telelink

Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

April 2019

Table of Contents:

Executive Summary

1. LockerGoga ransomware wreaks havoc in the US and Europe. Despite being inefficient in collecting money, it is good enough to slow down multinational companies and forces them to take immediate actions. Altran, Norsk Hydro, Hexion and Momentive are the victims who came forward and admitted that they have been hit. To learn more Jump to article.
2. It seems like every couple of months there is a new data breach and billions of unique user names and password are either offered for sale or published on the dark web. Unfortunately, the more data is being leaked, the more the opportunities for attackers grow. They are finding new, creative ways to improve the social-engineering aspects of their spear-phishing attacks. To learn more Jump to article.
3. "The number of Android users attacked by banking malware saw an alarming 300% increase in 2018, with 1.8 million of them being impacted by at least one such attack during the last year.". More than half of the detected attack are attributed to an Android malware, while the desktop malware has a new champion Zbot and Gozi. To learn more Jump to article.
4. The smart aftermarket car alarms are turning into a bigger risk, than a security. Pen testers have found that alarm systems developed by Pandora and Viper are susceptible to hacking and "simply by tampering with parameters, one can update the email address registered to the account without authentication, send a password reset to the modified address (i.e. the attacker's) and take over the account.". Moreover, the car alarm APIs also expose vast amounts of personally identifiable information. To learn more Jump to article.
5. "Cisco Systems is warning customers that a discovery tool for network devices can be accessed by a remote and unauthenticated attacker. The flaw could allow an adversary to log into the system and collect sensitive data tied to host operating systems and hardware." To learn more Jump to article.
6. "A new insidious malware bent on siphoning credit-card numbers from point-of-sale (PoS) systems has recently been spotted on a crimeware forum." The malware is relatively cheap, it can be bought on the Dark Web for$250 and it "is spread via email, purporting to be a game involving "various pictures of cats."". To learn more Jump to article.
7. "Google was fined €1.494.459.000 ($1.698.064.094) or 1.29% of Google's 2018 turnover for abusing its market dominance to block rival advertising companies from displaying search ads on publisher search results pages says a European Commission statement". To learn more Jump to article.
8. For years now Facebook has been storing between 200 and 600 million passwords in an unencrypted, readable plain text format on their servers. The company has that it found no wrong doing or security breach, but still "2,000 engineers or developers made around nine million internal queries for data elements containing plain text user passwords". To learn more Jump to article.

9. Operation ShadowHammer is in full speed and has "led to the backdoored version of ASUS Live Update being downloaded and installed by more than 57,000 Kaspersky users". To learn more Jump to article.
10. "Security incidents do not simply occur, they are caused — either by legitimate users who unintentionally expose company data or malicious actors who seek to breach enterprise systems undetected." The time to contain a breach matters is of the essence and there are 6 steps you can take to strengthen your incident response plan. To learn more Jump to article.

1. Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers'

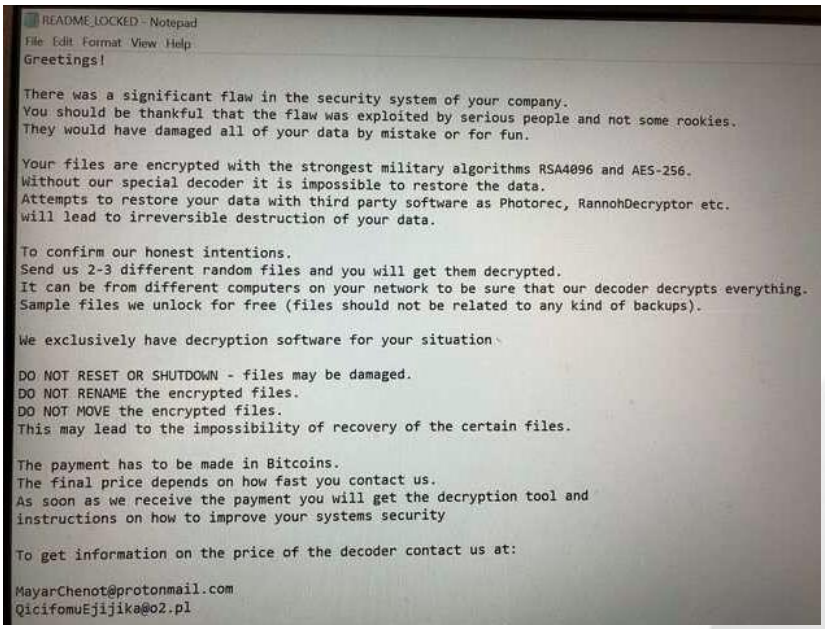
Hexion and Momentive, which make resins, silicones, and other materials, and are controlled by the same investment fund, were hit by the ransomware on March 12, according to a current employee. An internal email obtained by Motherboard and signed by Momentive's CEO Jack Boss refers to a "global IT outage" that required the companies to deploy "SWAT teams" to manage.

Based on the ransom message, the ransomware that hit Hexion and Momentive appears to be LockerGoga, the same ransomware that forced an aluminum manufacturing giant Norsk Hydro to shut down its worldwide network this week. Motherboard cross-referenced the ransom message associated with the Momentive attack to known LockerGoga attacks, and found that the language and formatting were identical.

On the day of the attack, some of the companies' Windows computers were hit with a blue screen error and their files encrypted, said the current employee, who asked to remain anonymous as they were not authorized to speak to the press.

"Everything [went down]. Still no network connection, email, nothing," they said in an online chat on Thursday.

Boss's email said that the data on any computers that were hit with the ransomware is probably lost, and that the company has ordered "hundreds of new computers."



Pic. 1: A screenshot of the ransom notice displayed on a Momentive laptop. Image: Motherboard

On Friday evening, Hexion announced in a press release that it was working to resume normal operations "in response to a recent network security incident."

Boss's email indicates that the ransomware first hit the company last week, and explains what the company is doing to recover. Among the measures taken, Boss wrote that the Momentive is giving some employees new email accounts because their old ones are still inaccessible. The company notes that it is using a new domain—momentiveco.com for new email addresses rather than momentive.com.

Motherboard sent an email to a known Momentive email address that uses the old domain, momentive.com, but it bounced back. The error message noted that "due to a network event," email services are currently unavailable.

The leaked email also notes that as more people who email the company receive the same error message that Motherboard saw, the more likely employees are to be contacted by third parties looking to more information. It then lists an email address and phone number that should be given to the media. Motherboard called this number and emailed this address but did not get a response.

On Friday, Motherboard called Hexion's main phone line. The employee who answered declined to provide any information about the attack. When asked whether there had been an incident, the employee said "no comment" and immediately hung up. Motherboard called back and spoke to someone else, who did not identify themselves but said that they could not provide any information to us.

News of this attack shows that the hackers behind the LockerGoga ransomware may be more active than previously thought.

Until today, there were only two known victims of LockerGoga, a relatively new type of malware that infects computers, encrypts their files and ask for a ransom. The first known victim was Altran, a French engineering consulting firm that was hit in late January. Then earlier this week, the Norwegian aluminum giant Norsk Hydro revealed that it had been hit by a ransomware attack. A Kaspersky Lab spokesperson said that they have knowledge of more victims around the world.

Hydro did not mention what malware hit it. But Norwegian media, citing local cybersecurity authorities, said it was LockerGoga. MalwareHunterTeam, a group of independent security researchers, found a sample of LockerGoga on the online malware repository VirusTotal that had been uploaded from Norway on the day Hydro was hit.

MalwareHunterTeam told Motherboard that the ransom notice shared by our source is very similar to the one found in LockerGoga attacks.

Joe Slowik, a security researcher at Dragos, a cybersecurity company that focuses on critical infrastructure and who has studied the malware, said that LockerGoga does not appear to be very good at its purported goal: collecting money from the victims. In fact, as the ransom note shows, and unlike other popular ransomware, victims have to email the hackers and negotiate a price to get files decrypted, making it harder for the criminals to scale their earnings.

"It's a piece of very inefficient ransomware," Slowik told Motherboard in a phone call.

