telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

October 2019

This security bulletin is powered by Telelink's

Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

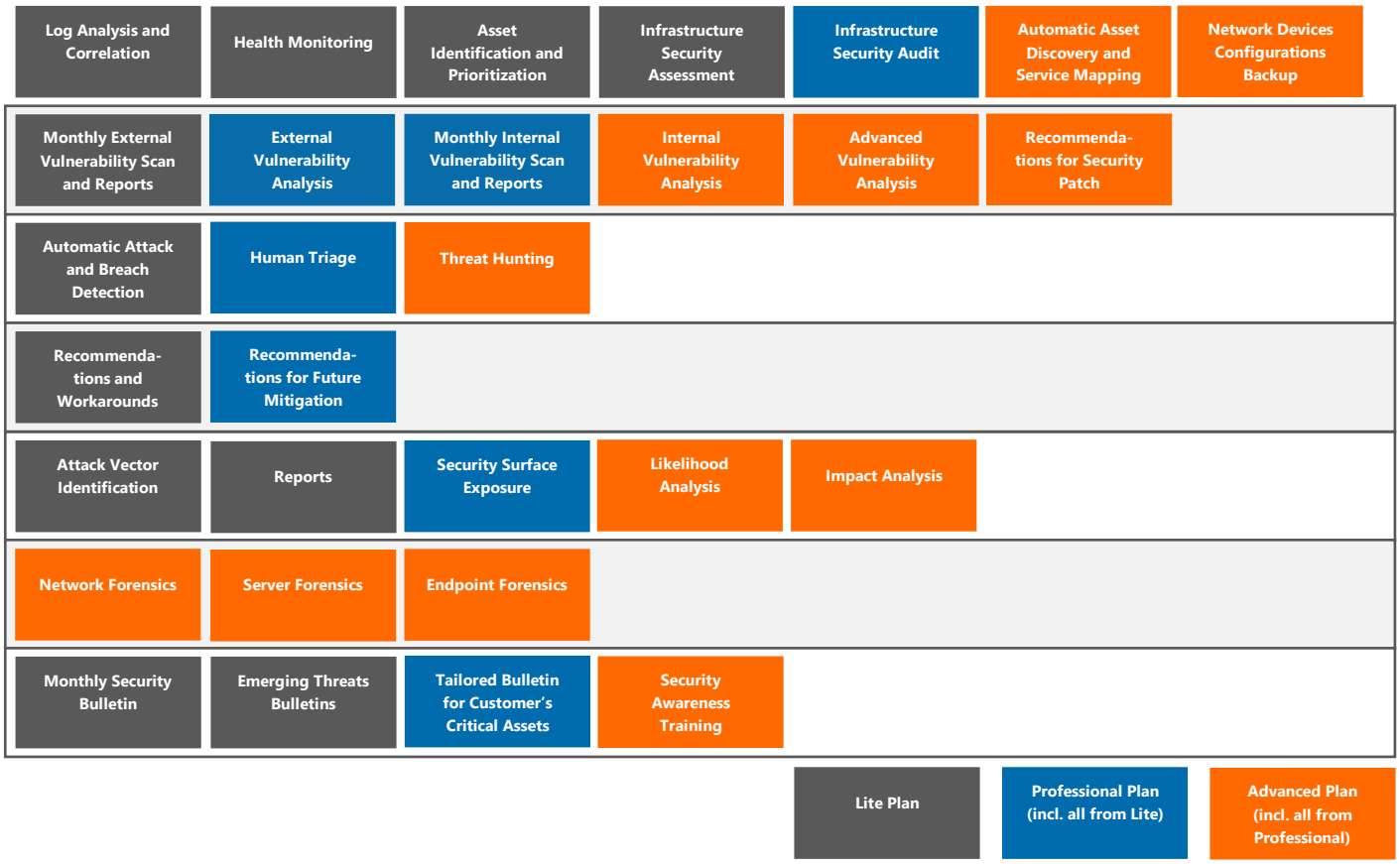
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!



What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state of the art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Contents

Executive summary

1. Elasticsearch server leaked more than 20 million records of personal data on Ecuador's 17 million citizens, including their family trees, children, and some users' financial records and car registration information. The data was stored on poorly security Elasticsearch server that was property of local company named Novaestrat that provides analytics services for the Ecuadorian market. →

2. More than 1,000 security bug bounty reports were submitted during a three-day live hacking event in Las Vegas. The total payout for the participating hackers was almost $2 million and the event was organized by HackerOne, a program that since it's founding in 2012 already made six hackers millionaires →

3. An Android zero-day exploit is now worth more than one for the iPhone on the global cyberweapons market as exploit broker Zerodium put $2.5 million price tag for a zero-click 0-day in Android. →

4. Cybercrooks successfully fooled a company into transferring $243,000 to their bank account using an AI-powered deep fake of a chief executive's voice, according to a report. This is the first known case of successful financial scamming via audio deep fakes, where the cybercrooks were able to create a near-perfect impersonation of a chief executive's voice – and then used the audio to fool his company. →

5. We may be witnessing a second wave of North Korea hack-to-finance campaign: state-sponsored actors seeking to steal bitcoin and other virtual currencies as a means of evading sanctions and obtaining hard currencies to fund the regime. Since May 2017, Mandiant experts observed North Korean affiliated actors target at least three South Korean cryptocurrency exchanges with the suspected intent of stealing funds →

6. Newly discovered threat group, called TortoiseShell is compromising IT providers in what seems to be supply-chain attacks intended to reach the network of specific customers. The group is tracked since July 2018, although it is possible that it has been operating for a longer time. The group relies on both custom and ready-made malware for their operations. →

7. Security vendors released decryptors online, free of charge, for three ransomware infections today that allow victims to recover their files for free - WannaCryFake, Yatron, and FortuneCrypt →

8. After someone published a zero-day exploit on Securelist this week, for the popular online forum platform vBulletin, without providing necessary time for the vendor to issue an fix, now there are number of ongoing attacks in the wild. The exploit is critical remote code execution (RCE) bug affecting default 5.x versions of vBulletin (CVE-2019-16759) and allows unauthenticated attackers to take control of web hosts. →

9. A new fileless malicious campaign, dubbed Nodersok was discovered by Microsoft Defender ATP Research Team. The mallware drops its own LOLBins to infect Windows computers with a Node.js-based malware that will turn the devices into proxies and also delivers the legitimate Node.exe Node.js framework and the Windows Packet Divert (WinDivert) network packet capture tool to support the exploitation →

1. Data leak on most of Ecuador's citizens, including 6.7 million children

Elasticsearch server leaks personal data on Ecuador's citizens, their family trees, and children, but also some users' financial records and car registration information.

Quito, Ecuador Image: Reiseuhu

The personal records of most of Ecuador's population, including children, has been left exposed online due to a misconfigured database, **ZDNet** has learned.

The database, an Elasticsearch server, was discovered two weeks ago by vpnMentor security researchers Noam Rotem and Ran Locar, who shared their findings exclusively with **ZDNet**. Together, we worked to analyze the leaking data, verify its authenticity, and contact the server owner.

The leaky server is one of the, if not the biggest, data breaches in Ecuador's history, a small South American country with a population of 16.6 million citizens.

20.8 million user records

The Elasticsearch server contained a total of approximately 20.8 million user records, a number larger than the country's total population count. The bigger number comes from duplicate records or older entries, containing the data of deceased persons.

The data was spread across different Elasticsearch indexes. These indexes contained different information, supposedly obtained from different sources. They stored details such as names, information on family members/trees, civil registration data, financial and work information, but also data on car ownership.

