuff, too. Anything you do to make it harder for hackers to get into your accounts makes it less likely you'll be a victim.

Source: Techlicious

Hackers Are Now Using Farm Sprinklers As Cyber Weapons

It was in the bygone days when hackers would invade only in your computers and servers in order to get access to your data. Apparently, the taste of hackers, and their capabilities, are changing and growing which goes to the extent that they can get control over the sprinklers in your farm.

Researchers have found a glitch in commercial irrigation system which can allow hackers to get access to the sprinklers and activate them whenever they want. They can feed false weather data into the system which leads to the sprinklers getting operational at absurd intervals.

This doesn't only affect or hamper the system of the owner of sprinklers or the farm but the side-effects go on a wider level. If the hackers keep running 24,000 sprinklers, it can make an enormous water reservoir empty in just a few hours.

The disruption of systems by hackers is not limited to water reservoirs and sprinklers but they can also acquire control over power grid and hinder the whole power supply of a big area. Once they manage to obtain a control over such important systems, the expenses to fix the problem could up to several millions.

In Israel, the researchers who discovered these glitches have warned the manufacturers about vulnerabilities their sprinklers are subjected to. All of this could be attributed to IoT which makes it easy for hackers to fetch internal information about the systems.

Source: Deccan Chronicle

Hackers account for 90% of login attempts at online retailers

Selling stolen personal data is a big business for hackers: Somewhere on the dark web, your e-mail address and a few passwords are probably for sale (hopefully, old ones). Cyber criminals buy troves of this information to try to login to websites where they can grab something valuable like cash, airline points, or merchandise like expensive cheese. Yes, cheese.

Online retailers are hit the most by these attacks, according to a report by cyber security firm Shape Security. Hackers use programs to apply stolen data in a flood of login attempts, called "credential stuffing." These days, more than 90% of e-commerce sites' global login traffic comes from these attacks. The airline and consumer banking industries are also under siege, with about 60% of login attempts coming from criminals.

These attacks are successful as often as 3% of the time, and the costs quickly add up for businesses, Shape says. This type of fraud costs the e-commerce sector about $6 billion a year, while the consumer banking industry loses out on about $1.7 billion annually. The hotel and airline businesses are also major targets—the theft of loyalty points is a thing—costing a combined $700 million every year.

Targeting “little monsters”

“Criminals harvest usernames and passwords from data breaches and test them on every website and mobile app imaginable,” Shape said in its report. The Mountain View, California-based company says it monitors 1.6 billion accounts for credential stuffing. The seven-year-old firm’s co-founders were Pentagon advisors and worked at defense contractor Raytheon.
The process starts when hackers break into databases and steal login information. Some of the best known “data spills” took place at Equifax and Yahoo, but they happen fairly regularly—there were 51 reported breaches last year, compromising 2.3 billion credentials, according to Shape. Hackers frequently target web forums: The Lady Gaga “Little Monster” fan site had a breach last year that reportedly impacted about 1 million accounts containing birthday, password, and e-mail information.

Adult and porn websites, by contrast, didn’t report any data breaches last year. It will take some time to know whether these sites successfully blocked hackers, or if they simply haven’t yet realized (or reported) that data may have been compromised. AdultFriendFinder.com’s database was one of the biggest credential exploits in 2016.

By the time you hear about a hacker intrusion, it’s usually too late; on average, it takes 15 months from the day credential data is stolen to the day an intrusion is revealed. That’s more than enough time for criminals to deploy the data of unsuspecting people in thousands of credential stuffing attacks.

Premium cheddar

Criminals steal personal data from places with weak protection and then use login data on sites and apps that are much higher value and better protected. Taking over bank accounts is one way to monetize stolen login information—in the US, community banks are attacked far more than any other industry group. According to Shape’s data, that sector is attacked more than 200 million times each day.

Another way to turn stolen data into cash is to buy merchandise, from gift cards to physical goods like electronics, that can easily be resold. It turns out that expensive cheese, like $200-per-pound Wyke Farms cheddar, is sometimes used in criminal schemes. Hackers use stolen credentials to break into online grocery accounts to buy high-priced cheese and then resell it to restaurants for cash, Shape says.

Airlines’ frequent flyer miles are also targeted. Shape points out that these miles or points aren’t protected with the sophisticated security used for financial accounts, and users are often much slower to notice their account has been broken into and drained.
Stolen frequent flyer miles have helped give rise to a gray market for these awards. Criminals sell them to specialist brokers who purchase award points from hotels and airlines. After the miles are transferred to the broker’s account, the cyber thief is usually paid via PayPal, Shape says. The mileage brokers then sell the points to online travel agencies, which they use to sell discounted tickets for business class and first class airfares. Some discounted online deals really are too good to be true.

Change your passwords

Cyber criminals are becoming more sophisticated, sharing successful techniques and tools with others hackers on the dark web. But not all is lost—the number of reported credential breaches was roughly stable at 51 last year, compared with 52 in 2016, Shape says. The size of data spills also declined. This suggests cyber security is improving, even as threats escalate. In the mean-time, consumers can do their part to minimize these attacks by changing their passwords.

Source: QZ

Malware Author Builds 18,000-Strong Botnet in a Day

A malware author has built a huge botnet comprised of over 18,000 routers in the span of only one day.

This new botnet has been spotted yesterday by security researchers from NewSky Security, and their findings have been confirmed today by Qihoo 360 Netlab, Rapid7, and Greynoise.

Botnet built with one exploit only

The botnet has been built by exploiting a vulnerability in Huawei HG532 routers, tracked as CVE-2017-17215.

Scans for this vulnerability, which can be exploited via port 37215, started yesterday morning, July 18, according to data collected by Netlab's NetScan system.