It may be inefficient at collecting money, but it's apparently good enough to slow down multinational companies in both Europe and the United States.

Source: https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers

2. How the Dark Web Data Bazaar Fuels Enterprise Attacks

It seems every aspect of our lives is available to be found somewhere on the Internet. And the information available isn't simply embarrassing browsing histories but ranges from our medical histories to the logon credentials we use to access many of our online services. This is certainly a privacy concern, but it's also increasingly an enterprise cybersecurity hazard. The more information adversaries have about us, the more effectively they can target their attacks.

Consider the news that broke earlier this year regarding 2.2 billion unique usernames and passwords that came to light. These usernames and passwords emerged from the dark web and are being shared more openly throughout online hacker groups. As Wired's Andy Green accurately put it, the credential troves threw "out the private data of a significant fraction of humanity like last year's phone book."

We can be confident that all of these emails and passwords have already been used to a great extent – both en masse against websites to try to break into online accounts and as part of spear-phishing attacks. Many accounts were probably accessed – users do tend to reuse so many passwords and usernames. Also, by industry estimates, phishing attacks are how the vast majority of cyberattacks are initiated.

It's good news that there's no new immediate risk from these massive credential dumps – except to those who haven't checked or changed their passwords – but plenty remains to be concerned about. It's a near certainty that these emails will be used for targeted attacks. And the dangerous fact remains that attackers can learn just about anything they want about anyone they want online. And now with everyone's email essentially a matter of public record, we will likely see a lot more spear phishing in the year ahead.

Social engineers find new data, tools to attack

Unfortunately, attackers will use the vast amount of information at their disposal to improve the social-engineering aspects of their spear-phishing attacks, making them even more creative and effective.

Consider how photographs are increasingly becoming weaponized. Attackers are using manipulated photos to attempt to steal bitcoin from cryptocurrency exchanges. Researchers

are getting better at fooling facial recognition, whether by using a number of photos to create a photograph that can defeat the device or by using photos to create a mask that is the likeness of their target to fool smartphone facial recognition.

Now consider deep fake videos. Not too long ago, these videos were very kludgy – so kludgy one could be spotted nearly instantly. But they are no longer so obviously fakes. Given the right skills, software and quantity of video and audio material to work with, the end result can be very good. When one considers the average pace of technological improvement, we can only imagine how difficult it will be to detect deep fakes in a year or two. It'll become relatively trivial to fake video statements from employees, executives, the CEO – virtually anyone. Think of the potential attacks on people that could consist of believable photographs and video, along with convincing faked and forged documents. The truth may prevail (eventually), but what about immediate impact on stocks, or reputations tarnished or destroyed by the initial, fake information that was disseminated? Attacks like this won't just affect politics; they will also hit business and community leaders.

When considering the vast amount of data that we know has been breached, it's reasonable to expect that such attacks, along with traditional phishing and spear-phishing attacks, will continue to become more effective. According to the Privacy Rights Clearing House, which has tracked data breaches since 2005, there have been 9,071 data breaches that have collectively exposed 11.5 billion records since they began tracking. That's financial records, health records, government and criminal records, educational records and more. In fact, there's so much data available on the dark web that it's possible for reasonably motivated and funded adversaries to build accurate models of our interests and how we interact with the world. That kind of data is certainly helpful in any social engineering attack.

Bracing for the inevitable

The thing is, so much data about us is available that it is bound to be used as part of phishing, spear-phishing and other targeted attacks. Increasingly, attackers are going to be able to leverage highly accurate and personal information to trick employees, contractors and even executives into clicking on a file or link that places their organization at risk. That's why enterprises need to be prepared with powerful incident response and investigation technologies as well as employee awareness training.

Phishing and social engineering attacks are no longer just about adversaries having an email address and searching LinkedIn for a current position and work history. They are increasingly about uncovering all of the information about us that has made its way to the dark web and the broader internet. And when one considers all of the information about nearly everyone that is so widely available, it really is just a matter of imagination when it comes to how adversaries can and will use this data to socially engineer and attack enterprises and their staff.

What does this mean for enterprise security and the ability to defend against spear phishing? Straightforward, specific advice would help enterprises better protect themselves against these types of emerging attack techniques, but that information is not yet available.

The best advice for now is to make sure good security practices are in place and everyone within the organization – from PR and crisis communication teams, to legal and HR, to security and incident response – who could be called upon by way of such attacks is made aware of the growing possibility.

Of course, good security practices include having the right security defenses in place – from security awareness, antimalware through good backup and recovery through incident-response capabilities. If we've learned one thing from the past that will certainly inform the future, it's that despite all of the best efforts from IT and security teams, some of these attacks will succeed, and adversaries are going to come at enterprises with these new tools and data sets. You have to be ready for it.

Source: *https://threatpost.com/dark-web-enterprise-security/142399/*

3. 1.8 Million Users Attacked by Android Banking Malware, 300% Increase Since 2017

The number of Android users attacked by banking malware saw an alarming 300% increase in 2018, with 1.8 million of them being impacted by at least one such attack during the last year.

While in 2016 the overall number of attacked users was of 786,325 and during 2017 it dropped to 515,816, in April 2018 the number of attacks went on a severely increasing trend.

The growth in the number of incidents reached the highest values during June and September, the year ending with an astounding 1,799,891 of users having been hit by at least one Android banking malware family.

Out of the total number of Android users affected by financial malware, the highest percentage was found in Russia, South Africa, and the United States, while 85% of the attacks were conducted by bad actors using only three banking malware families.

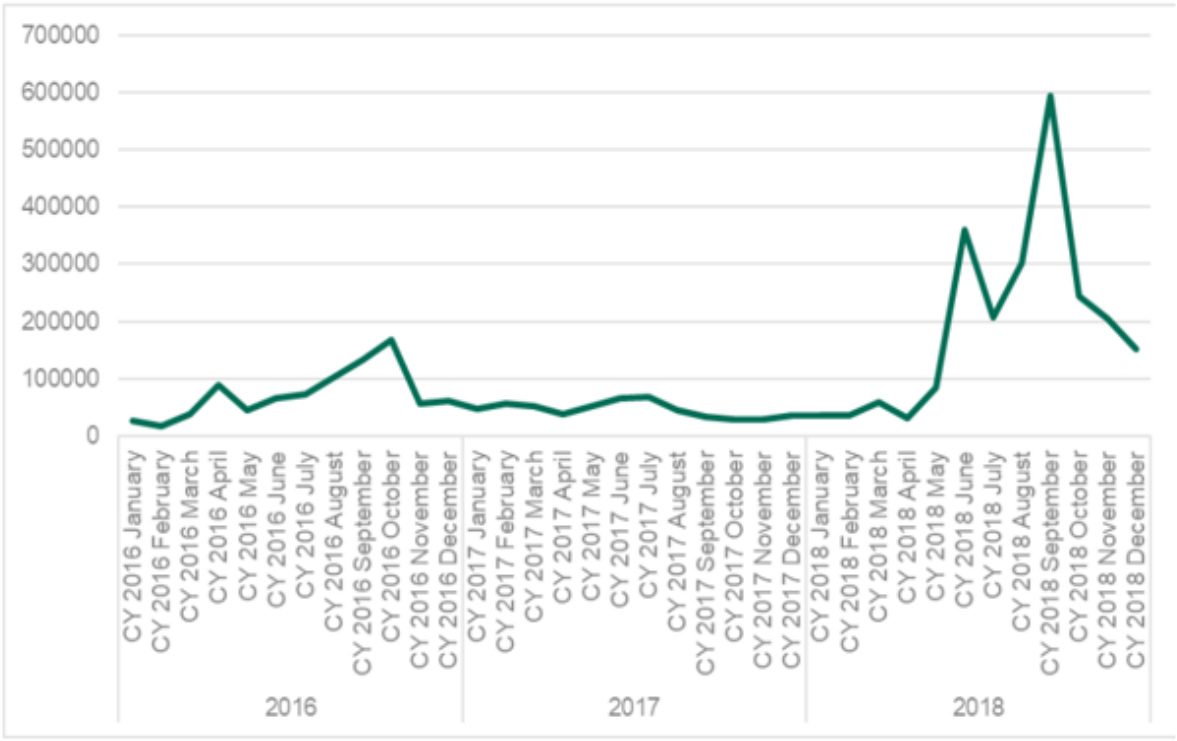


Fig.2: the change in the numbers of users attacked with Android banking malware 2016-2018(Fig. 19 in the original article)

According to Kaspersky Lab's "Financial Cyberthreats in 2018" report, "Asacub peaked more than twice to almost 60%, followed by Agent(14.28%) and Svpeng (13.31%). All three of them experienced explosive growth in 2018, especially Asacub as it peaked from 146,532 attacked users in 2017 to 1,125,258.