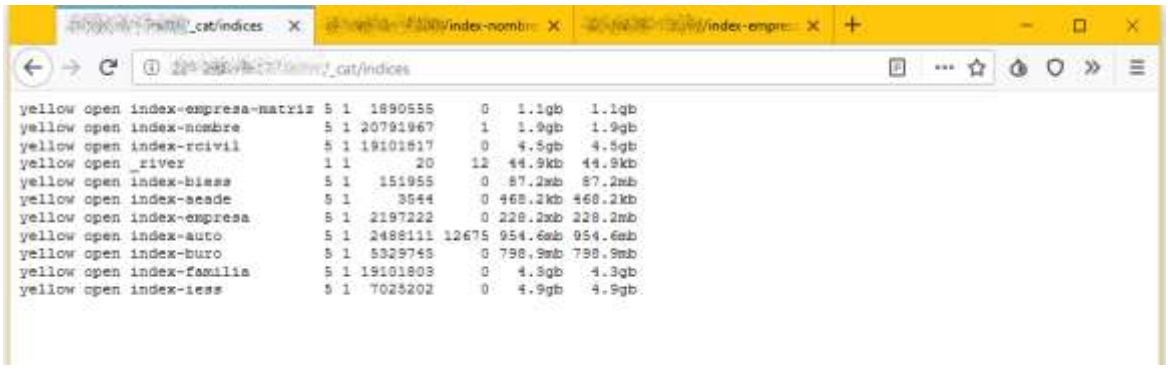


Image: ZDNet

Based on the names of these indexes, the entire database could be split in two main categories, based on the data's supposed origin. There's data that appears to have been gathered from a government sources, and data that appears to have been gathered from private databases.

The data from government sources

The most extensive data was the one that appears to have been gathered from the Ecuadorian government's civil registry.

This data contained entries holding citizens' full names, dates of birth, places of birth, home addresses, marital status, cedulas (national ID numbers), work/job information, phone numbers, and education levels.

ZDNet verified the authenticity of this data by contacting some users listed in the database. The database was up to date, containing information as recent as 2019.

We were able to find records for the country's president, and even Julian Assange, who once received political asylum from the small South Americam country, and was issued a national ID number (cedula).

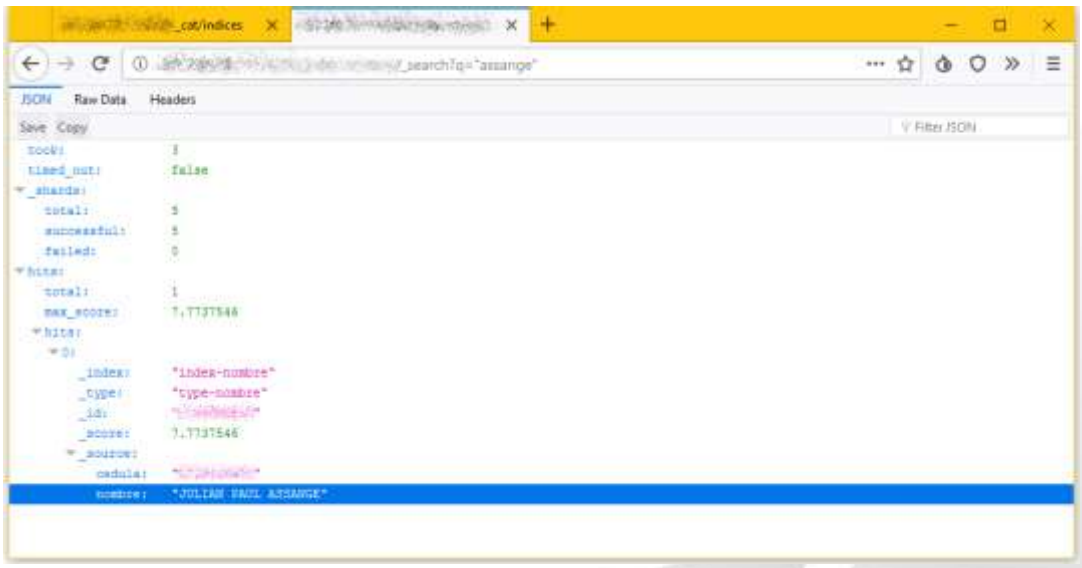


Image: ZDNet

Image: ZDNet

Family and kids data

But we only truly understood the extent of this data when we looked at an index named "familia" (family in Spanish), which contained information about every citizen's family members, such as children and parents, allowing anyone to reconstruct family trees for the entire country's population.

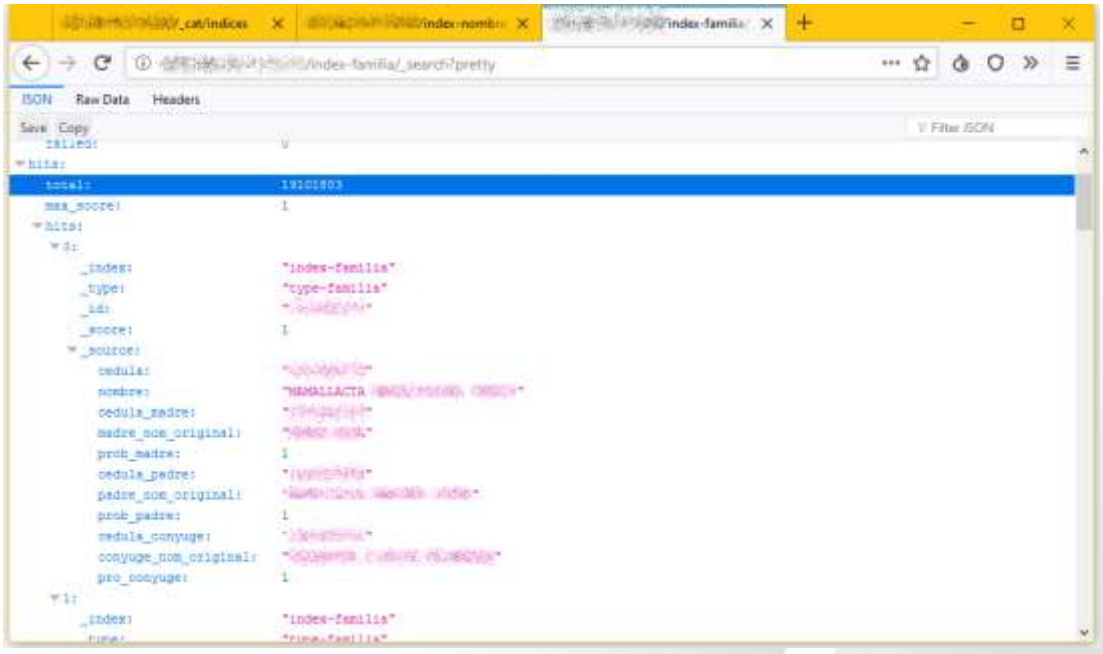


Image: ZDNet

However, things didn't stop here. When looking at this index we also realized that there were entries for children, some of whom were born as recent as this spring.

For example, we found 6.77 million entries for children under the age of 18. These entries contained names, cedulas, places of birth, home addresses, and gender.

Image: ZDNet

The table below shows the number of children records we found in the leaky database. With the exception of the past few years, the rest of the database entries are in tune with public reporting on the country's natality rate.