By late in the evening, NewSky security researcher Ankit Anubhav says the botnet had already gathered 18,000 routers.

Anubhav told *Bleeping Computer* the botnet author reached out to him to brag about his actions, even sharing a list with the IP addresses of all of the botnet's victims.

Botnet author is a known threat actor

The botnet herder identified himself with the pseudonym "Anarchy." Answering inquiries from both Anubhav and Bleeping Computer, Anarchy did not provide a reason why he created the botnet.

But Anubhav believes Anarchy may actually be a hacker who previously identified as Wicked, which Anubhav interviewed on NewSky's blog and Fortinet featured in a report here.

Wicked/Anarchy is a well-known malware author who, in the past, has created variations of the Mirai IoT malware. These variations and their respective botnets were known as Wicked, Omni, and Owari (Sora), and had been previously used for DDoS attacks.

Botnet will also target Realtek routers

But the real problem here is not a malware author doing what he does best. The problem is the relative ease with which Anarchy built a gigantic botnet within one day.

He didn't do it with a zero-day or some vulnerability that had not been exploited before. He did so with a high-profile vulnerability that many botnets have exploited before.

CVE-2017-17215 is a well-known exploit that has been abused by at least two versions of the Satori botnet [1, 2], and many of the smaller Mirai-based offshoots. You'd think that by now users would have patched devices or ISPs would have blocked incoming connections on port 37215.

But Anarchy is not done yet. The botnet author told Anubhav that he also plans to target CVE-2014-8361, a vulnerability in Realtek routers exploitable via port 52869.

"Testing has already started for the Realtek exploit during the night," Anubhav told Bleeping Computerin a private conversation today. [Update: Both Rapid7 and Greynoise are confirming that scans for Realtek have gone through the roof today.]

It's both hilarious and sad that somebody can nowadays build a huge DDoS botnet in less than a day. This only shows the real sad state of SOHO router security.
IOCs, courtesy of NewSky Security and CERT Tunisia:

SHA-256: 61440574aafaf3c4043e763dd4ce4c628c6c92fb7d7a2603076b3f60f2813f1b [Source]
C2: hxxp://104.244.72.82

Source: Bleeping Computer

Singapore Personal Data Hack Hits 1.5m, Health Authority Says

Hackers have stolen personal data in Singapore belonging to some 1.5 million people, or about a quarter of the population, officials say.

They broke into the government health database in a "deliberate, targeted and well-planned" attack, according to a government statement.

Those targeted visited clinics between 1 May 2015 and 4 July of this year.
Data taken include names and addresses but not medical records, other than medicines dispensed in some cases.

"Information on the outpatient dispensed medicines of about 160,000 of these patients" was taken, **the statement** says.

"The records were not tampered with, ie no records were amended or deleted. No other patient records, such as diagnosis, test results or doctors' notes, were breached. We have not found evidence of a similar breach in the other public healthcare IT systems."

The data of Prime Minister Lee Hsien Loong, including information on his outpatient dispensed medicines, was "specifically and repeatedly targeted". Mr Lee has survived cancer twice.
Singapore, a wealthy city state, prides itself on its stability and security.

- Singapore PM's website is hacked
- Singapore profile
- What are malware, patches and worms?

How were systems breached?

It appears that a computer belonging to SingHealth, one of the state's two major government healthcare groups, was infected with malware through which the hackers gained access to the database.

They struck some time between 27 June and 4 July, according to the government.

SingHealth has temporarily banned staff from accessing the internet on all 28,000 of its work computers, according to the Straits Times.

The move is aimed at plugging leaks from work e-mails and shared documents as well as guarding against possible cyber-attacks. Other public healthcare institutions are expected to do the same.

How vulnerable is Singapore to hacking?

The government has previously warned of cyber-attacks, saying it has been the target of international hackers, but most attacks were foiled.

It has stepped up measures in recent years, including disconnecting computers for certain key ministries in the civil service from the internet, so that they operate on intranet only.
A cyber-attack last year targeted the defense ministry but only got basic information on military conscripts.

In 2013, Mr Lee's official website was "compromised" by people claiming to be members of the hacking group Anonymous.

The hackers posted an image of a Guy Fawkes mask - the symbol of the Anonymous group - on the prime minister's site with the words: "It's great to be Singaporean today."

Anonymous had earlier threatened to target infrastructure in Singapore in what it said was a protest against licensing regulations on news websites.

Singapore is not the only country to be subjected to high-profile attacks by hacking groups.
Others include:

- Earlier this year, Germany's government IT network was attacked by hackers targeting the interior ministries' private networks. It was reported that a group known as Fancy Bear was responsible
- In February, the US and UK said that the Russian military was behind a "malicious" cyber-attack on Ukraine last year that spread globally. Moscow denied being behind the attack

- A cyber-attack crippled the UK's National Health Service (NHS) and other organizations around the world in May last year. A hacking group in North Korea known as Lazarus is believed to have launched the attack, which involved malware known as WannaCry
- **In 2014, the US claimed that North Korea was behind cyber-attacks on Sony Pictures**, after the entertainment company released a film featuring the fictional killing of its leader Kim Jong-un

Why target health services?

Health records are often targeted because they contain valuable information to governments, says Eric Hoh, the Asia Pacific president of security company FireEye.

"Nation states increasingly collect intelligence through cyber espionage operations which exploit the very technology we rely upon in our daily lives," he says, adding: "Many businesses and governments in South East Asia face cyber threats, but few recognise the scale of the risks they pose."

Source: BBC

Hackers Breach Russian Bank and Steal $1 Million Due to Outdated Router

A notorious hacker group known as MoneyTaker has stolen roughly $1 million from a Russian bank after breaching its network via an outdated router.