While Asacub was also the top dog in the Android banking malware rankings in 2017, during 2018 this Android malware family was behind 58% of all detected attacks, more than doubling its "market share."

The second and third places were taken by Agent and Svpeng with 14% and 13% of the total number of attacks, pushing down the Faketoken and Hqwar families to the middle of the top most dangerous Android malware during 2018.

This was an interesting evolution especially since Svpeng was almost out of the picture until May 2018, when it started landing on Android devices around the world, eventually being detected on around 100,000 of them during June.

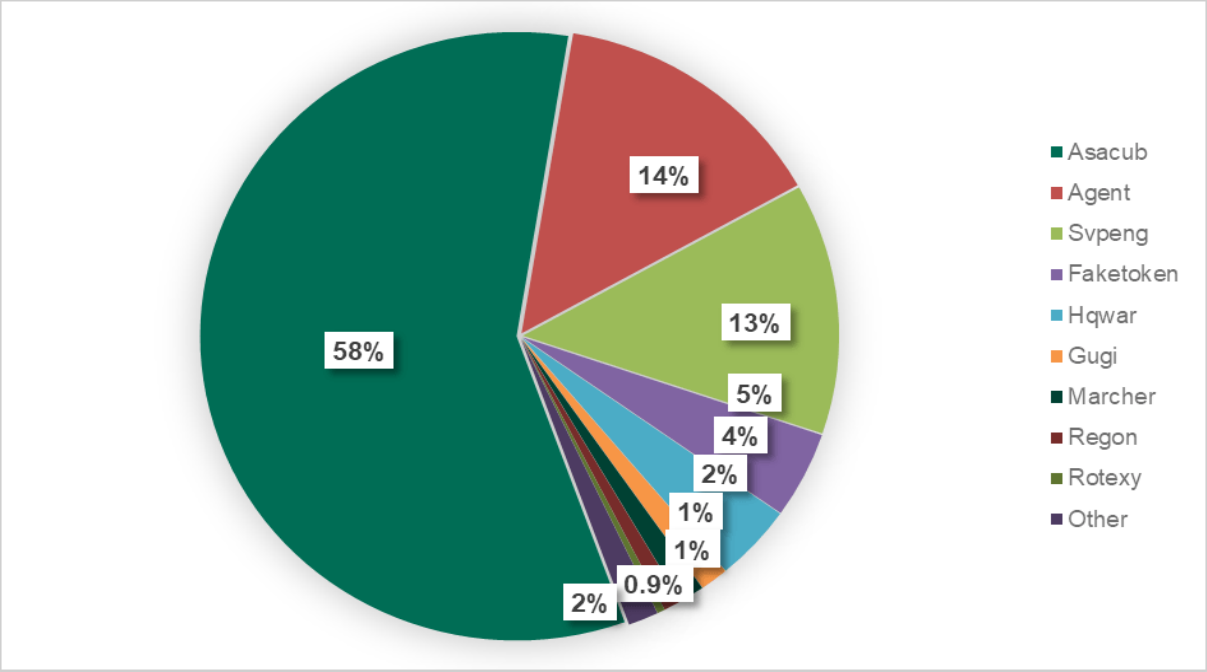


Fig. 3: Android banking malware in 2018

Banking malware on Windows desktops

As detailed in Kaspersky Lab's report, Windows users were also targeted by banking Trojans, with this malware strain being behind 889,452 incidents, "an increase of 15.9% in comparison with 767,072" during 2017.

Approximately 24% of them were also from corporate environments, which translates into an apparent upward trend from the 19% share of 2017.

Also, "Zbot and Gozi are still the kings when comes to most widespread banking malware family (over 26% and 20% of attacked users), followed by SpyEye (15.6%)," says Kaspersky.

Despite this, on the whole, the two malware families at the top saw a decrease in the number of detections, while families that placed in the middle of the rankings -- SpyEye, RTM, Emotet, Caphaw -- solidified their positions since 2017.

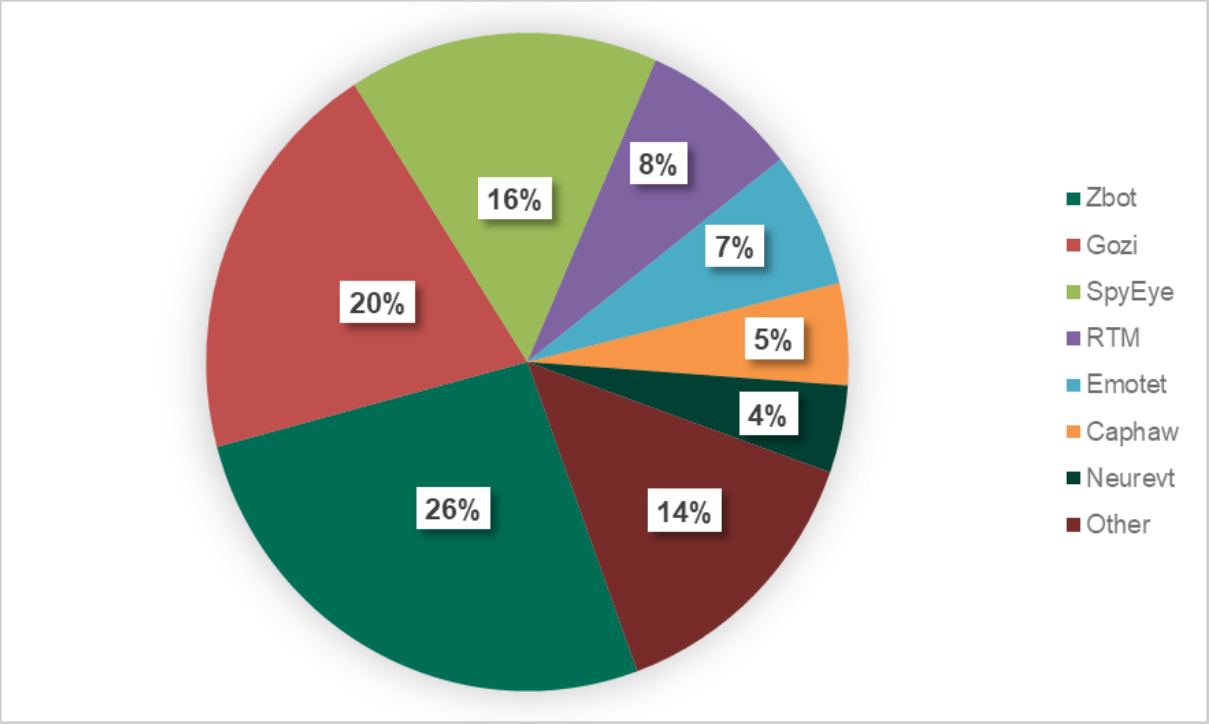


Fig. 4: Financial threats targeting desktop users

Malicious mobile software attacks doubled during 2018

A previous report on the mobile malware evolution during for 2018, also signed by Kaspersky Lab, saw that mobile users were targeted by almost twice as many attacks using malicious software during the previous year, going up from 66.4 million in 2017 to 116.5 million until the end of 2018.

However, in spite of this astonishing increase, only 5,321,142 installation packages with malware samples were identified on all mobile platforms, down 409,774 when compared to the stats collected during 2017.