YEAR	NUMBER OF ENTRIES
2019	187
2018	231
2017	182

2016	222
2015	145,941
2014	456,687
2013	467,604
2012	501,560
2011	542,050
2010	539,124
2009	546,147
2008	536,624
2007	528,335
2006	521,197
2005	491,148
2004	492,139
2003	498,561
2002	511,235

The leak of childrens' data is without a doubt the biggest privacy concern about this incident. This leak not only exposes children to potential identity theft, but also puts them in physical danger because their home addresses have been left exposed online for anyone to find.

The data from private sources

But this wasn't all what the database contained. While initially we thought vpnMentor security researchers stumbled upon a database belonging to the Ecuadorian government, this didn't turn out to be true.

At a closer look, the database also contained indexes labeled with the acronyms of private entities, suggesting they were either imported or scraped from those particular sources. Of note, two indexes were named BIESS and AEADE.

The first, BIESS, stands for Banco del Instituto Ecuatoriano de Seguridad Social, and contained financial information for some Ecuadorian citizens, such as account status, account balance, credit type, and information about the account owner, including job details.

The second, AEADE, stands for Asociación de Empresas Automotrices del Ecuador, and contained information on car owners, and their resective cars, including car models and car license plates.

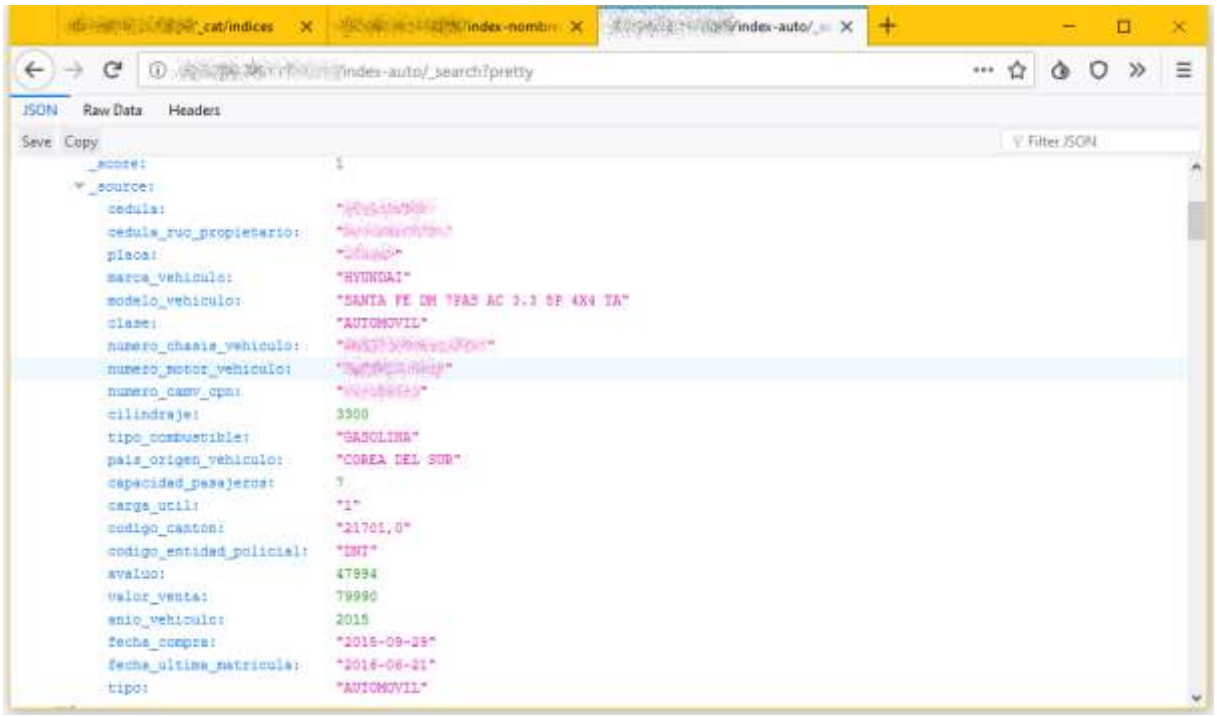


Image: ZDNet

In total, we found 7 million financial records, and 2.5 million records containing car and car owner details.

Just like the Elasticsearch index holding the data of children, these two indexes are also extremely sensitive. The information in both indexes would be as valuable as gold in the hands of criminal gangs.

Crooks would be able to target the country's most wealthy citizens (based on ther financial records) and steal expensive cars (having access to car owners' home addresses and license plate numbers).

Connect the about children and the data about financial records, and criminals would have a list of the most wealthy Ecuadorians, their home addresses, and if they had any children -- making it trivially easy to target and kidnap children from rich families.

The source of the data

When it came time to tracking down the source of this leak, both **ZDNet** and vpnMentor independently reached the same source, namely a local company named Novaestrat.

According to its website, the company provides analytics services for the Ecuadorian market. Its website boldy displays the statement "Make financial decisions with updated information of the entire Ecuadorian Financial System" [translated].

However, getting in contact with the company was not as easy as it sounded. The company did not display an email address or phone number where it could be reached. **ZDNet** reached out to the company via Facebook, and tried contacting employees via LinkedIn, to no success. The company's support forum yielded a PHP error when we tried registering an account.

The database was eventually secured later last week, but only after vpnMentor reached out to the Ecuador CERT (Computer Emergency Response Team) team, which served as an intermediary.

This is the second major leak of user data originating from a South American country in as many months. In August, **ZDNet** reported about a similar Elasticsearch server that exposed the voter records of 14.3 million Chileans, around 80% of the country's entire population.

Additional coverage of this leak can be found on vpnMentor's blog.

Source: https://www.zdnet.com/google-amp/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/

---

2. Hackers Get $1.9M in Bug Bounties at Live Hacking Sessions

More than 1,000 security bug bounty reports were submitted during a three-day live hacking event in Las Vegas. The total payout for the participating hackers was almost $2 million. Three organizations paid the money, one of them covering more than half of the total.

Called h1-702, the event is organized by Hacker One bug bounty platform and was at its fifth edition. 100 hackers from all over the world tested their skills at finding security flaws vulnerabilities.

Not just for experienced hackers

Over 1,049 bugs were submitted to participating companies and $1,902,668 was paid in rewards; a round $1 million came from Verizon Media, which is the highest payout from a single customer at a live hacking event.

"We consider our bug bounty researchers an extension of our team, and these live hacking events help us strengthen our relationships and empower our community" - Chris Holt, Senior Technical Security Engineer at Verizon Media

After the first night of the event, 637 reports had been submitted and over $745,000 were paid in bounties.

The event was not just for seasoned hackers, though. A mentorship program was also available, introducing attendees to security concepts, tools, the basics of the hacker mindset, and how various flaws work.

Compared to a regular bug bounty program, live hacking events are in-person and allow hackers and the security teams of participating organizations work together to identify and validate security flaws.

After three nights of hacking, one participant stood out as the most valuable hacker. That was Romanian national Cosmin Iordache, who earlier this year at a live hacking event in Singapore was able to find a bug in Dropbox and was rewarded with $23,000 for it.

First six millionaires

Founded in 2012, HackerOne has grown into a popular bug bounty program. Earlier this year, the platform announced that 19-year-old Santiago Lopez was the first hacker to make $1million from bug bounty reports.

Lopez was present at this year's edition and along with Ian Bouchard and Jon Colston won the top nightly honors.

Last week, the program announced that five more hackers reached the millionaire status through responsible vulnerability disclosure.