The victim of the hack is PIR Bank, which lost at least $920,000 in money it had stored in a corresponding account at the Bank of Russia.

Group-IB, a Russian cyber-security firm that was called in to investigate the incident, says that after studying infected workstations and servers at PIR Bank, they collected "irrefutable digital evidence implicating MoneyTaker in the theft."

Group-IB are experts in MoneyTaker tactics because they unmasked the group's existence and operations last December when they published a report on their past attacks.

Experts tied the group to thefts at US, UK, and Russian banks and financial institutions going back as far as 2016. According to Group-IB, the MoneyTaker attacks that hit banks were focused on infiltrating inter-banking money transfer and card processing systems such as the First Data STAR Network and the Automated Work Station Client of the Russian Central Bank (AWS CBR) system.

How the hack unfolded

This is what happened this time as well, according to Group-IB. Hackers infiltrated PIR Bank's network at the end of May via an outdated router at one of the bank's regional branches.

"The router had tunnels that allowed the attackers to gain direct access to the bank’s local network," Group-IB experts said. "This technique is a characteristic of MoneyTaker. This scheme

has already been used by this group at least three times while attacking banks with regional branch networks."

Hackers then used the router to infect the bank's local network with malware. They then used PowerShell scripts to gain persistence and carry out malicious operations without being detected.

When, finally, the hackers breached PIR Bank's main network, they also gained access to its AWS CBR account, the system they needed to control financial transactions.

On July 3, MoneyTaker used this system to transfer funds from PIR Bank's account at the Bank of Russia to 17 accounts they created in advance. Moments after the stolen funds landed in these accounts, money mules withdrew it from ATMs across Russia.

PIR Bank employees discovered the hack a day later, on July 4, but by that moment it was already too late to reverse transactions.

In typical MoneyTaker fashion, hackers tried clearing logs from infected computers in order to hide their tracks, but Group-IB said they found reverse shells the group used to access compromised computers.

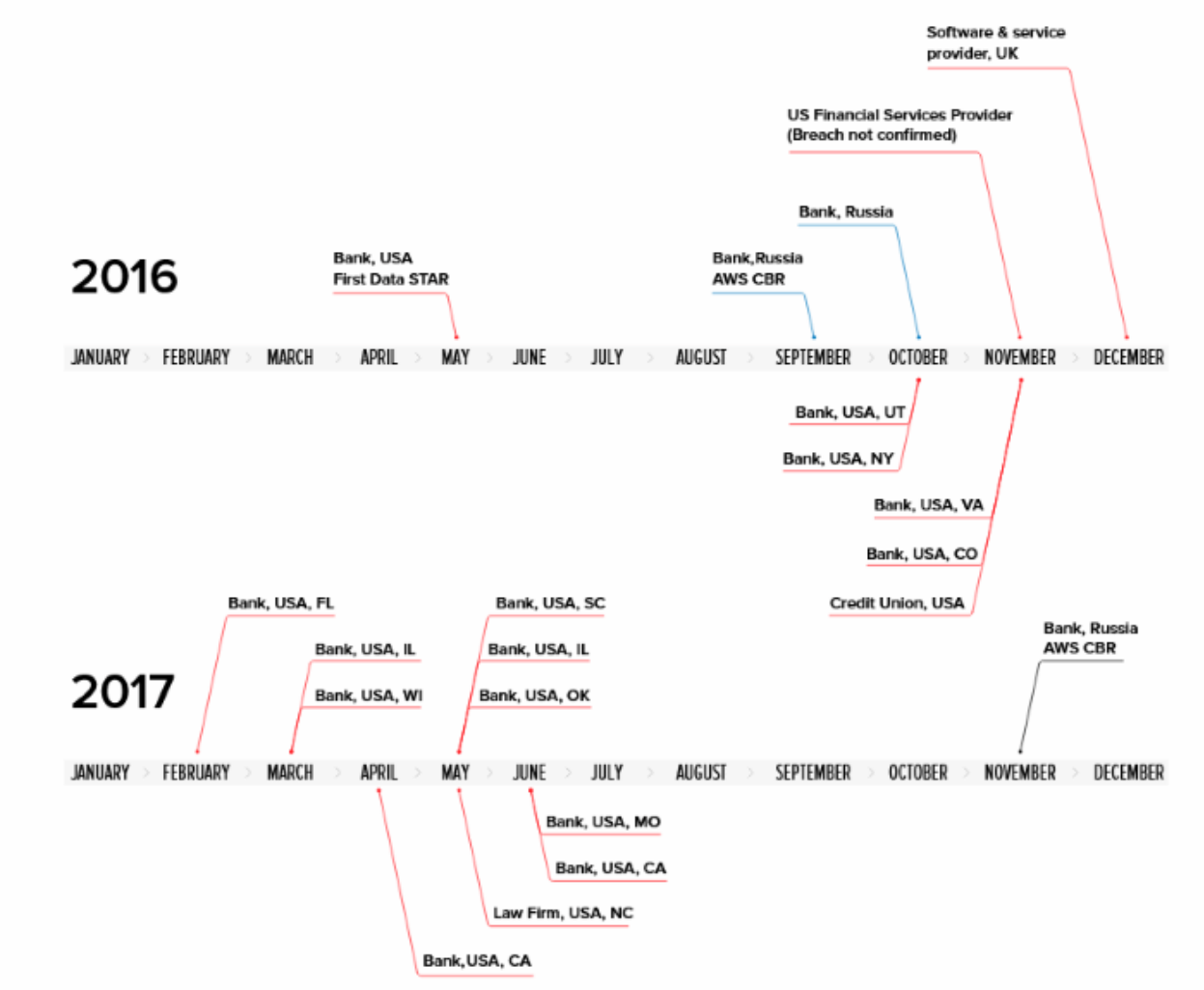
Not the first MoneyTaker hack in Russia this year

"This is not the first successful attack on a Russian bank with money withdrawal since early 2018," says Valeriy Baulin, Head of Digital Forensics Lab Group-IB. "We know of at least three similar incidents, but we cannot disclose any details before our investigations are completed."
Group-IB says that at least two of these 2018 hacks of Russian banks have been carried out by the MoneyTaker group.