Even more, while cybercriminals who chose to target mobile users were seen using tried-and-tested methods such as SMS spam, some of them were also willing to try attack methods like DNS hijacking, previously reserved for attacking desktop platforms.

Source: https://www.bleepingcomputer.com/news/security/18-million-users-attacked-by-android-banking-malware-300-percent-increase-since-2017/

4. Smart Car Alarms Ironically Expose Millions of Vehicles to Remote Hijacking

Aftermarket car alarm systems developed by Pandora and Viper have been found to be vulnerable to remote exploitation, enabling potential attackers to hijack the vehicles they're installed on and to spy on their owners.

The exploitable software flaws were found in the smartphone apps used to control the alarm systems developed by Pandora and Viper (known as Clifford in the UK), two of the most popular smart car alarms worldwide.

Just taking into account the claims made by Viper on the website of the SmartStart alarm system designed to help customers "Start, Control, and Locate" their cars from "virtually anywhere," the smartphone application has already been downloaded over 3,000,000 times.

Locate and hijack cars with the push of a button

The Pen Test Partners researchers who unearthed these flaws say that "the vulnerabilities are relatively straightforward insecure direct object references (IDORs) in the API," and "simply by tampering with parameters, one can update the email address registered to the account without authentication, send a password reset to the modified address (i.e. the attacker's) and take over the account."

As discovered by Pen Test Partners' research team, the aftermarket smart alarm systems would allow would-be attackers to exploit security flaws which enable:

- The car to be geo-located in real time
- The car type and owner's details to be identified
- The alarm to be disabled
- The car to be unlocked
- The immobiliser to be enabled and disabled
- In some cases, the car engine could be 'killed' whilst it was driving
- One alarm brand allowed drivers to be 'snooped' on through a microphone
- Depending on the alarm, it may also be possible to steal vehicles

The researchers also said that some of the smart alarms they tested also gave them the ability to listen to all conversations using a microphone installed as part of the alarm system, allowing criminals to also snoop on millions of car owners who installed them on their cars.

To make matters even worse, the flaws observed in the car alarm APIs exposed huge amounts of personally identifiable information.

Additionally, "It should also be noted that you don't need to buy either two of these products to have an account on the system. Both products allow anyone to create a test/demo account. With that demo account it's possible to access any genuine account and retrieve their details," said the researchers.

While Pen Test Partners gave the two companies behind the vulnerable smart car alarm systems only 7 days to fix the security issues because of the high chance that criminals already were aware and possibly exploiting them in the wild, both Pandora and Viper responded and patched them very quickly, a lot faster than the researchers expected.

Pandora's UK representative responded in about 48 hours and had their Moscow-based HQ take action quickly. The IDOR was fixed overnight and we confirmed that the following morning.

Viper responded faster, but took a little longer to fix the vulnerability. That one is also confirmed as fixed.

The Pen Test Partners security researchers also gave a 'conservative' estimate of the number of cars possibly affected by the issues they found, stating that "the manufacturers had inadvertently exposed around 3 million cars to theft and their users to hijack" and "$150 Billion worth of vehicles were exposed."

Automotive software and apps vulnerable to hacking

This is not the first time and it will most definitely not be the last when cars have been hacked using vulnerabilities identified in both built-in software added by their manufacturers or in various apps used to control them with the help of their owners' smartphones.

Tesla's electric cars, for instance, were found to be vulnerable during 2016, with car thieves being able to hack and steal a Tesla by infecting the owner's Android smartphone with a malware strain and using that to control the Tesla Android App and, subsequently, their car.

During April 2018, a Dutch cyber-security company discovered that multiple in-vehicle infotainment (IVI) systems used by some Volkswagen Group cars were exposed to remote hacking.

In May, BMW announced that they've started working on a number of firmware updates designed to patch 14 security issues found in BMW i Series, BMW X Series, BMW 3 Series, BMW 5 Series, and BMW 7 Series cars by researchers from the Tencent Keen Security Lab.

The same researchers were also able to identify several vulnerabilities in Tesla Model X cars which would have allowed attackers to remotely control vehicles, forcing the car to brake while in motion or controlling its lights, in-vehicle displays, and open its doors and trunk when stationary.

During October 2017, an electronics designer uncovered a security flaw in the key fob system of several Subaru models, an issue that could likely be abused to hijack customers' cars and that the automaker refused to patch when contacted.

BMW, Nissan, Ford, and Infiniti were impacted by two buffer overflows—CVE-2017-9647 and CVE-2017-9633—in the TCU (telematics control unit) components (2G modems) during the summer of 2017, the TCUs which used S-Gold 2 (PMB 8876) cellular baseband chipsets.

Mazda cars have also been found to be vulnerable, with the Mazda MZD Connect infotainment system being easily hackable by plugging in a USB flash drive into the car's dashboard.

That "feature" was successfully used by Mazda car owners to alter their vehicles' infotainment systems -- installing new apps and tweaking settings.

To put everything into perspective, as detailed in a study conducted by Ponemon Institute -- when it comes to testing software vulnerabilities -- around 63% percent of all automotive companies will test less than half of the software, hardware, and other technologies they develop.

Source: https://www.bleepingcomputer.com/news/security/smart-car-alarms-ironically-expose-millions-of-vehicles-to-remote-hijacking/

5. Cisco Patches Critical 'Default Password' Bug

Cisco Systems is warning customers that a discovery tool for network devices can be accessed by a remote and unauthenticated attacker. The flaw could allow an adversary to log into the system and collect sensitive data tied to host operating systems and hardware.

The disclosure is part of a Cisco Security Advisory and patch (CVE-2019-1723) issued Wednesday. The vulnerability is rated critical, with a CVSS rating of 9.8.

Affected is the Cisco Common Service Platform Collector (CSPC), a tool used for discovering and collecting information from the Cisco devices installed on a network. The flaw includes a default, static password that can be accessed remotely by an unauthenticated adversary. Cisco stresses, that access to CSPC does not grant administrator privileges to an attacker.

"The vulnerability exists because the affected software has a user account with a default, static password," Cisco wrote. "An attacker could exploit this vulnerability by remotely connecting to the affected system using this account. A successful exploit could allow the attacker to log in to the CSPC using the default account."

The CSPC tool is used extensively by Cisco service offerings such as Smart Net Total Care (SmartNet), Partner Support Service (PSS) and Business Critical Services. Data gathered by CSPC includes inventory reports, product alerts, configuration best practices, technical service coverage and lifecycle information for both the hardware and operating system software.

Vulnerable are Cisco CSPC releases 2.7.2 through 2.7.4.5 and all releases of 2.8.x prior to 2.8.1.2. Cisco said it is unaware of a public exploit of the vulnerability.

Two Additional Bugs Rated High

On Wednesday, Cisco also alerted customers to two high-rated vulnerabilities. One is related to the Cisco Email Security Appliances (CVE-2018-15460) and the other (CVE-2018-0389) Cisco Small Business SPA514G IP Phones.

With the Cisco Email Security Appliances, the security advisory warns that the vulnerability is tied to the devices' implementation of Session Initiation Protocol processing. The vulnerability allows "remote attacker to cause an affected device to become unresponsive, resulting in a denial of service condition," Cisco wrote.

Cisco said it will not patch or issue a workaround for the email appliance. It explained that the SPA514G IP Phones have reached end-of-life and therefore will not receive an update. It also stressed that similar IP-based phone (SPA51x, SPA51x and SPA52x) are not affected.

Cisco AsyncOS Software for ESA Major Release	First Fixed Release for This Vulnerability
Prior to 9.0	Affected; Migrate to 11.0.2-044 MD
9.x	Affected; Migrate to 11.0.2-044 MD
10.x	Affected; Migrate to 11.0.2-044 MD
11.0.x	11.0.2-044 MD[1]
11.1.x	11.1.2-023 MD[2]
12.x	Not affected

The second bug, found in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances, leaves impacted systems open to denial of service attacks.

"[The flaw] could allow an unauthenticated, remote attacker to cause the CPU utilization to increase to 100 percent, causing a denial of service (DoS) condition on an affected device," Cisco wrote.