"Now, Mark Litchfield (@mlitchfield) from the U.K., Nathaniel Wakelam (@nnwakelam) from Australia, FransRosen (@fransrosen) from Sweden, Ron Chan (@ngalog) from Hong Kong, and Tommy DeVoss (@dawgyg) from the U.S. joined the $1M hacker ranks by hacking for improved internet security,"

Source: https://www.bleepingcomputer.com/news/security/hackers-get-19m-in-bug-bounties-at-live-hacking-sessions/

---

3. Android Zero-Days Now Worth More Than iPhone Exploits

Exploit broker Zerodium has implemented a $2.5 million price tag for a zero-click 0-day in Android.

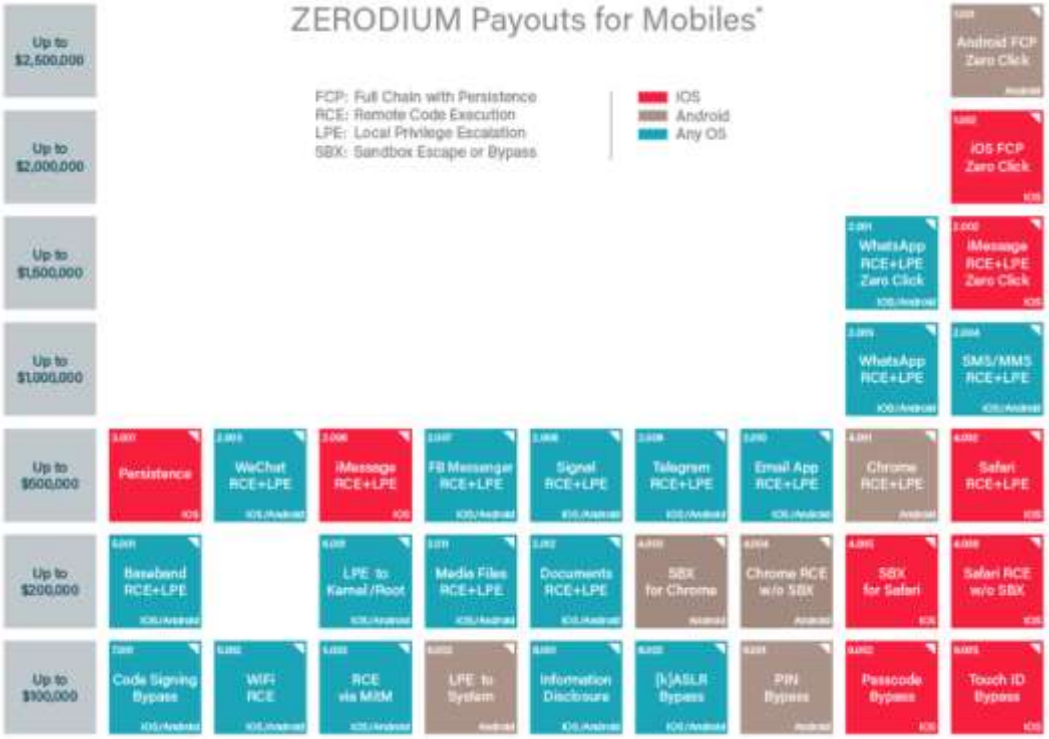
An Android zero-day exploit is now worth more than one for the iPhone on the global cyberweapons market.

Exploit acquisition vendor Zerodium said Tuesday that it is willing to pay a whopping $2.5 million for a zero-click Android zero-day with persistence. That number significantly increases the company's previous payout ceiling of $2 million (for remote iOS jailbreaks).

Android outstripping iPhone in zero-day value is a new turn of events; iPhone exploits have until now commanded top pay-outs from gray-market exploit brokers like Zerodium because they were rare. But as further evidence of iPhone's waning value (and possibly a glut of exploitable bugs in the platform), Zerodium also decreased payouts for another Apple flaw: Apple iOS one-click zero-days with persistence are now worth $1 million (previously worth $1.5 million).

Also, on the iMessage front, most payouts for iMessage zero-days for remote code-execution (RCE) with privilege escalation (LPE) without persistence have been slashed in half, to reach $500,000 instead of $1 million. However, those that are zero-click have been upped in value, with payouts increasing to $1.5 million from $1 million.

Zerodium also added another new bounty — $500,000 for Apple iOS persistence exploits or techniques – and increased payouts for WhatsApp RCE + LPE zero-click exploits from $1 million to $1.5 million.



The move means that payouts for eligible zero-day exploits now range from $2,000 to $2.5 million per submission. The exact bounty amount depends on "the popularity and security level of the affected software/system, as well as the quality of the submitted exploit (full or partial chain, supported versions/systems/architectures, reliability, bypassed exploit mitigations, default vs. non-default components, process continuation, etc.)," according to the company.

Zerodium, launched in 2015 by VUPEN cofounder Chaouki Bekrar, is known for offering lofty payouts for high-risk zero-day exploits. Shortly after it was founded, the company offered a million-dollar bounty for iOS 9 exploits. It then one-upped itself in 2016 by offering a $1.5 million bounty for an iOS 10 remote jailbreak. In 2017, it debuted payouts for private messaging apps such as Signal and WhatsApp, and it said that it will pay up to $1 million for zero-day exploits for Tor Browser on Tails Linux and Windows. And in January, it upped its zero-day payout maximum once again, to $2 million, for remote iOS jailbreaks.

As an vulnerability dealer, Zerodium has not been without controversy for brokering exploits that could end up in the wrong hands. Yet it bills itself as an effort "to build a global community of talented and independent security researchers working together to provide the most up-to-date source of cybersecurity research and capabilities."

It also says that it "analyzes, documents and reports the findings to its clients," (a small set of organizations and governments), "along with protective measures and security recommendations."

Source: https://threatpost.com/android-zero-days-worth-more-iphone-exploits/147981/

---

4. CEO 'Deep Fake' Swindles Company Out of $243K

Cybercrooks successfully fooled a company into a large wire transfer using an AI-powered deep fake of a chief executive's voice, according to a report.

In the first known case of successful financial scamming via audio deep fakes, cybercrooks were able to create a near-perfect impersonation of a chief executive's voice – and then used the audio to fool his company into transferring $243,000 to their bank account.

A deep fake is a plausible video or audio impersonation of someone, powered by artificial intelligence (AI). Security experts say that the incident, first reported by the Wall Street Journal, sets a dangerous precedent.

"In the identity-verification industry, we're seeing more and more artificial intelligence-based identity fraud than ever before," David Thomas, CEO of identity verification company Evident, told Threatpost. "As a business, it's no longer enough to just trust that someone is who they say they are. Individuals and businesses are just now beginning to understand how important identity verification is. Especially in the new era of deep fakes, it's no longer just enough to trust a phone call or a video file."

The WSJ's report, which went live over the weekend, was attributed to the victim company's insurance firm, Euler Hermes Group SA, which declined to name the impacted company but outlined the incident in detail.

The incident kicked off in March, when the CEO of an energy company thought he was speaking via phone to his boss, the chief executive of the firm's German parent company. The caller on the phone asked the CEO to send the funds – totaling €220,000, or $243,000, to a Hungarian supplier in an "urgent" request, with the promise that it would be reimbursed.

The victim, deceived into thinking that the voice was that of his boss – particularly because it had a similar slight German accent and voice pattern – made the transfer. However, once the transaction went through, the fraudsters called back, asking for another urgent money transfer. At that point, the CEO became suspicious and refused to make the payment.

The funds reportedly went from Hungary to Mexico before being transferred to other locations. Euler Hermes Group SA was able to reimburse the affected company, according to the report.