The group's activities are very hard to track because they tend to use common OS utilities to perform malicious actions instead of relying on actual malware. They also clear logs and study each bank's network and system in advance, even stealing documentation to understand with what they're dealing with.

During its three-year lifespan, it is believed the group stole tens of millions from banks since they started their hacking spree back in 2016. Group-IB says the average losses are of $500,000 per incident in the US and around $1.2 million per incident in Russia.

Past MoneyTaker hacks include 15 US banks, a US services provider, a UK banking software company, 5 Russian banks, and one Russian law firm. Below is a chart of past MoneyTaker hacks, last updated December 2017.



Source: Bleeping Computer

DHS: Russian Hackers Targeted Control Systems for Electric Utilities

WASHINGTON — The Department of Homeland Security told representatives of electric utilities Monday about a round of efforts by Russian hackers last year to target control systems for electric power plants and grids.

In an unclassified webinar, DHS officials said the hackers last summer got access to vendors who provide computer services to electric utilities, and used that to provide a way into power company control systems.
"Over the course of the past year as we continued to investigate the activity, we learned additional information which would be helpful to industry in defending against this threat."
The webinar was first reported by The Wall Street Journal.

DHS has been warning the industry for years about efforts to target power plants and other utilities with cyber attacks. One of the ways utilities have responded has been to take their control

systems off the internet, so they cannot be easily hacked. The webinar said the latest Russian effort involved the roundabout means of getting access through third-party vendors.

Source: NBC News

Idaho Inmates Exploit Tablet Software Flaw to Steal $225K

Over 360 inmates exploited a vulnerability in JPay, which prisoners use to access email, news, and entertainment, to manipulate the credit amounts in their JPay accounts.

Tablet computers and a software vulnerability were enough to help 364 prison inmates in Idaho collectively steal $225,000.
According to the Idaho Department of Correction, the inmates were caught earlier this month exploiting a vulnerability in their prison-issued tablets, which allowed them to manipulate the digital credits they used to buy games and music.

The tablets were issued by JPay, which specializes in offering an online system for prison inmates. The services on board the tablets can let inmates read and write emails, view educational materials, and access entertainment.

But apparently, the JPay system also contained a vulnerability involving account credit amounts, which inmates across five Idaho correctional facilities decided to hack. "Fifty inmates credited their accounts in amounts of more than $1,000. The highest amount credited by a single inmate was $9,990.35," Jeff Ray, spokesman for the Idaho Department of Correction, said in an email.

"This conduct was intentional, not accidental," he added. "It required a knowledge of the JPay system and multiple actions by every inmate who exploited the system's vulnerability to improperly credit their account."

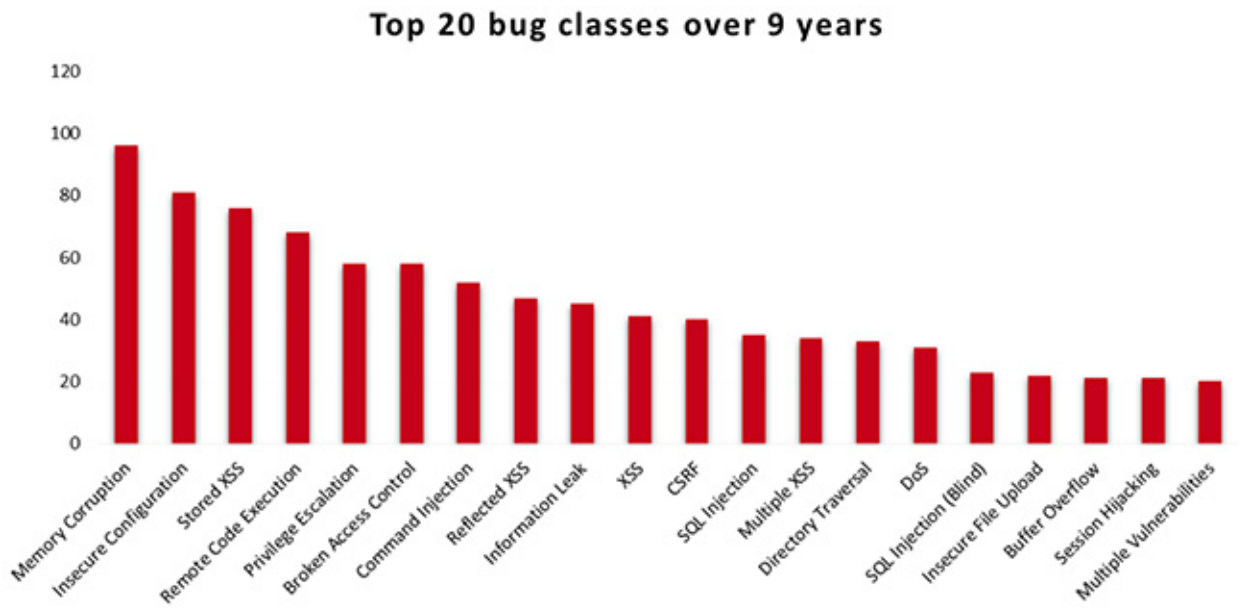
CenturyLink, which operates JPay, declined to disclose how the software was breached, but the vulnerability has been fixed, it said. The $225,000 was also stolen from the JPay system and was not taxpayer dollars.

