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

Monthly Security Bulletin

November 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!

⬛ Log Analysis and Correlation	⬛ Health Monitoring	⬛ Asset Identification and Prioritization	⬛ Infrastructure Security Assessment	🟦 Infrastructure Security Audit	🟧 Automatic Asset Discovery and Service Mapping	🟧 Network Devices Configurations Backup
⬛ Monthly External Vulnerability Scan and Reports	🟦 External Vulnerability Analysis	🟦 Monthly Internal Vulnerability Scan and Reports	🟧 Internal Vulnerability Analysis	🟧 Advanced Vulnerability Analysis	🟧 Recommendations for Security Patch	
⬛ Automatic Attack and Breach Detection	🟦 Human Triage	🟧 Threat Hunting				
⬛ Recommendations and Workarounds	🟦 Recommendations for Future Mitigation					
⬛ Attack Vector Identification	⬛ Reports	🟦 Security Surface Exposure	🟧 Likelihood Analysis	🟧 Impact Analysis		
🟧 Network Forensics	🟧 Server Forensics	🟧 Endpoint Forensics				
⬛ Monthly Security Bulletin	⬛ Emerging Threats Bulletins	🟦 Tailored Bulletin for Customer's Critical Assets	🟧 Security Awareness Training			

⬛ Lite Plan 🟦 Professional Plan (incl. all from Lite) 🟧 Advanced Plan (incl. all from Professional)

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. Rise of the internet and subsequent explosion in mobile device usage has led to a more than 300% increase of observation in the wild of specific type of surveillance software – known as stalkerware. The software allows customers to spy on other people after simple manual installation on targeted victim smart phone and for example to monitor their messages, call information and GPS locations – in complete stealth. It can often be used to abuse the privacy of current or former partners and even strangers. →

2. Cuc service software company Zendesk announced an breach that might have impacted roughly 10,000 Zendesk Support and Chat accounts activated prior to November 1, 2016. Currently the platform is used by over 145,000 organizations worldwide according to the company's website, with customers such as Uber, Shopify, Airbnb, and Slack, so the breach affects small number of company's clients. Also only usernames and hashed and salted passwords were exposed →

3. An auction on underground forums for a database allegedly containing personal information of 92 million Brazilian citizens was announced with starting price of $15000. The database allegedly contains names, dates of birth, mother name, gender, taxpayer ID (CPF - Cadastro de Pessoas Físicas) and taxpayer details about legal entities, or the CNPJ (Cadastro Nacional da Pessoa Jurídica) →

4. Researchers from McAfee examined the tools and tactics used by the Sodinokibi ransomware-as-a-service (REvil). Some of the monitored affiliates dropped cryptomining payloads such as MinerGate and XMRig In addition to the Sodinokibi Ransomware payload →

5. In "an extremely sophisticated attempt" hackers accessed the internal network of Czech cybersecurity company Avast, using compromised credentials via a temporary VPN account, likely aiming for a supply chain attack targeting CCleaner. As response on September 25 the company stopped the upcoming updates for the software and checked prior releases for malicious modification. Simultaneously internal user credentials were reset and the new versions are re-signed with new certificate. →

6. Microsoft is currently rolling Office 365 feature dubbed 'Unverified Sender' to help users identify potential spam or phishing emails that reach their inbox. →

7. Microsoft introduced a new range of devices called Secured-core PCs which come with built-in protection against firmware attacks that have been increasingly used by state-sponsored hacking groups like APT28. This new type of secured devices is designed to closely meet an array of software and hardware requirements that will "apply the security best practices of isolation and minimal trust to the firmware layer, or the device core, that underpins the Windows operating system." →

8. Servers belonging to the NordVPN and TorGuard VPN (with possible access to VikingVPN as well) companies were hacked and attackers stole and leaked the expired private keys associated with certificates used to secure their web servers and VPN configuration file. This potentially would allow and adversary to execute MiTM attack against users of the two popular VPN services. →

9. With recent data breaches containing usernames and passwords we see uptake in credential-stuffing attacks - an malicious actor with a list of stolen usernames and passwords is testing them at various other sites via automated means. →

10. Security researchers confirmed that Google and Amazon smart speakers can be leveraged to record user conversation or to phish for passwords through malicious voice apps that allow the audio to reach third party servers →

11. Two plugins for popular CMS Wordpress - The Qode Instagram Widget and Qode Twitter Feed, included in popular Bridge theme, have bugs that could allow redirects to malicious sites. This is commonly used in phishing scams →