The incident points to how voice fraud, powered by artificial intelligence, is a burgeoning cybersecurity threat to enterprises and consumers alike. A 2018 report by Pindrop found that voice fraud had jumped 350 percent from 2013 to 2017 – with one in 638 calls synthetically created.

While the cybersecurity industry has touted AI as a way for developers to automate functions and for enterprises to sniff out anomolies, this incident also shows how the technology could easily be used maliciously.

In fact, after creating a replica of popular podcaster Joe Rogan's voice (generating life-like speech using only text inputs), Dessa, a company that offers enterprise-grade tools for machine-learning engineering, warned that anyone could utilize AI to impersonate people. That means spam callers could impersonate victims' family members to obtain personal information; criminals could gain entrance to high-security clearance areas through impersonating a government official; or deep fakes of politicians could be used to manipulate election results, said Dessa in a May post.

"Right now, technical expertise, ingenuity, computing power and data are required to make models like [these] perform well," said Dessa. "So not just anyone can go out and do it. But in the next few years (or even sooner), we'll see the technology advance to the point where only a few seconds of audio are needed to create a life-like replica of anyone's voice on the planet. It's pretty… scary."

Security experts have warned that AI is also a boon for cybercriminals who may use the tool to automate phishing, use voice authentication AI applications for spoofing attacks, or for scalable packet sniffing. Luckily, verification techniques do exist that could help flag such fraud attempts, said Evident's Thomas.

"Businesses must be vigilant and employ proper verification techniques – like multi-factor identification, facial recognition and comprehensive identity proofing – to thwart today's AI threats," Thomas told Threatpost.

Source: https://threatpost.com/deep-fake-of-ceos-voice-swindles-company-out-of-243k/147982/

5. Why Is North Korea So Interested in Bitcoin?

In 2016 we began observing actors we believe to be North Korean utilizing their intrusion capabilities to conduct cyber crime, targeting banks and the global financial system. This marked a departure from previously observed activity of North Korean actors employing cyber espionage for traditional nation state activities. Yet, given North Korea's position as a pariah nation cut off from much of the global economy – as well as a nation that employs a government bureau to conduct illicit economic activity – this is not all that surprising. With North Korea's tight control of its military and intelligence capabilities, it is likely that this activity was carried out to fund the state or personal coffers of Pyongyang's elite, as international sanctions have constricted the Hermit Kingdom.

Now, we may be witnessing a second wave of this campaign: state-sponsored actors seeking to steal bitcoin and other virtual currencies as a means of evading sanctions and obtaining hard currencies to fund the regime. Since May 2017, Mandiant experts observed North Korean actors target at least three South Korean cryptocurrency exchanges with the suspected intent of stealing funds. The spearphishing we have observed in these cases often targets personal email accounts of employees at digital currency exchanges, frequently using tax-themed lures and deploying malware (PEACHPIT and similar variants) linked to North Korean actors suspected to be responsible for intrusions into global banks in 2016.

Add to that the ties between North Korean operators and a watering hole compromise of a bitcoin news site in 2016, as well as at least one instance of usage of a surreptitious cryptocurrency miner, and we begin to see a picture of North Korean interest in cryptocurrencies, an asset class in which bitcoin alone has increased over 400% since the beginning of this year.

2017 North Korean Activity Against South Korean Cryptocurrency Targets

- April 22 – Four wallets on Yapizon, a South Korean cryptocurrency exchange, are compromised. (It is worth noting that at least some of the tactics, techniques, and procedures were reportedly employed during this compromise were different than those we have observed in following intrusion attempts and as of yet there are no clear indications of North Korean involvement).
- April 26 – The United States announces a strategy of increased economic sanctions against North Korea. Sanctions from the international community could be driving North Korean interest in cryptocurrency, as discussed earlier.

- Early May – Spearphishing against South Korean Exchange #1 begins.
- Late May – South Korean Exchange #2 compromised via spearphish.
- Early June – More suspected North Korean activity targeting unknown victims, believed to be cryptocurrency service providers in South Korea.
- Early July – South Korean Exchange #3 targeted via spear phishing to personal account.

Benefits to Targeting Cryptocurrencies

While bitcoin and cryptocurrency exchanges may seem like odd targets for nation state actors interested in funding state coffers, some of the other illicit endeavors North Korea pursues further demonstrate interest in conducting financial crime on the regime's behalf. North Korea's Office 39 is involved in activities such as gold smuggling, counterfeiting foreign currency, and even operating restaurants. Besides a focus on the global banking system and cryptocurrency exchanges, a recent report by a South Korean institute noted involvement by North Korean actors in targeting ATMs with malware, likely actors at the very least supporting similar ends.

If actors compromise an exchange itself (as opposed to an individual account or wallet) they potentially can move cryptocurrencies out of online wallets, swapping them for other, more anonymous cryptocurrencies or send them directly to other wallets on different exchanges to withdraw them in fiat currencies such as South Korean won, US dollars, or Chinese renminbi. As the regulatory environment around cryptocurrencies is still emerging, some exchanges in different jurisdictions may have lax anti-money laundering controls easing this process and make the exchanges an attractive tactic for anyone seeking hard currency.

Conclusion

As bitcoin and other cryptocurrencies have increased in value in the last year, nation states are beginning to take notice. Recently, an advisor to President Putin in Russia announced plans to raise funds to increase Russia's share of bitcoin mining, and senators in Australia's parliament have proposed developing their own national cryptocurrency.

Consequently, it should be no surprise that cryptocurrencies, as an emerging asset class, are becoming a target of interest by a regime that operates in many ways like a criminal enterprise. While at present North Korea is somewhat distinctive in both their willingness to engage in financial crime and their possession of cyber espionage capabilities, the uniqueness of this combination will likely not last long-term as rising cyber powers may see similar potential. Cyber criminals may no longer be the only nefarious actors in this space.

Source: http://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html

6. New TortoiseShell Group Hacks 11 IT Providers to Reach Their Customers

A newly discovered threat group that security researchers call TortoiseShell is compromising IT providers in what seems to be supply-chain attacks intended to reach the network of specific customers.

The earliest sign of activity from the actor has been tracked to July 2018, although it is possible that it has been operating for a longer time. The most recent time the threat group was seen active is two months ago, in July.

Group uses custom malware and public tools

Security researchers at Symantec identified 11 organizations that had been hit by TortoiseShell. Most of the targets are based in Saudi Arabia and in at least two cases there are enough clues to conclude that the attacker had privileges of a domain administrator, which come with access to all systems on the network.

With two of the victims, TortoiseShell infected hundreds of hosts, likely because they needed to find the machines that were of interest, the researchers say.

"This is an unusually large number of computers to be compromised in a targeted attack," Symantec says in a report published today.

The researchers say that the group relies on both custom and ready-made malware for their operations. One threat TrotoiseShell uses is the Syskit trojan, a custom backdoor discovered on August 21.

The malware sends to its command and control (C2) server system-related data belonging to the compromised host. Details include (IP address, version of the operating system, computer name, MAC address, running apps, and network connectivity.

It can also execute commands from the C2 be used to download other malware and launch PowerShell to unzip a file or run commands in the Command Prompt console.

Additional tools seen by Symantec are publicly available and count two info stealers and a PowerShell script:

- Infostealer/Sha.exe/Sha432.exe
- Infostealer/stereoversioncontrol.exe
- get-logon-history.ps1

The two info-grabbing malware can collect details about the machine they landed on and "Firefox data of all users of the machine."

These three pieces of malware are not TortoiseShell's full arsenal as the actor relies on other data dumping tools and PowerShell-based backdoors.