So far, only $65,000 of the stolen credits has been recovered. As a punishment, Idaho correctional facilities have suspended the inmates' ability to download more music and games until they refund JPay. The inmates are also facing further disciplinary action that could reclassify the severity of their custody level.

Source: PCMag

Same web-based vulnerabilities still prevalent after nine years

Analysis of vulnerabilities discovered by NCC Group researchers over the last nine years found that instances of common web-based vulnerabilities have largely refused to fall over during this time, with cross-site scripting (XSS) vulnerabilities appearing the most frequently.



The global cyber security and risk mitigation expert found that despite this type of vulnerability being understood across the industry for decades, XSS flaws, which enable attackers to inject malicious scripts into websites or victim browsers, still account for 18% of all bugs logged.

However, some classes of bugs have become almost non-existent, including format string flaws, in which submitted data is evaluated as a command by the application, as well as some memory-related flaws, and flaws that allow the exploitation of XML applications and services.

Commenting on this analysis, Matt Lewis, research director at NCC Group, said: “While some historically common vulnerabilities have disappeared over the last nine years, cross-site scripting has been around for almost 20 years. We should have seen a significant fall in these types of vulnerabilities, but this hasn’t been the case, which highlights the need for better education around security within the software development life cycle.”

Overall, the team uncovered vulnerabilities in 53 different categories, and found that there was an increase in the number of bugs targeting complex applications and hardware. This included deserialization flaws – when untrusted data is used to abuse the logic of an application and inflict DDoS or remote code attacks – and the exploitation of multiple low-risk issues in a chain across a complex web application, resulting in full, unauthorized control.

As well as this, researchers saw an increase in hardware-related design flaws, following an increased engagement with embedded systems and IoT devices.
Matt Lewis added: “Although there could be a lot of factors influencing the discovery of bugs over the last nine years – such as shifts in industry focus with regard to certain classes of bugs, and even the time that our consultants have available – there is still an ongoing prevalence of the most common vulnerabilities.

“As well as this, we’re already seeing an increasing variety of relatively new attack methods as applications and systems become more complex. This highlights the need for more investment

into security skills, as well as a wider understanding of how important the mitigation of these vulnerabilities is for the overall security of businesses."

Source: Help Net Security

Dixons Carphone data breach hit extra 9m customers

Dixons Carphone has apologized to all of its customers after revealing that a 2017 data breach affected personal data held in an additional 8.8 million customer records.

The admission early on Tuesday is the second revelation related to the data breach in six weeks and the third since 2015.

The company says it was alerted to the breach by investigators on Monday evening.
The admission early on Tuesday is the second revelation related to the data breach in six weeks and the third since 2015. The company says it was alerted to the breach by investigators on Monday evening.

Sky News reported in June that the company said it believed there had been other recently discovered attempts since last year to compromise 5.9 million cards in one of its processing systems for Currys PC World and Dixons Travel stores.

Dixons Carphone said an additional 1.2 million personal data records were hacked at the time.
The 8.8 million customer personal records the company flagged up on Tuesday, relating to dates of birth, addresses and phone numbers, take the total number of personal records affected to 10 million.

After acknowledging that customer data had been compromised a second time since last year, Dixons Carphone chief executive Alex Baldock said the company had been working "around the clock" to put it right.

He said: "That's included closing off the unauthorized access, adding new security measures and launching an immediate investigation, which has allowed us to build a fuller understanding of the incident that we're updating on today."

He added: "Again, we're disappointed in having fallen short here, and very sorry for any distress we've caused our customers. I want to assure them that we remain fully committed to making their personal data safe with us."

:: Customers angry Carphone hack kept 'secret'

The company said that while there was evidence that some of the compromised data may have left its systems, the records "do not contain payment card or bank account details and there is no evidence that any fraud has resulted".

Source: SKY

PSA: Security Flaws Exposed Partial Addresses & SSN's of 26M Comcast Users

Comcast Xfinity customers are the latest to be affected by lax online security. According to a report from *BuzzFeed News*, more than 26.5 million customers had their partial home addresses and social security numbers exposed…

Security researcher Ryan Stevenson first uncovered the security flaws. These vulnerabilities were in Comcast's online customer portal and made it "easy for even an unsophisticated hacker to access this sensitive information."
BuzzFeed News informed Comcast of the security holes, and the internet provider was quickly able to patch the flaws. In a statement addressing the data breach, a Comcast spokesperson explained that it blocked the security vulnerabilities within "hours," while also reaffirming the company's commitment to security:

Spokesperson David McGuire told BuzzFeed News, "We quickly investigated these issues and within hours we blocked both vulnerabilities, eliminating the ability to conduct the actions described by these researchers. We take our customers' security very seriously, and we have no reason to believe these vulnerabilities were ever used against Comcast customers outside of the research described in this report."

One of the flaws related to an "in-home authentication page" where a user is able to pay their bills without signing in. The portal allowed customers to verify their account information based on partial home addresses suggested by the Comcast site, if the device was or appeared to be connected to the home network:

Eventually, the page would show the first digit of the street number and first three letters of the correct street name, while asterisks hid the remaining characters. A hacker could then use IP lookup websites to determine the city, state, and postal code of the partial address.

The second vulnerability was discovered via a sign-up page for Comcast Authorized Dealers. By using a customer's billing address, a hacker could "brute force the last four digits of a customer's social security number." Eventually, because the page did not limit how many attempts, hackers would reveal the social security number:

Armed with just a customer's billing address, a hacker could brute force (in other words, repeatedly try random four-digit combinations until the correct combination is guessed) the last four digits of a customer's social security number. Because the login page did not limit the number of attempts, hackers could use a program that runs until the correct social security number is inputted into the form.

Comcast says it is still investigating the vulnerabilities, but has yet to find any foul play thus far.