Cisco said the vulnerability is "due to improper filtering of email messages that contain references to whitelisted URLs." It said an attacker could exploit the flaw by sending a malicious email message that contains a large number of whitelisted URLs. "A successful exploit could allow the attacker to cause a sustained DoS condition that could force the affected device to stop scanning and forwarding email messages," it wrote.

Cisco has released a software update and workaround instructions for impacted instances of Cisco AsyncOS Software for Cisco Email Security Appliances.

Source: https://threatpost.com/cisco-patches-critical-default-password-bug/142814/

6. GlitchPOS Malware Appears to Steal Credit-Card Numbers

A new insidious malware bent on siphoning credit-card numbers from point-of-sale (PoS) systems has recently been spotted on a crimeware forum.

Researchers at Cisco Talos said in a Wednesday analysis that they discovered the malware, dubbed "GlitchPOS," being peddled on the Dark Web for $250. The malware first appeared on Feb. 2, and researchers said they don't know yet how many cybercriminals bought it or are using it.

"Cisco Talos recently discovered a new PoS malware that the attackers are selling on a crimeware forum," said researchers in the post. "Our researchers also discovered the associated payloads with the malware, its infrastructure and control panel."

GlitchPOS joins other recently developed malware targeting the retail and hospitality space, including TreasureHunter and PinkKite – a trend that's rising given that cybercriminals look to profit from PoS systems that often represent a "soft target," researchers said.

Malware Details

Craig Williams, director of Cisco Talos Outreach, told Threatpost that GlitchPOS stands out in part because "the software is well designed to be easy to use, which allows non-technical bad guys to run PoS botnets."

The malware is spread via email, purporting to be a game involving "various pictures of cats."

A packer developed in VisualBasic protects the malware, researchers said: "The purpose of the packer is to decode a library that's the real payload, encoded with the UPX packer," researchers said. "Once decoded, we gain access to GlitchPOS, a memory grabber developed in VisualBasic."

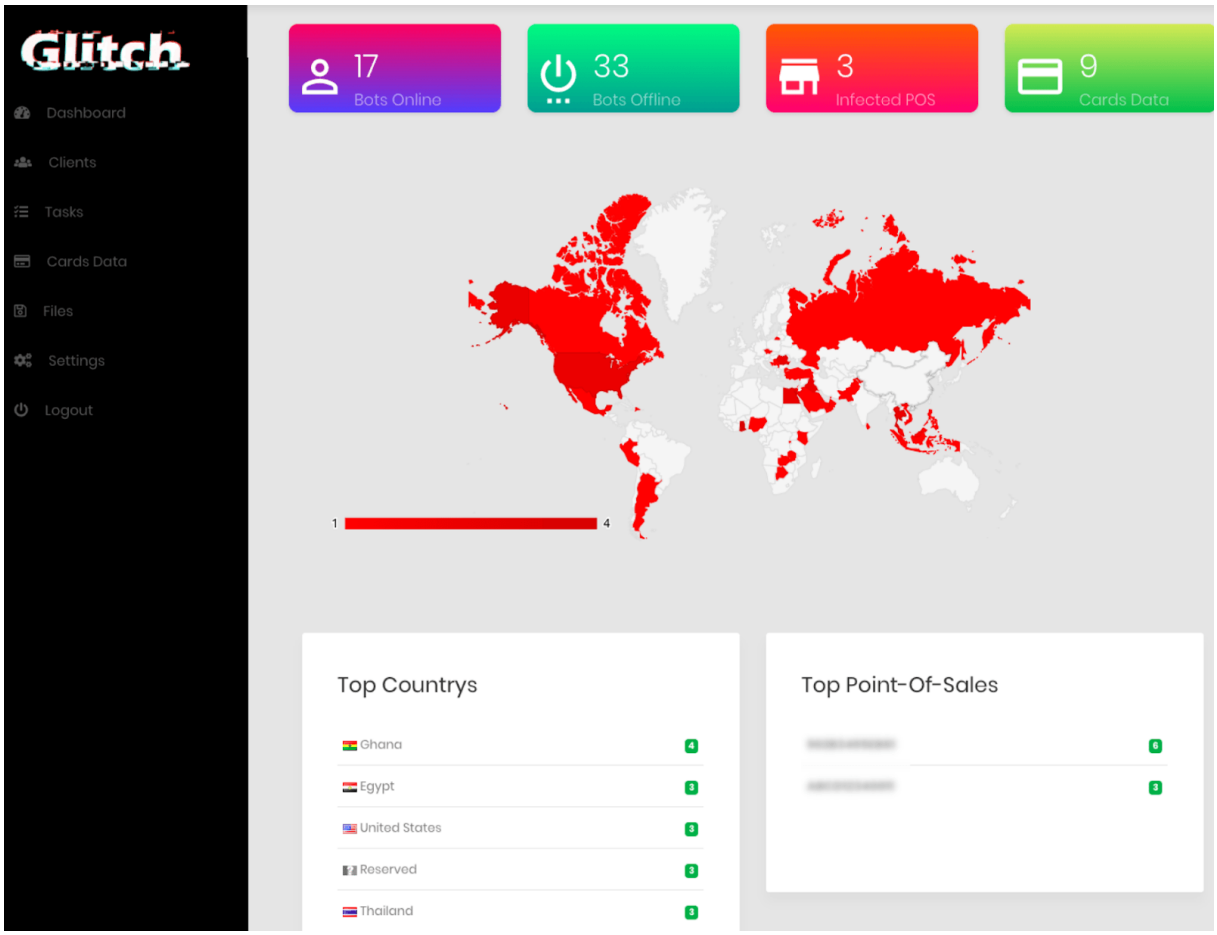


Fig. 5: GlitchPOS dashboard

The malware's payload is small and has few functions after connecting to a command-and-control server (C2), including registering the infected systems, receiving tasks from the C2 (executed via a shellcode sent directly by the server) and exfiltrating credit-card numbers from the memory of the infected systems.

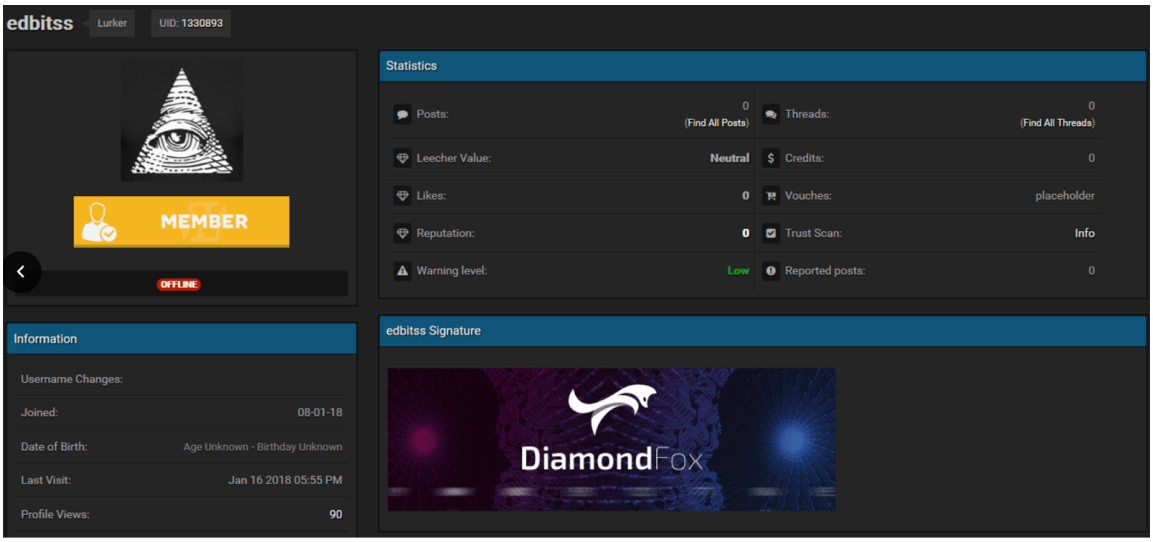
The GlitchPOS panel also includes other features provided by the seller to sweeten the malware package, including a dashboard, a "clients" list of the infected systems and a panel listing out the stolen credit-card numbers.