12. New ransomware called MedusaLocker is being actively distributed via yet to be determined method and victims have been seen from all over the world. →

13. The 15-year old hacking tool Metasploit is dangerous today - some actors, including AP20 and APT41 are using framework technique called Shikata Ga Nai to bypass even modern endpoint protection mechanisms. →

14. A buffer underflow bug in PHP could allow remote code-execution (RCE) on targeted NGINX servers was discovered during hCorem Capture the Flag competition in September. The bug is coded as CVE-2019-11043 and is trivial to exploit with public PoC →

15. Despite investing 2.4 billion euros since 2016 (when it was breached again) to upgrade its cybersecurity profile, Italian banking giant UniCredit announced that it has suffered its third recent data breach, this time impacting 3 million customers, leaking names, phone numbers, e-mails and cities. No bank account details were affected according to the bank. →

16. Scammers are hacking into WordPress and Blogger sites and using the hacked accounts to create posts stating that the blogger's computer has been hacked and that they were recorded while using adult web sites. The sextortion aims to extract money out of the affected users. →

1. The State of Stalkerware in 2019

Introduction and methodology

Six months ago, we created a special alert that notifies users about commercial spyware (stalkerware) products installed on their phones. This report examines the use of stalkerware and the number of users affected by this software in the first eight months of 2019.

Consumer surveillance technology has evolved rapidly in recent years and the very purpose of surveillance activity has changed dramatically. The rise of the internet and subsequent explosion in mobile device usage has led to a thriving type of surveillance software – known as stalkerware. The software allows users to spy on other people – for example, to monitor their messages, call information and GPS locations – in complete stealth. It can often be used to abuse the privacy of current or former partners and even strangers. This can be done by simply manually installing an application on the targeted victim's smartphone or tablet. Once in place, the stalker receives access to a range of personal data, despite being remote from the victim. It differs greatly from parental control software. While parental control apps aim to restrict access to risky and inappropriate content and persistently notifies a user about its requests, stalkerware is about providing the abuser with surveillance to spy on a victim, without the consent of an individual.

The vast majority of stalkerware apps are not available on official app stores – like Google Play – and installation requires access to a dedicated website and access to the victim's device. Those with bad intentions may use it to monitor employee emails, track children's movements and even spy on what a partner is up to. Such uses may lead to harassment, surveillance without consent, stalking and even domestic violence. However, current laws to regulate the use of stalkerware are not yet strong enough to deter culprits from abusing and taking advantage of other people.

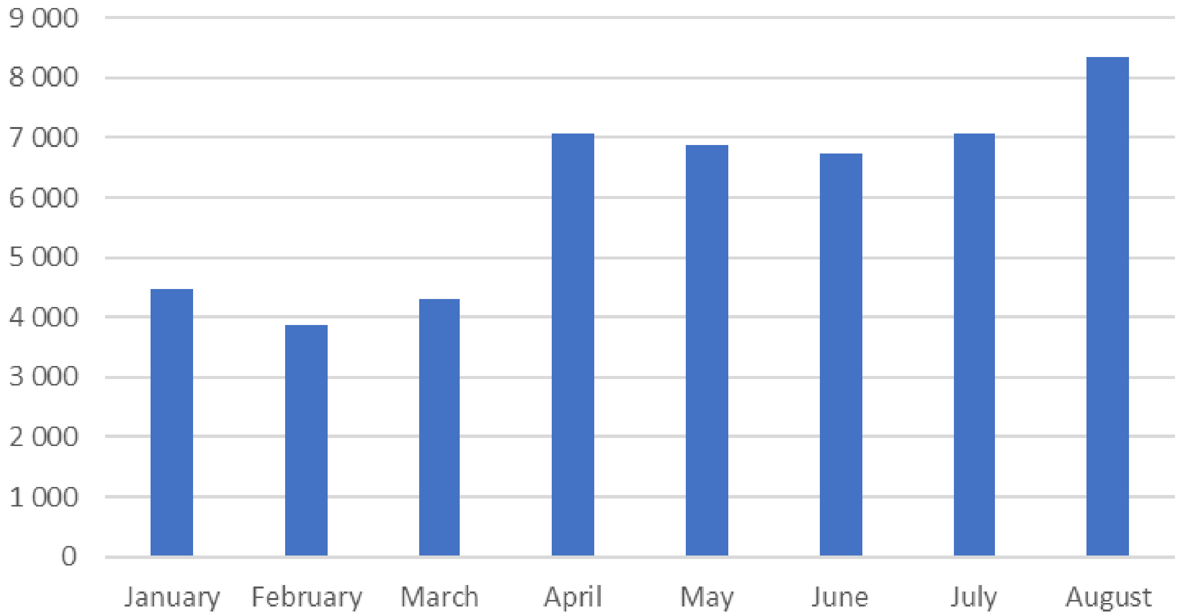
The data in this report has been taken from aggregated threat statistics obtained from the Kaspersky Security Network, to measure how often and how many users encountered stalkerware threats in the first eight months of 2019, compared to what was found last year. The Kaspersky Security Network is the infrastructure dedicated to processing cybersecurity-related data streams from millions of voluntary participants around the world. In this blog, we have explored why stalkerware is being used and where it is implemented most prolifically.