Source: 9to5mac

In-the-wild router exploit sends unwitting users to fake banking site

Hackers have been exploiting a vulnerability in DLink modem routers to send people to a fake banking website that attempts to steal their login credentials, a security researcher said Friday. The vulnerability works against DLink DSL-2740R, DSL-2640B, DSL-2780B, DSL-2730B, and DSL-526B models that haven't been patched in the past two years. As described in disclosures here, here, here, here, and here, the flaw allows attackers to remotely change the DNS server that connected computers use to translate domain names into IP addresses.

According to an advisory published Friday morning by security firm Radware, hackers have been exploiting the vulnerability to send people trying to visit two Brazilian bank sites—Banco de Brasil's www.bb.com.br and Unibanco's www.itau.com.br—to malicious servers rather than the ones operated by the financial institutions. In the advisory, Radware researcher Pascal

Geenens wrote:

"The attack is insidious in the sense that a user is completely unaware of the change. The hijacking works without crafting or changing URLs in the user's browser. A user can use any browser and his/her regular shortcuts, he or she can type in the URL manually or even use it from mobile devices such as iPhone, iPad, Android phones or tablets. He or she will still be sent to the malicious website instead of to their requested website, so the hijacking effectively works at the gateway level."

Convincing spoof

Geenens told Ars that Banco de Brasil's website can be accessed over unencrypted and unauthenticated HTTP connections, and that prevented visitors from receiving any warning the redirected site was malicious. People who connected using the more secure HTTPS protocol received a warning from the browser that the digital certificate was self-signed, but they may have been tricked into clicking an option to accept it. Other than the self-signed certificate, the site was a convincing spoof of the real site. If users logged in, their site credentials were sent to the hackers behind the campaign. The spoof site was served from the same IP address that hosted the malicious DNS server.

People who tried to visit Unibanco were redirected to a page hosted at the same IP address as the malicious DNS server and fake Banco de Brasil site. That page, however, didn't actually spoof the bank's site, an indication that it was probably a temporary landing page that had not yet been set up. The malicious operation was shut down early Friday morning California time after Geenens reported the malicious DNS server and spoof site to server host OVH. With the malicious DNS server inoperable, people connected to infected DLink devices will likely be unable to use the Internet until they change the DNS server settings on their router or reconfigure their connecting devices to use an alternate DNS server.
This is the latest hack campaign to exploit a router. In May, researchers uncovered what's likely an unrelated attack that infected an estimated 500,000 consumer-grade routers made by a variety of manufacturers. The FBI has warned that VPNFilter, as the highly advanced router malware has been dubbed, is the work of hackers working for the Russian government.

In 2016, malware known as DNSChanger caused routers that were running unpatched firmware or were secured with weak administrative passwords to use a malicious DNS server. Connected computers would then connect to fake sites. But in this case the router was reconfigured from within the home, not remotely from the Internet.

The best defense against router attacks is to ensure devices are running the most up-to-date firmware and are secured with a strong password. A good defense-in-depth move is also to configure each device that connects to use a trusted DNS server, such as 1.1.1.1 from Cloudflare or 8.8.8.8 from Google. These settings, which are made in the operating system of the connecting device, will override any settings made in the router.

Source: arstechnica

Americans are the Main Targets for Crypto Hackers, New Study Reveals

https://www.ccn.com/americans-are-the-main-targets-for-crypto-hackers-new-study-reveals/

Three Members of Notorious International Cybercrime Group "Fin7" In Custody for Role in Attacking Over 100 U.S. companies

Victim Companies in 47 U.S. States; Used Front Company 'Combi Security' to Recruit Hackers to Criminal Enterprise

Three high-ranking members of a sophisticated international cybercrime group operating out of Eastern Europe have been arrested and are currently in custody facing charges filed in U.S. District Court in Seattle, announced Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Annette L. Hayes for the Western District of Washington and Special Agent in Charge Jay S. Tabb Jr. of the FBI Seattle Field Office.

According to three federal indictments unsealed today, Ukrainian nationals Dmytro Fedorov, 44, Fedir Hladyr, 33, and Andrii Kolpakov, 30, are members of a prolific hacking group widely known as FIN7 (also referred to as the Carbanak Group and the Navigator Group, among other names). Since at least 2015, FIN7 members engaged in a highly sophisticated malware campaign targeting more than 100 U.S. companies, predominantly in the restaurant, gaming, and hospitality industries. As set forth in indictments, FIN7 hacked into thousands of computer systems and stole millions of customer credit and debit card numbers, which the group used or sold for profit.

In the United States alone, FIN7 successfully breached the computer networks of companies in 47 states and the District of Columbia, stealing more than 15 million customer card records from over 6,500 individual point-of-sale terminals at more than 3,600 separate business locations. Additional intrusions occurred abroad, including in the United Kingdom, Australia, and France. Companies that have publicly disclosed hacks attributable to FIN7 include such familiar chains as Chipotle Mexican Grill, Chili's, Arby's, Red Robin and Jason's Deli. Additionally in Western Washington, FIN7 targeted other local businesses.

"The three Ukrainian nationals indicted today allegedly were part of a prolific hacking group that targeted American companies and citizens by stealing valuable consumer data, including personal credit card information, that they then sold on the Darknet," said Assistant Attorney General Benczkowski. "Because hackers are committed to finding new ways to harm the American

public and our economy, the Department of Justice remains steadfast in its commitment to working with our law enforcement partners to identify, interdict, and prosecute those responsible for these threats."