The pre-built malware sells for $250, while the builder goes for $600.

Seller: Not His First Malware

Researchers suspect that the seller behind GlitchPOS – who goes by the name "Edbitss" – has developed malware before.

Researchers assessed "with high confidence" that Edbitss is also the developer of the DiamondFox L!NK botnet. That modular botnet, which has been offered for sale on various underground forums since 2015/2016, gives cybercriminals the tools to launch a wide variety of attacks – from tailored espionage campaigns to credential theft campaigns and even simple DDoS attacks.



Researchers found several similarities between the DiamondFox L!NK botnet and GlitchPOS that led them to believe that the same developer is behind both.

For instance, the malware language for both is similar, and their panels contain similar images, codes, terminologies and colors. "The author clearly reused code from DiamondFox panel on the GlitchPOS panel," said the researchers.

In another interesting twist that speaks to the popularity of PoS malware, researchers found other cybercriminals attempting to resell GlitchPOS on alternative websites at a higher price than the original.

"We also see that bad guys steal the work of each other and try to sell malware developed by other developers at a higher price," said researchers.

POS Malware Rising In Popularity

Point-of-sale malware is becoming a rising scourge; particularly in the hospitality industry.

In January 2018, fashion retailer Forever 21 revealed that malware had sat on certain POS terminals for almost eight months in its stores, allowing hackers steal consumer credit card data from the company, and in March 2018, malware was discovered on PoS systems at more than 160 Applebee's restaurants.

More recently, North Country Business Products (NCBP), a company that provides PoS systems and services for restaurant locations said that malware was able to scrape payment-card data from diners for about three weeks in January. NCBP's reach is long, with partner restaurants running the gamut from Collins' Irish Pub in Flagstaff, Ariz. To Vinyl Taco in Grand Forks, N.D.

PoS malware is typically deployed on retailers' websites or on retail PoS sale machines.

"If they successfully obtain credit-card details, they can use either the proceeds from the sale of that information or use the credit-card data directly to obtain additional exploits and

resources for other malware," researchers said. "Point-of-sale terminals are often forgotten about in terms of segregation and can represent a soft target for attackers."

Source: https://threatpost.com/glitchpos-malware-credit-card/142804/

7. Google Fined $1.7 Billion for Anti-Competitive Practices in Online Advertising

Google was fined €1.494.459.000 ($1.698.064.094) or 1.29% of Google's 2018 turnover for abusing its market dominance to block rival advertising companies from displaying search ads on publisher search results pages says a European Commission statement published today.

As explained by the European Commission, Google added so-called "exclusivity clauses" in contracts during 2006, prohibiting publishers from displaying competitors' search adverts within search results, forcing them to only display Google search ads delivered through the AdSense for Search online search advertising intermediation platform.

Three years later, starting with March 2009, the search giant replaced "exclusivity clauses with so-called 'Premium Placement' clauses" which would "to reserve the most profitable space on their search results pages for Google's adverts and request a minimum number of Google adverts."

This way, Google blocked competitors from placing their adverts on the most clicked and visible parts of publishers' websites, effectively removing them from visitors' view.

Also during March 2009, Google added new clauses to contracts requiring publishers to ask for "written approval from Google before making changes to the way in which any rival adverts were displayed," allowing the Alphabet unit to "control how attractive, and therefore clicked on, competing search adverts could be."

To summarize the European Commission's findings, using contract clauses introduced in publisher contracts over time, Google removed rivals' search ads from search results pages, reserved the best ad spots for its own search adverts, and controlled how their rivals' search ads looked when they were eventually displayed.

As detailed within the Commission's press release:

Based on a broad range of evidence, the Commission found that Google's conduct harmed competition and consumers, and stifled innovation. Google's rivals were unable to grow and offer alternative online search advertising intermediation services to those of Google. As a result, owners of websites had limited options for monetizing space on these websites and were forced to rely almost solely on Google.

This is not the first time the European Commission fined Google for abusing its market dominance. In June 2017, EU's competition watchdog imposed a record €4.34 billion ($5.04 billion) fine on Google for "for illegal practices regarding Android mobile devices to strengthen the dominance of Google's search engine."

Also, during July 2018, Google received a €2.42 billion ($2.72 billion) penalty for preventing competitors' from competing in the online search comparison shopping market by abusing its search engine dominance.

According to the Commission, Google had "a market share above 70% from 2006 to 2016" in online search advertising intermediation within the European Economic Area (EEA), while in 2016 the search giant "also held market shares generally above 90% in the national markets for general search and above 75% in most of the national markets for online search advertising."

Competition Policy Commissioner Margrethe Vestager said that:

Google has cemented its dominance in online search adverts and shielded itself from competitive pressure by imposing anti-competitive contractual restrictions on third-party websites. This is illegal under EU antitrust rules. The misconduct lasted over 10 years and denied other companies the possibility to compete on the merits and to innovate - and consumers the benefits of competition.

The Commissioner also published a more detailed statement regarding the Commission's decision to fine Google €1.49 billion for breaking the EU antitrust rules by abusing its market dominance.

Source: https://www.bleepingcomputer.com/news/security/google-fined-17-billion-for-anti-competitive-practices-in-online-advertising/

8. Facebook Stored Passwords in Plain Text For Years

Hundreds of millions of Facebook user passwords have been stored in plain text for years, the social media giant acknowledged on Thursday.

KrebsOnSecurity, which first reported the news, said that specifically between 200 and 600 million passwords were stored in plain text as early as 2012, and were searchable by thousands of Facebook employees. Plain text means that the stored passwords are unencrypted, meaning they can be easily accessed and read by people who had access to Facebook's internal data storage systems.

"As part of a routine security review in January, we found that some user passwords were being stored in a readable format within our internal data storage systems," said Pedro Canahuati, vice president of engineering, security and privacy at Facebook in a Thursday post. "This caught our attention because our login systems are designed to mask passwords using techniques that make them unreadable. We have fixed these issues and as a precaution we will be notifying everyone whose passwords we have found were stored in this way."

Facebook said it will notify hundreds of millions of Facebook Lite users (Facebook Lite is a version of Facebook predominantly used by people in regions with limited connectivity), as well as tens of millions of other Facebook users, and tens of thousands of Instagram users.

Canahuati said that the passwords were never visible to anyone outside of Facebook and that Facebook has found no evidence to date that anyone internally abused or improperly accessed them.

Despite that, Krebs reported that 2,000 engineers or developers made around nine million internal queries for data elements containing plain text user passwords.

"No matter how large is a company, how many CISOs it has, there is always this temptation among developers to make their life easier by simplifying basic security rules," Bob Diachenko, cyber threat intelligence director at Security Discovery consultancy, told Threatpost. "It is only a question of time when improperly stored passwords or data become visible to the public internet and search engines index them. It can be anything – firewall down, electricity outage, software update – and a perimeter which you considered as internal goes public."

Security researcher Troy Hunt told Threatpost that the Facebook faux pas seems similar to a Twitter glitch had last year, where they inadvertently logged passwords in the clear. Twitter said that the glitch caused account passwords to be stored in plain text on an internal log, sending users across the platform scrambling to change their passwords.

"It's certainly undesirable, but without evidence of the captured passwords being exposed the risk is pretty minimal," he told Threatpost. "This feels like a disclosure out of an abundance of caution rather than a disclosure due to a serious risk. For consumers, using Facebook's 2-step verification process goes a long way to mitigating this risk."

The exposure of account passwords is not only a threat to the information stored in those accounts, but any private information stored in a Facebook-enabled application, Greg Pollock, vice president of product at BreachSight, told Threatpost.

"Password reuse attacks are also a consideration in any incident like this, anyone who uses their Facebook password for other systems should change it there as well," he said. "Through our research we've often found that massive collections of log files are frequently exposed via public Elasticsearch instances. Logs need to be considered as carefully as the database itself."