Possible overlapping ops

It is unclear how the adversary infects the targets but researchers believe that at least once, the attacker got access by compromising a web server.

This assumption is based on a web shell discovered at one victim, which explains how malware was deployed on the network.

"On at least two victim networks, Tortoiseshell deployed its information gathering tools to the Netlogon folder on a domain controller. This results in the information gathering tools being executed automatically when a client computer logs into the domain." - Symantec

Systems of one TortoiseShell victim had been previously compromised with Poison Frog, a PowerShell-based backdoor associated in the past with activities from another advanced threat, OilRig (a.k.a. APT34, HelixKitten) linked to the Iranian government.

Poison Frog was leaked to the public in April 2019, before the victim had been compromised, and had been deployed a month before TortoiseShell tools. This leads to the assumption that there were two distinct operations, the OilRig actor not necessarily being involved.

Symantec says that IT providers are an attractive target because they offer "high-level access to their client's computers," an advantage that allows sending malicious updates and getting remote access to them.

"This provides access to the victims' networks without having to compromise the networks themselves, which might not be possible if the intended victims have strong security infrastructure, and also reduces the risk of the attack being discovered." - Symantec

Another advantage stemming from attacking a third-party service provider is that the true target is more difficult to identify, hence the real purpose of the campaign, too.

This also applies to TortoiseShell, as researchers do not have details on the customer profiles of the targeted IT providers.

Source: https://www.bleepingcomputer.com/news/security/new-tortoiseshell-group-hacks-11-it-providers-to-reach-their-customers/

---

7. Ransomware Decryptors Released for Yatron, WannaCryFake, & FortuneCrypt

Security vendors released decryptors for three ransomware infections today that allow victims to recover their files for free. These decryptors are for the WannaCryFake, Yatron, and FortuneCrypt Ransomware infections.

While none of these ransomware variants have seen much activity in the wild, even if one user can get their files back for free, it is a win.

Emsisoft releases WannaCry Fake decryptor

Emsisoft has released a decryptor for the WannaCry Fake Ransomware. This ransomware tries to ride on the coattails of the the infamous WannaCry infection by appending the .wannacry extension to encrypted files.

"WannaCryFake is a strain of ransomware that uses AES-256 to encrypt a victim's files. Files that have been encrypted by WannaCryFake are appended with the file extension: ".[][recoverydata54@protonmail.com].WannaCry"."

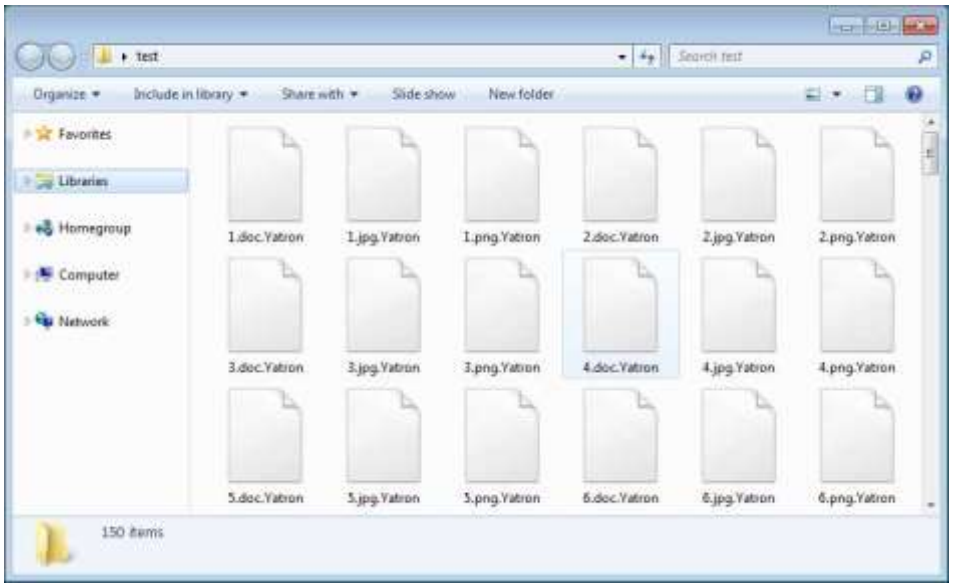
Users who are infected will see a ransom note similar to the one below:

If you were encrypted by this ransomware, you can download the decryptor to recover your files for free.

Kaspersky releases decryptors for Yatron and FortuneCrypt

Kaspersky has released decryptors for the Yatron and the FortuneCrypt ransomwares today due to weaknesses in their encryption algorithms.

We covered Yatron in the past when they started promoting their Ransomware-as-a-Service. Users who were infected with this ransomware would have the .Yatron extension appended to their encrypted files.



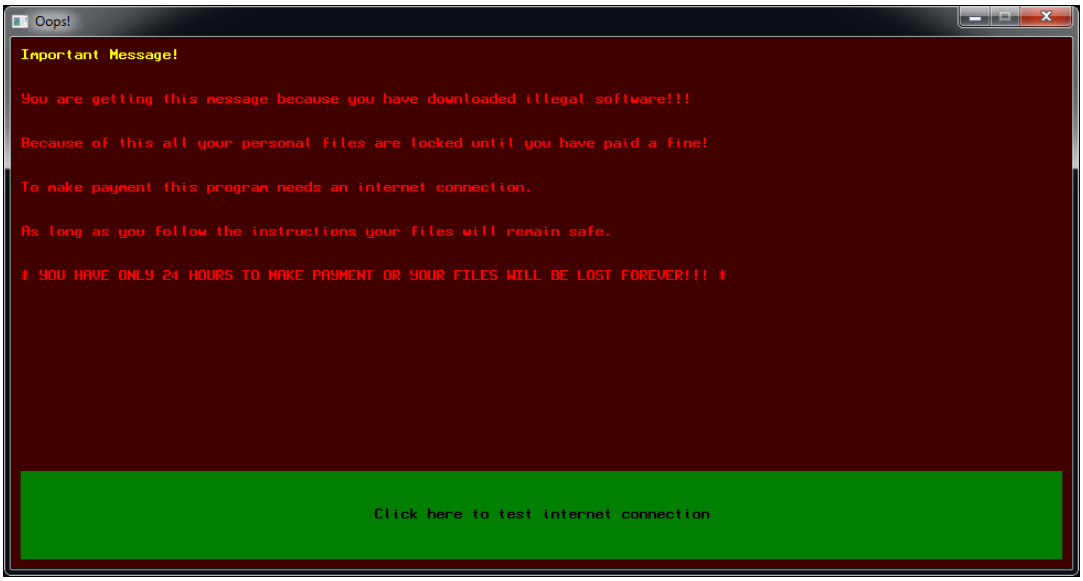
As this ransomware is based off of HiddenTear, which has known weaknesses in its encryption, Kaspersky states they were able to create a decryptor for it. According to Kaspersky, most of the victims of this ransomware are based out of Germany, China, the Russian Federation, India and Myanmar.

"The authors of the ransomware chose the first scenario mentioned above and based their 'creation' on the code used in Hidden Tear, a well-known sample of open-source ransomware. According to our statistics, during the last year alone our products have prevented more than 600 infections by various modifications of Trojan-Ransom.MSIL.Tear, with most attacks recorded in Germany, China, the Russian Federation, India and Myanmar."

Kaspersky also released a decryptor for the FortuneCrypt ransomware that mostly targeted Russian Federation, Brazil, Germany, South Korea and Iran.