"Protecting consumers and companies who use the internet to conduct business – both large chains and small 'mom and pop' stores -- is a top priority for all of us in the Department of Justice," said U.S. Attorney Hayes. "Cyber criminals who believe that they can hide in faraway countries and operate from behind keyboards without getting caught are just plain wrong. We will continue our longstanding work with partners around the world to ensure cyber criminals are identified and held to account for the harm that they do – both to our pocketbooks and our ability to rely on the cyber networks we use."

"The naming of these FIN7 leaders marks a major step towards dismantling this sophisticated criminal enterprise," said Special Agent in Charge Tabb. "As the lead federal agency for cyber-attack investigations, the FBI will continue to work with its law enforcement partners worldwide to pursue the members of this devious group, and hold them accountable for stealing from American businesses and individuals."

Each of the three FIN7 conspirators is charged with 26 felony counts alleging conspiracy, wire fraud, computer hacking, access device fraud, and aggravated identity theft.

In January 2018, at the request of U.S. officials, foreign authorities separately arrested Ukrainian Fedir Hladyr and a second FIN7 member, Dmytro Fedorov. Hladyr was arrested in Dresden, Germany, and is currently detained in Seattle pending trial. Hladyr allegedly served as FIN7's systems administrator who, among other things, maintained servers and communication channels used by the organization and held a managerial role by delegating tasks and by providing instruction to other members of the scheme. Hladyr's trial is currently scheduled for Oct. 22.

Fedorov, a high-level hacker and manager who allegedly supervised other hackers tasked with breaching the security of victims' computer systems, was arrested in Bielsko-Biala, Poland. Fedorov remains detained in Poland pending his extradition to the United States.

In late June 2018, foreign authorities arrested a third FIN7 member, Ukrainian Andrii Kolpakov in Lepe, Spain. Kolpakov, also alleged to be a supervisor of a group of hackers, remains detained in Spain pending the United States' request for extradition.

According to the indictments, FIN7, through its dozens of members, launched numerous waves of malicious cyberattacks on numerous businesses operating in the United States and abroad.

FIN7 carefully crafted email messages that would appear legitimate to a business' employee, and accompanied emails with telephone calls intended to further legitimize the email. Once an attached file was opened and activated, FIN7 would use an adapted version of the notorious Carbanak malware in addition to an arsenal of other tools to ultimately access and steal payment card data for the business' customers. Since 2015, FIN7 sold the data in online underground marketplaces. (Supplemental document "How FIN7 Attacked and Stole Data" explains the scheme in greater detail.)

FIN7 used a front company, Combi Security, purportedly headquartered in Russia and Israel, to provide a guise of legitimacy and to recruit hackers to join the criminal enterprise. Combi Security's website indicated that it provided a number of security services such as penetration testing. Ironically, the sham company's website listed multiple U.S. victims among its purported clients.

The charges in the indictments are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The indictments are the result of an investigation conducted by the Seattle Cyber Task Force of the FBI and the U.S. Attorney's Office for the Western District of Washington, with the assistance of the Justice Department's Computer Crime and Intellectual Property Section and Office of International Affairs, the National Cyber-Forensics and Training Alliance, numerous computer security firms and financial institutions, FBI offices across the nation and globe, as well as numerous international agencies. Arrests overseas were executed in Poland by the "Shadow Hunters" from CBŚP (Polish Central Bureau of Investigation); in Germany by the LKA Sachsen - Dezernat 33, (German State Criminal Police Office) and the Polizeidirektion Dresden (Dresden Police); and in Spain the Grupo de Seguridad Logica within the Unidad de Investigación Technologica of the Cuerpo Nacional de Policía (Spanish National Police)..

This case is being prosecuted by Assistant U.S. Attorneys Francis Franze-Nakamura and Steven Masada of the Western District of Washington with assistance from Trial Attorney Anthony Teelucksingh of the Justice Department's Computer Crime and Intellectual Property Section.

Source: DOJ

Half a Billion IoT Devices Vulnerable to DNS Rebinding Attacks

Armis, the cyber-security firm that discovered the BlueBorne vulnerabilities in the Bluetooth protocol, warns that nearly half a billion of today's "smart" devices are vulnerable to a decade-old attack known as DNS rebinding.

Spurred by recent reports regarding DNS rebinding flaws in Blizzard apps, uTorrent, and Google Home, Roku TV, and Sonos devices, the company has recently analyzed the impact this type of attack has on Internet-of-Things-type of devices.

What is a DNS rebinding attack

DNS rebinding attacks are when an attacker tricks a user's browser or device into binding to a malicious DNS server and then make the device access unintended domains.
DNS rebinding attacks are normally used to compromise devices and use them as relay points inside an internal network. A typical DNS rebinding attack usually goes through the following stages:

1) Attacker sets up a custom DNS server for a malicious domain.
2) Attacker fools victim into accessing a link for this malicious domain (this can be done via phishing, IM spam, XSS, or by hiding a link to the malicious domain on a malicious site or inside ads delivered on legitimate sites).

3) The user's browser makes a query for that domain's DNS settings. 4) The malicious DNS server responds, and the browser caches an address like XX.XX.XX.XX.
5) Because the attacker has configured the DNS TTL setting inside the initial response to be one second, after one second, the user's browser makes another DNS request for the same domain, as the previous entry has expired and it needs a new IP address for the malicious domain.
6) The attacker's malicious DNS setting responds with a malicious IP address, such as YY.YY.YY.YY, usually for a domain inside the device's private network.
7) Attacker repeatedly uses the malicious DNS server to access more and more of these IPs on the private network for various purposes (data collection, initiating malicious actions, etc.).