Canahuati also stressed that Facebook has been looking at the ways it stores certain other categories of information, such as access tokens, and has "fixed problems as we've discovered them."

Between the Cambridge Analytica incident that occurred about a year ago, to several other Facebook security problems over the past year (such as sketchy data sharing partnerships and other privacy violations), Facebook continues to be criticized for data privacy issues.

Source: https://threatpost.com/facebook-stored-passwords-in-plain-text-for-years/143032/

9. ASUS Live Update Infected with Backdoor in Supply Chain Attack

A new advanced persistent threat (APT) campaign detected by Kaspersky Lab in January 2019 and estimated to have run between June and November 2018 has allegedly impacted over one million users who have downloaded the ASUS Live Update Utility on their computers.

Kaspersky Lab's Global Research and Analysis (GReAT) team named this malicious campaign Operation ShadowHammer and, as initially reported by Kim Zetter, it is supposed to have led to the backdoored version of ASUS Live Update being downloaded and installed by more than 57,000 Kaspersky users.

While Kaspersky has only been able to count the total numbers of users infected by the trojanized ASUS Live Update who were also running one of the company's security solutions, their research team estimates a much larger number of impacted users with a total count of over one million compromised machines.

"ASUS Live Update is an utility that is pre-installed on most ASUS computers and is used to automatically update certain components such as BIOS, UEFI, drivers and applications," says GReAT in the report.

Also, "According to Gartner, ASUS is the world's 5th-largest PC vendor by 2017 unit sales. This makes it an extremely attractive target for APT groups that might want to take advantage of their userbase."

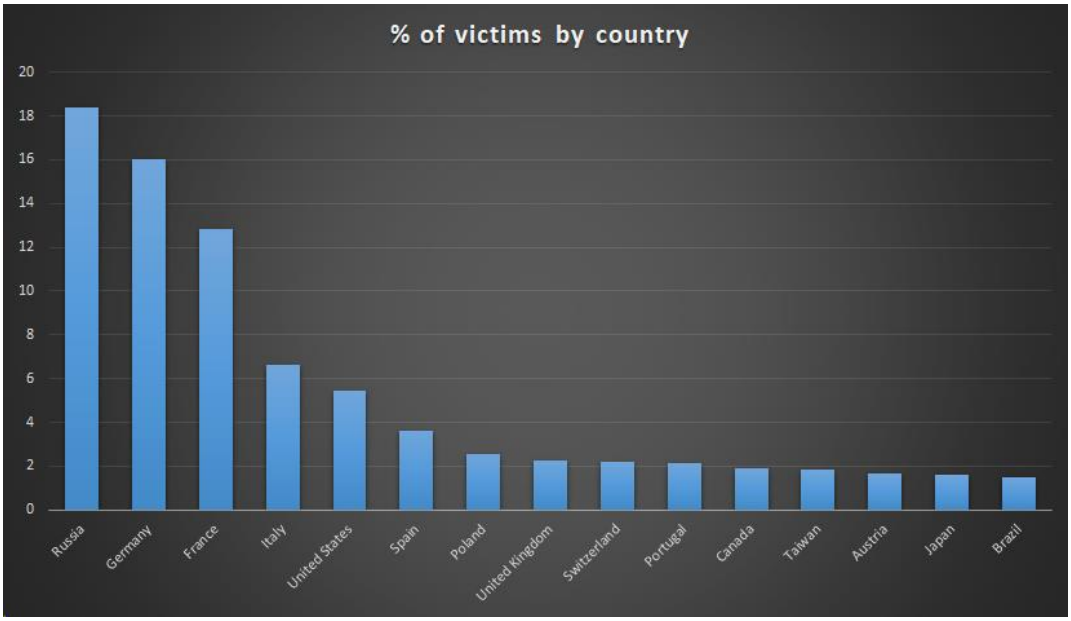


Fig. 6:ShadowHammer victim distribution

As explained by GReAT, there were multiple versions of infected ASUS Live Update binaries distributed with every one of them targeting "unknown pool of users, which were identified by their network adapters' MAC addresses."

The attackers behind Operation ShadowHammer used the hardcoded list of MAC addresses to detect if their backdoors landed on one of the machines using the MAC addresses on their hit list, Kaspersky successfully being able to collect 600 MACs from more than 200 samples used in this attack.

"If the MAC address matched one of the entries, the malware downloaded the next stage of malicious code. Otherwise, the infiltrated updater did not show any network activity," found the researchers.

The second stage backdoor would be downloaded from a command-and-control server located at asushotfix[.]com, a server which was eventually shut down during November, way before the operation was detected by Kaspersky and, thus, making it impossible to obtain a malware sample.

Kaspersky's researchers also discovered that the trojanized ASUS Live Update setup installers were also digitally signed using legitimate "ASUSTeK Computer Inc." certificates that were "hosted on the official liveupdate01s.asus[.]com and liveupdate01.asus[.]com ASUS update servers."