Main findings

- From January to August 2019, around the world, there were more than 518,223 cases when our protection technologies either registered presence of stalkerware on users' devices or detected an attempt to install it – a 373% increase in the same period in 2018
- In the first eight months of 2019, 37,532 users encountered stalkerware at least once. This is a 35% increase from the same period in 2018 when 27,798 users were targeted
- The number of users targeted by full-throttle spyware detected as Trojan-Spy reached 26,620 the first eight months of 2019, which makes it a minority compared to the number of users who encountered stalkerware
- The Russian Federation remains the most prominent region for stalkerware globally, accounting for 25.6% of potentially affected users, in the first eight months of 2019. India is in second place with 10.6% of affected users, and Brazil is in third place (10.4%). The United States hold forth place with 7.1%
- When it comes to Europe – Germany, Italy and the UK hold the top three places respectively

Rise of the stalkerware problem

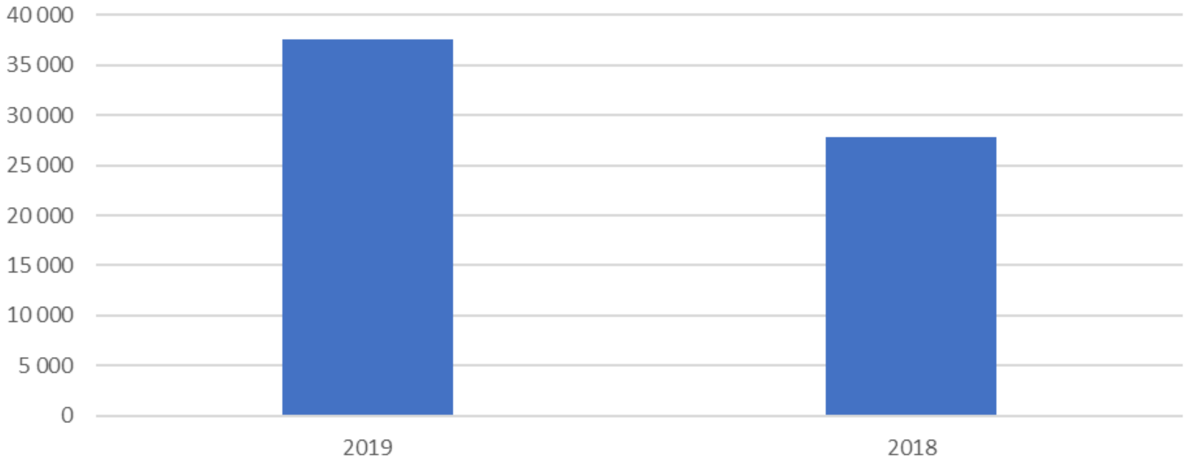
This year has seen a sharp rise in the number of detections of stalkerware on Android devices protected by Kaspersky products. One reason for this rise could be the improvement in detecting stalkerware software through cybersecurity solutions. In April, Kaspersky launched functionality in its Android security app – Privacy Alert – that specifically alerts users if a software that can be used for stalking is found on their device. Since then, the number of detections has steadily risen. For instance, 4,315 users encountered stalkerware in March 2019, compared to 7,075 in April – a 64% increase in just one month. This figure rose to 9,251 during August, 94% higher than the month before the functionality was launched.



Number of users who encountered stalkerware in Jan-Aug 2019

These openly-sold consumer surveillance programs are often used for spying on colleagues, family members or partners, and are in great demand. For a relatively modest fee, sometimes as little as $7 per month, these apps stay hidden while keeping their operators informed about the device activity, such as its owner's location, browser history, text messages, social media chats, and more. Some of them can even make video and voice recordings.