"During the last year, our products registered more than 6,000 attacks carried out by the numerous variations of the malicious Trojan-Ransom.Win32.Crypren family (FortuneCrypt is part of this family). The top five countries attacked by the malware are: the Russian Federation, Brazil, Germany, South Korea and Iran."

As this ransomware does not append an extension to encrypted file names, victims would first be alerted when they saw the ransom screen appear as shown below.



Source: Kaspersky

If you have been infected with either the Yatron or FortuneCrypt ransomware infections, you can download Kaspersky's decryptors directly from their site or at No More Ransom.

Source: https://www.bleepingcomputer.com/news/security/ransomware-decryptors-released-for-yatron-wannacryfake-and-fortunecrypt/

---

8. Rash of Exploits Targets Critical vBulletin RCE Bug

After someone dropped a zero-day exploit on Securelist this week, the platform rushed out a fix -- time to apply it.

A critical remote code execution (RCE) bug affecting default 5.x versions of vBulletin (CVE-2019-16759) is being actively exploited in the wild, allowing unauthenticated attackers to take control of web hosts.

A zero-day proof-of-concept code was anonymously published on Monday, ahead of vBulletin issuing a patch. Also, Tenable vice president of intelligence Gavin Millard said via email that there is now a script to leverage Shodan and mass identify thousands of vulnerable systems.

Bug Details

A successful exploit would allow an attacker to take control of a site using vBulletin, a popular platform for powering online forums and communities.

According to Sucuri researcher Marc-Alexandre Montpas, the bug is caused by a flaw in vBulletin's PHP widgets, which are rendered at runtime and used to create dynamic widgets without having to directly access the hosting server.

"The researcher found a way to force the site to render arbitrary widgets using the ajax/render/widget_php route," he explained in a blog post this week. "Since the evalCode callback does exactly what you think it does, essentially running eval on the code it is fed, this makes it possible to run arbitrary code on the underlying server."

Tenable Research analysis showed that an unauthenticated attacker can exploit the issue by sending a specially crafted HTTP POST request to a vulnerable vBulletin host and execute commands.

"These commands would be executed with the permissions of the user account that the vBulletin service is utilizing," said Tenable researcher Ryan Seguin, in the analysis. "Depending on the service user's permissions, this could allow complete control of a host….the published exploit code returns its successful execution in a JSON formatted response."

The fix is for versions 5.5.2, 5.5.3 and 5.5.4; users on earlier versions of vBulletin 5.x will need to update to one of the currently supported versions in order to apply the patch. The fix has also been applied to the cloud version of the platform.

Administrators should apply the patch as soon as possible.

Montpas warned, "This vulnerability is extremely severe. It allows any website visitors to run PHP code and shell commands on the site's underlying server. As if it wasn't bad enough, this bug doesn't require the attacker to have any kind of privilege to conduct a successful attack. vBulletin's default settings also make the vulnerable endpoint accessible by default."

Attacks in the Wild

Sucuri and Tenable telemetry has identified a rash of attacks already taking place in the wild, just days after the PoC was dropped on Securelist.

"The payload attackers are using is very interesting: It essentially modifies the vulnerable snippet by adding a password validation," Montpas noted. "This is a way for attackers to maintain access to sites they've hacked for themselves, as well as lock out other potential hackers from getting in. From this point, the bad actor can use his newly acquired site to do other malicious things in the future."

To find out if a site has been compromised, the researcher said to look for "ajax/render/widget_php" in the access logs. That's because some of the parameters used in the attacks can be located on POST requests, which wouldn't leave any traces in the logs.

Mike Bittner, associate director of Digital Security and Operations at The Media Trust, said that it was just a matter of time before bad actors fixed their crosshairs on forums, which are rich storehouses of user information.

"The argument that many of today's sites do not collect users' information betrays a very uninformed notion of how websites work," he said via email. "Most, if not all, of today's websites are built using a vendor's platform. If you're a small business, you probably don't have the time or the money to build your own platform. If you're a medium-sized or large organization, you don't have the time or money to build a platform with all the bells and whistles users have come to expect. Forums are just one example. Unfortunately, vendors that supply these features too often collect information on users without site owners' authorization, while failing to equip their products with the needed security and privacy protections, leaving website owners to fend for themselves and shoulder the blame for any data breaches involving their sites. In an environment where bad actors are always looking out for vulnerabilities they can exploit or well-intentioned products like vBulletin they can abuse, site owners will need to close the security gaps themselves–ideally by carefully vetting their vendors and ensuring those vendors observe digital policies."

Source: https://threatpost.com/exploits-critical-vbulletin-rce-bug/148712/

---

9. Microsoft Spots Nodersok Malware Campaign That Zombifies PCs

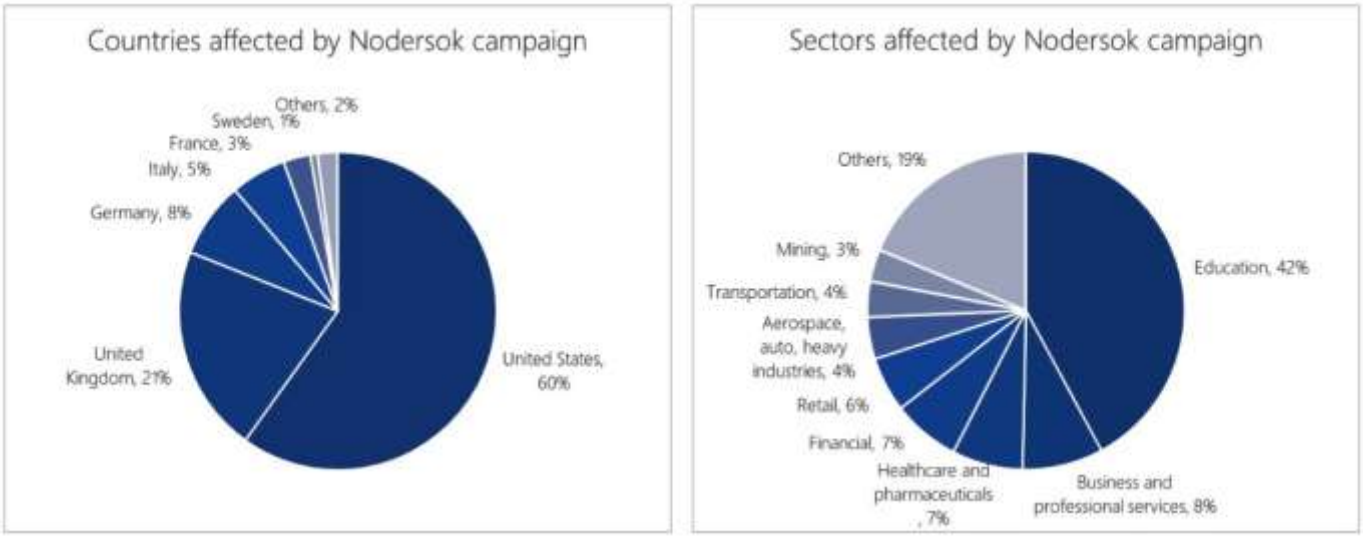
A new fileless malicious campaign, dubbed Nodersok by Microsoft Defender ATP Research Team researchers who discovered it, drops its own LOLBins to infect Windows computers with a Node.js-based malware that will turn the devices into proxies.

Unlike other fileless malware attacks that only use living-off-the-land binaries (LOLBins) present on the devices they compromise, the attackers behind Nodersok have been observed while also delivering the legitimate Node.exe Node.js framework and the Windows Packet Divert (WinDivert) network packet capture tool to devices they target.