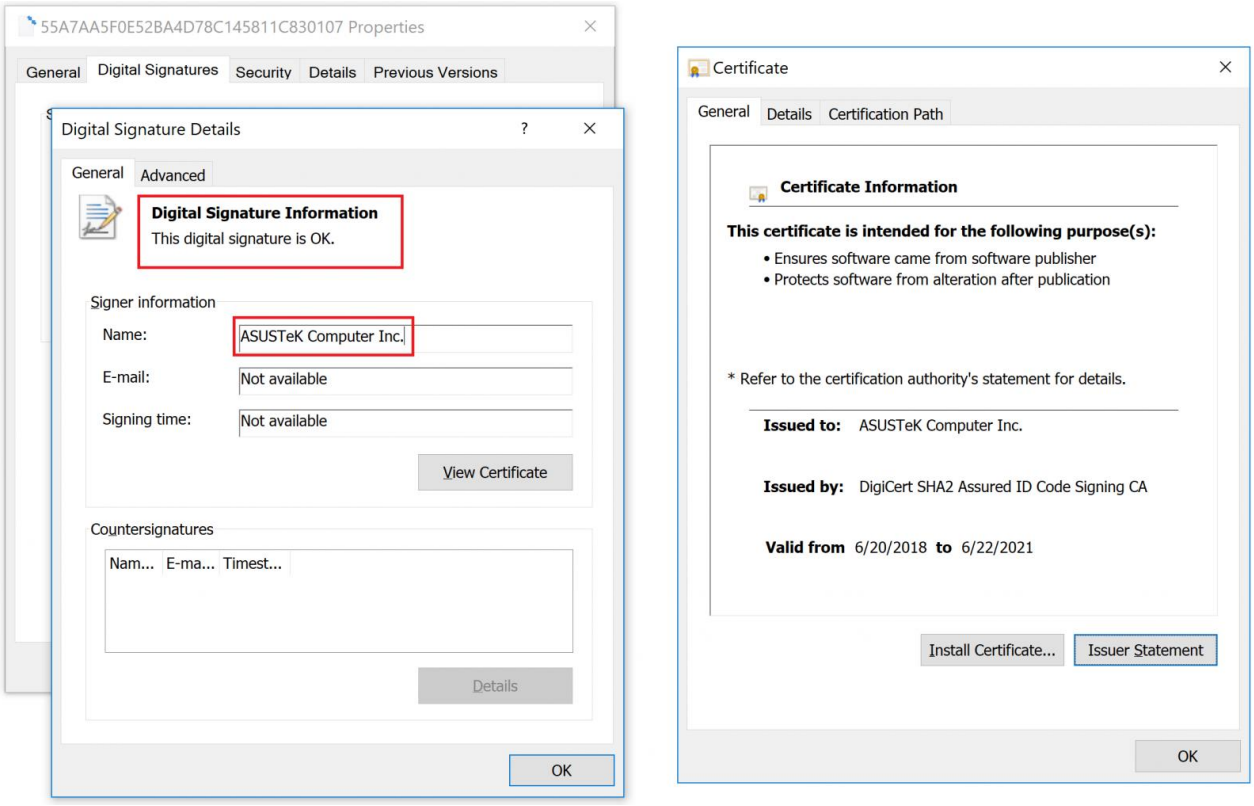


Fig.7: Signed backdoor ASUS Live Update setup installer

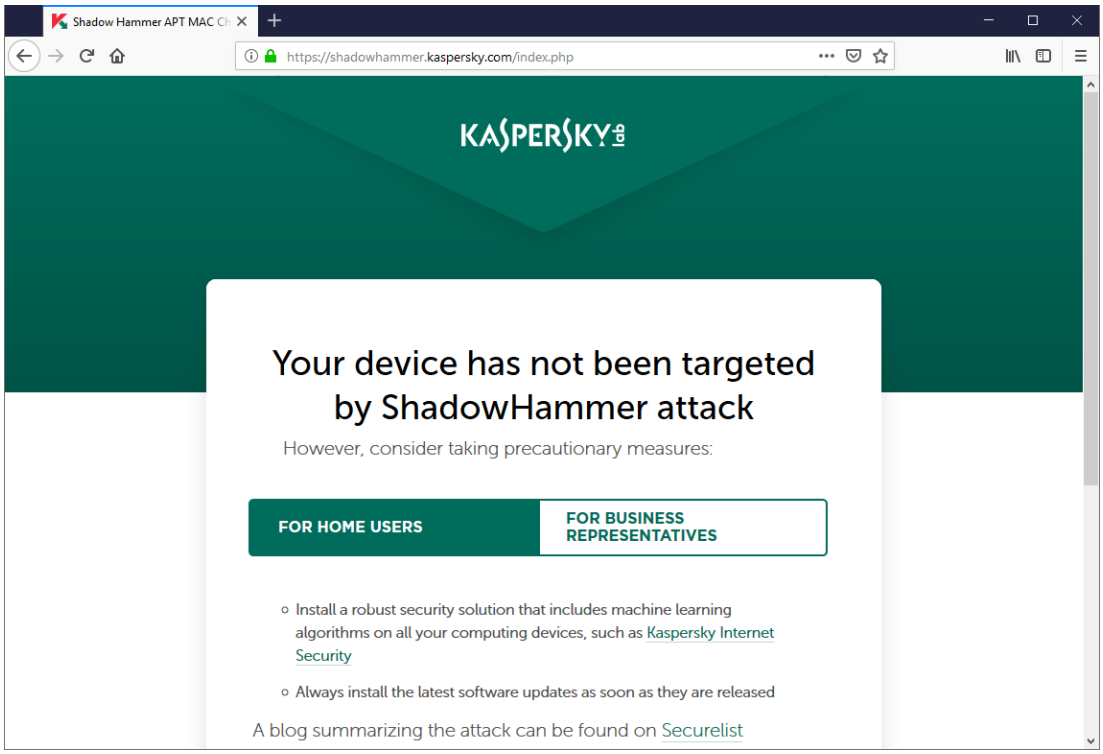
GReAT says that Kaspersky contacted Asus on January 31 to inform them about the supply chain attack targeting the ASUS Live Update utility, also providing the Taiwan-based company with details of the malware used in the attack and IOCs.

Even though Asus was notified about the attack, they haven't maintained active communication channels with Kaspersky and they've also failed to alert Asus users according to Zetter.

Kaspersky also has evidence which matches the methods used during Operation ShadowHammer with the ones utilized against CCleaner and in the ShadowPad supply chain attack from 2017 that affected NetSarang.

As detailed by GReAT, the threat actor behind the latter has already been identified as BARIUM — known users of the Winnti backdoor — by both Microsoft, ESET, and other security researchers.

Kaspersky also provides an offline utility and an online web checker for users who want to check if their computer has been impacted by Operation ShadowHammer. "To check this, it compares MAC addresses of all adapters to a list of predefined values hardcoded in the malware and alerts if a match was found," says GReAT.



Source: https://www.bleepingcomputer.com/news/security/asus-live-update-infected-with-backdoor-in-supply-chain-attack/

10. When It Comes to Incident Response, Failing to Plan Means Planning to Fail

If there's one thing I've learned from working in cybersecurity, it's that security incidents do not simply occur, they are caused — either by legitimate users who unintentionally expose company data or malicious actors who seek to breach enterprise systems undetected. Unfortunately, it is much easier for attackers to identify exploitable vulnerabilities than it is for security teams to fix every flaw in the company's network.

While it would seem the odds are insurmountably stacked against cyberdefenders, there is at least one element of an effective incident response program that even the most ingenious attackers cannot take away from security teams: preparedness and thorough planning.

Why the Time to Contain a Breach Matters

One of the most important metrics in incident response is the time its takes to respond to and contain a security event. According to the "2018 Cost of a Data Breach Study," the costs associated with a breach were 25 percent lower for organizations that managed to contain the incident within 30 days. That's a difference of more than $1 million when you consider the overall average cost of a breach, which is particularly concerning since the average time between detection and containment is 69 days.

This so-called mean time to contain (MTTC) depends on the organization's level of preparedness to rapidly switch into emergency response mode and execute the right tasks in the right order — all under the intense pressure and confusion that invariably arises from a crisis situation. That's why MTTC is a crucial metric in any emergency response plan template.

6 Steps to Strengthen Your Incident Response Plan

Companies with a mature security posture don't just take a proactive approach to mitigating threats, they also train their employees on what to do in a worst-case scenario and how to implement a break-glass policy within their organizations. This requires security leaders to continuously review their plans for gaps and inefficiencies and adjust them accordingly to thoroughly understand the impact of a potential breach from a remediation perspective.

Below are six key steps organizations can take to step beyond proactive measures and prepare to respond in a worst-case scenario.

1. Get Management Support

An incident response plan does not just apply to IT and security. You will need cooperation and resources from people outside the security organization, including legal, human resources and other departments.

2. Know Your Risks

To develop your incident response plan, you must understand the kind of events you are addressing and their potential impact to your organization. The loss and exposure of data is one example that is critical to virtually all companies, and not just since the General Data Protection Regulation (GDPR) took effect. Other risks to consider include production outages, flawed products and third-party breaches. Security leaders should work closely with risk officers to identify the threats with the greatest potential business impact.

3. Define Roles and Responsibilities

It takes a lot of hard work from a variety of people and business functions to identify, contain and eradicate an incident. Roles must be clear in advance, and everyone must know his or her responsibility in the event of a security incident.

Typically, this is where a predefined group of response specialists, known as a computer security incident response team (CSIRT), steps in. In addition to security experts, this team should include representatives from management as well as other business units.

4. Determine Communication Channels

In case of emergency, it's critical to define the relevant communication channels. Communication channels must be open at all times, even if the normal channels are compromised or temporarily unavailable. It's also important to establish guidelines for what details should be communicated to IT, senior management, relevant departments, affected customers and the public.

5. Rules of Engagement

A lot can go wrong during incident response activities. Valuable information can be destroyed through recklessness and thoughtlessness or, worse, by an attacker who is just waiting to exploit poor user behaviors. Therefore, incident response steps should follow a clear structure and methodology, such as the SANS Institute's six-step incident response framework and other publicly available resources that can be adapted to fit an organization's unique needs.

6. Train the Plan

The worst thing you can do is wait until a crisis occurs to execute your incident response process for the first time. Tabletop exercises and run books are always beneficial, but it is most critical to regularly drill the response flow and strive to improve its results in every subsequent drill. It's also helpful for team members to join discussion groups and share successful practices with other teams to sharpen incident response plans and reduce the potential damage from an impending attack.

The Benefits Outweigh the Costs

While a break-glass policy can add more layers of protection in the event of a breach, it also adds to the workload of your already overwhelmed staff. That's why many organizations are hesitant to step forward. But the benefits of containing the damage within a short period of time outweigh the value of this investment by far. By adapting a tried-and-true emergency response plan template to your organization's incident response needs and business goals, you will be in a much better position to minimize the damage associated with a data breach.

The post When It Comes to Incident Response, Failing to Plan Means Planning to Fail appeared first on Security Intelligence.

If you want to learn more about ASOC and how it can improve your security posture, contact us at: **asoc.sales@telelink.com**

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.