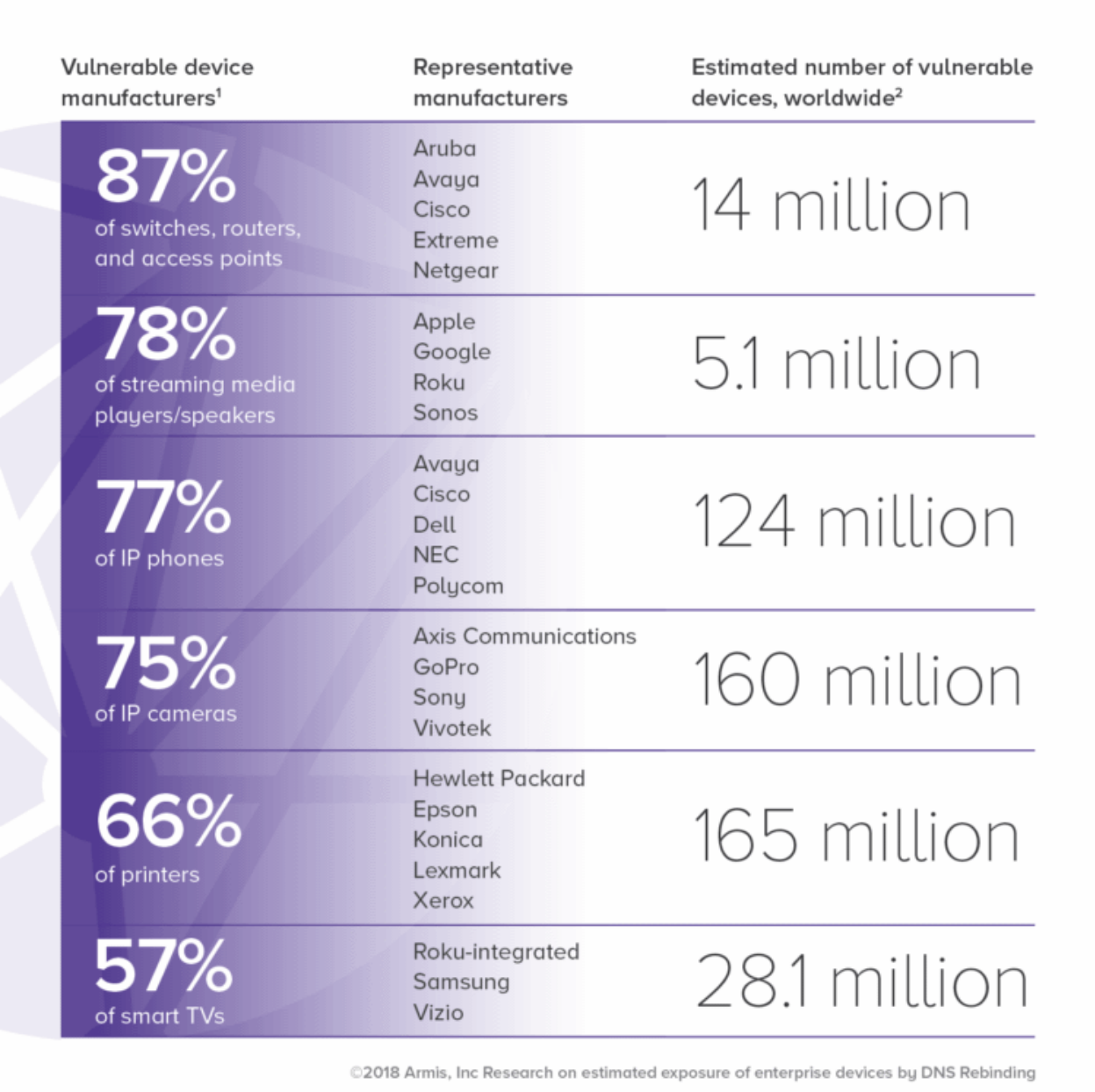
Almost all types of IoT devices are vulnerable

Armis says that IoT and other smart devices are perfect for attackers to target via DNS rebinding, mainly due to their proliferation inside enterprise networks, where they can play a key role into facilitating reconnaissance and data theft operations.

Experts say that following their investigation, they found out that nearly all types of smart devices are vulnerable to DNS rebinding, ranging from smart TVs to routers, from printers to surveillance cameras, and from IP phones to smart assistants.

All in all, experts put the number of vulnerable devices in the hundreds of millions, estimating it at roughly half a billion.

Vulnerable device manufacturers[1]	Representative manufacturers	Estimated number of vulnerable devices, worldwide[2]
87% of switches, routers, and access points	Aruba Avaya Cisco Extreme Netgear	14 million
78% of streaming media players/speakers	Apple Google Roku Sonos	5.1 million
77% of IP phones	Avaya Cisco Dell NEC Polycom	124 million
75% of IP cameras	Axis Communications GoPro Sony Vivotek	160 million
66% of printers	Hewlett Packard Epson Konica Lexmark Xerox	165 million
57% of smart TVs	Roku-integrated Samsung Vizio	28.1 million



Source: Armis

Don't expect a massive patching effort

Patching all these devices against DNS rebinding attacks is a colossal task that may never be done, requiring patches from vendors that can't be bothered with security for trivial flaws like XSS and CSRF vulnerabilities, let alone complex attacks such as DNS rebinding.

But Armis experts say that integrating IoT devices into current cyber-security monitoring products may be the easiest and cost-effective solution, rather than looking and auditing new devices to replace the old ones.

Because IoT security has been a proverbial shitshow for the past year, the cyber-security market has reacted and adapted, and there are now many firms that provide specialized platforms for monitoring IoT devices for enterprises which want to avoid nasty surprises.
For example, just recently PIR Bank of Russia got a nasty surprise when discovered that hackers stole $1 million after they breached its network thanks to an outdated router.
It's not the 2000s anymore, and any respectable company nowadays must update its threat model to account for IoT devices, regardless if their vulnerable to DNS rebinding or any other flaw.

Source: Bleeping Computer