The Nodersok malware was used to attack thousands of machines within several weeks, with a focus on home users from U.S. and Europe, with roughly 3% of all attacks also targeting organization from industry sectors such as education, business and professional services, healthcare, finance, and retail.

Cisco Talos also spotted this malware and named it Divergent based on "the naming convention used by the malware during variable declaration and the creation of environment variables."

"This malware can be leveraged by an attacker to target corporate networks and appears to be primarily designed to conduct click-fraud," says Cisco Talos.



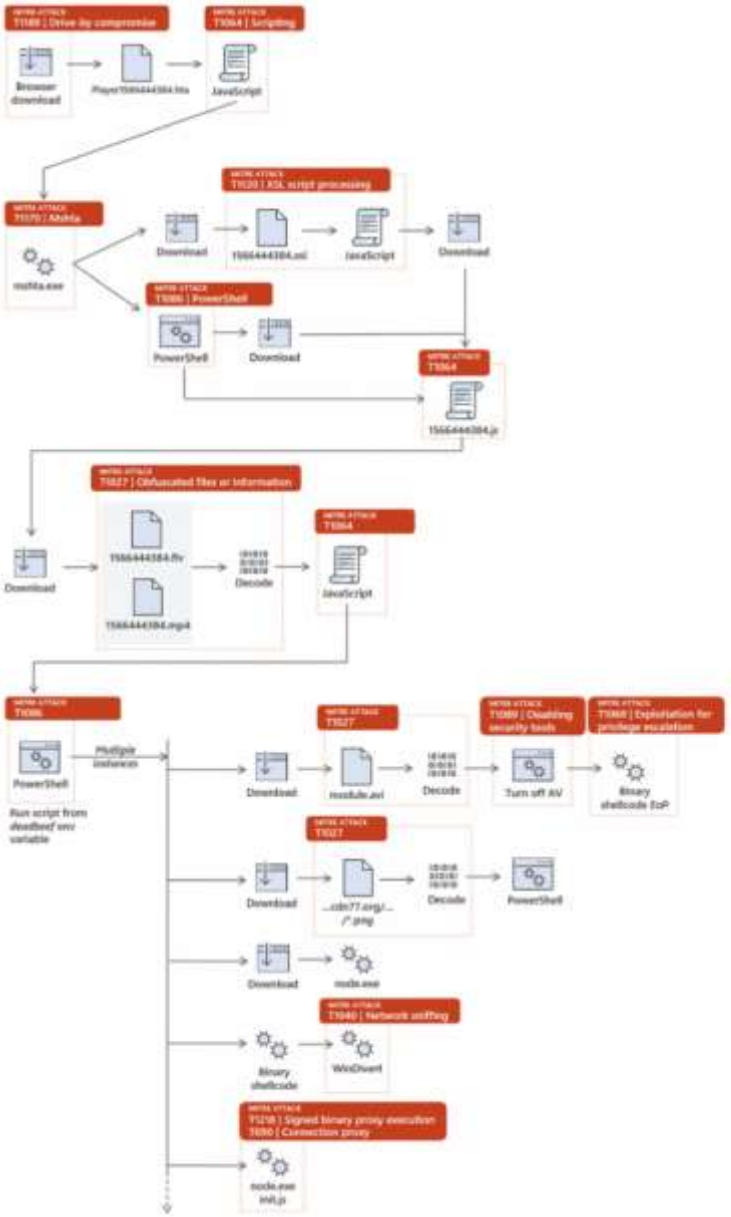
Nodersok attack distribution (Microsoft)

"The campaign is particularly interesting not only because it employs advanced fileless techniques, but also because it relies on an elusive network infrastructure that causes the attack to fly under the radar," found the Microsoft researchers.

"We uncovered this campaign in mid-July, when suspicious patterns in the anomalous usage of MSHTA.exe emerged from Microsoft Defender ATP telemetry."

Nodersok uses a multi-stage infection process that begins with a drive-by compromise of the target's web browser, leading to the execution of a downloaded HTA file delivered either via malvertising or by the user clicking on a malicious link.

The JavaScript code bundled within the HTA downloads a second-stage component in the form of an XSL file containing a JavaScript-based script or a standalone JavaScript file.



1. User runs an HTA file as a download from the browser (by clicking on it, or by browsing a malicious advertisement)
2. JavaScript code in the HTA file downloads a second-stage component (another JavaScript file, or an XSL file containing JavaScript code)
3. The second-stage component launches a PowerShell command by hiding the encoded command text inside an environment variable (the code launches additional PowerShell instances)
4. The PowerShell commands download and run additional encrypted components:
   - A PowerShell module that attempts to disable Windows Defender Antivirus and Windows Update
   - A binary shellcode that attempts to perform an elevation of privilege
   - The Windivert packet capture library
   - A shellcode to run and call the Windivert packet filtering engine
   - Node.exe (from the Node.JS framework)
   - The final payload app.js, a JavaScript module written in Node.JS framework that can turn the machine into a proxy

Nodersok attack chain (Microsoft)

This, in turn, runs a PowerShell command encoded within a deadbeef environment variable to hide it from the PowerShell process' command-line, a command that will launch multiple other PowerShell instances to download and execute the rest of the malicious modules.

The list of modules downloaded by the second-stage PowerShell is quite long and it ends with the final Node.js-based framework designed to zombify the infected computer:

- A PowerShell module that attempts to disable Windows Defender Antivirus and Windows Update
- A binary shellcode that attempts to perform an elevation of privilege
- The Windivert packet capture library
- A shellcode to run and call the Windivert packet filtering engine
- Node.exe (from the Node.JS framework)

- The final payload appjs, a JavaScript module written in Node.JS framework that can turn the machine into a proxy

The zombified PCs now turned into proxies will be used by the threat actors behind the attacks as relay servers designed to provide them with access to other integral parts of their infrastructure like command-and-control (C2) servers and other compromised sites and machines in an effort to make it easier for them to stay hidden during their malicious actions.

According to the Microsoft Defender ATP Research Team, "every step of the infection chain only runs legitimate LOLBins, either from the machine itself (mshta.exe, powershell.exe) or downloaded third-party ones (node.exe, Windivert.dll/sys)."

"All of the relevant functionalities reside in scripts and shellcodes that are almost always coming in encrypted, are then decrypted, and run while only in memory. No malicious executable is ever written to the disk."

Microsoft Security Intelligence

@MsftSecIntel

A new malware campaign we dubbed #Nodersok delivers two very unusual LOLBins to turn infected machines into zombie proxies. Read our latest research here: http://msft.social/FcqeyW

8:42 PM – Sep 26, 2019

The researchers also enumerate the various techniques used by Nodersok's operators as part of each infection stage, as well as the legitimate Windows tools they employed for stealthily spreading the infection on infected systems.

During July, the Microsoft Defender ATP Research Team researchers discovered yet another fileless malware campaign that dropped the information-stealing Astaroth Trojan into the memory of compromised machines.

Just like in the case of the Nodersok campaign, the attacks delivering the Astaroth Trojan also used various fileless techniques and a multi-stage infection process, with the initial infection vector being a spear-phishing email containing a malicious link.

Update September 26, 18:33 EDT: Added more information from Cisco Talos' report on this malware loader.

Source: https://www.bleepingcomputer.com/news/security/microsoft-spots-nodersok-malware-campaign-that-zombifies-pcs/

If you want to learn more about ASOC and how we can improve your security posture, contact us at: **tbs.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 BUSINESS SERVICES 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 BUSINESS SERVICES'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 BUSINESS SERVICES 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.