To further examine the extent of the stalkerware problem, Kaspersky has analyzed the last eight months' worth of activity. Between January to August 2019, 37,533 users encountered stalkerware on their devices at least once. This is a 35% increase from the same period in 2018 when 27,798 users were targeted. Overall, there were 518,223 cases when Kaspersky products either registered the presence of stalkerware on users' devices or detected an installation attempt in the period from January to August 2019 – a staggering 373% increase compared to the period in 2018.



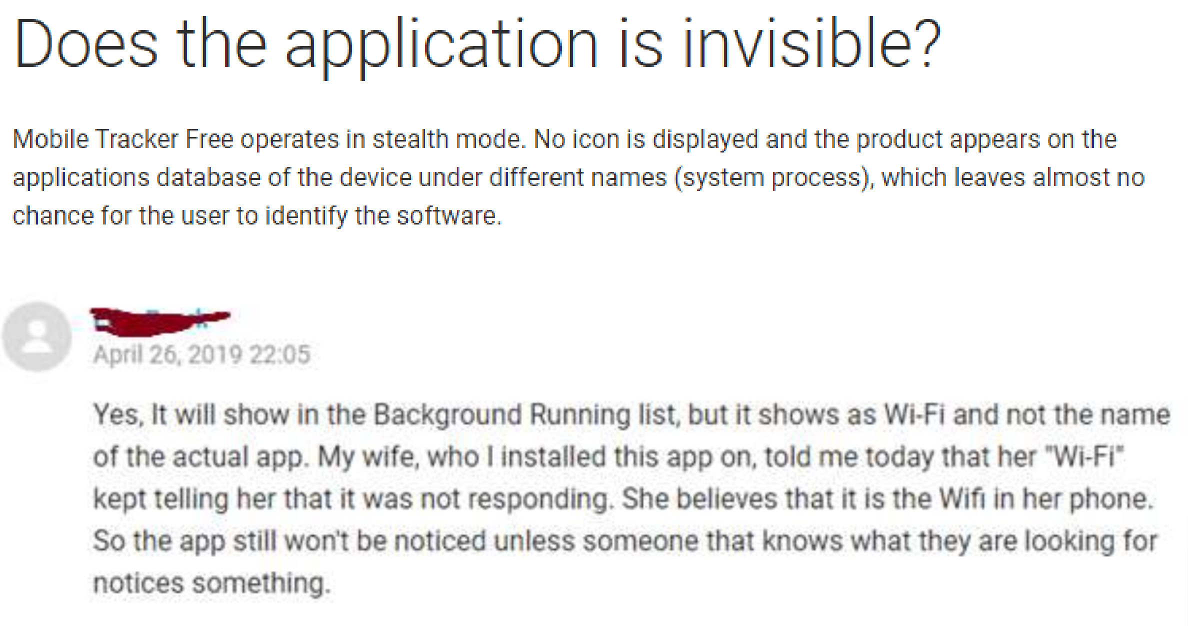
Users targeted by stalkerware 2018 vs 2019

Examples of software used for stalking purposes

The most prolific stalkerware family in 2019 was identified as Monitor.AndroidOS.MobileTracker.a, which affected 6,559 unique users. In second place, Monitor.AndroidOS.Cerberus.a was detected on the devices of 4,370 users, closely followed in third place by Monitor.AndroidOS.Nidb.a (4,047).

Comparing the results from 2018, the top two differ from last year. Monitor.AndroidOS.Nidb.a and Monitor.AndroidOS.PhoneSpy.b were found most on the devices of users in 2018, reaching 4,427 and 2,819 respectively. Monitor.AndroidOS.XoloSale.a was the third most common stalkerware reaching 1,946 users.

In our internal classification system, a Monitor.AndroidOS.MobileTracker.a record is used to identify a Mobile Tracker Free application, which is positioned as a tool to track the activity of children or employees. In fact, the application allows tracking of the user's location, their correspondence both in SMS messages and messenger applications (WhatsApp, Hangouts, Skype, Facebook Messenger, Viber, Telegram, etc.), as well as calls. A third-party can also access victims' photos from the phone and the camera in real-time, along with their browser history, files on the device, calendar and contact list. In addition, the application provides the ability to remotely control the device. As well as all of this, there is a possibility of working in a hidden mode under the disguise of system applications.



Does the application is invisible?

Mobile Tracker Free operates in stealth mode. No icon is displayed and the product appears on the applications database of the device under different names (system process), which leaves almost no chance for the user to identify the software.

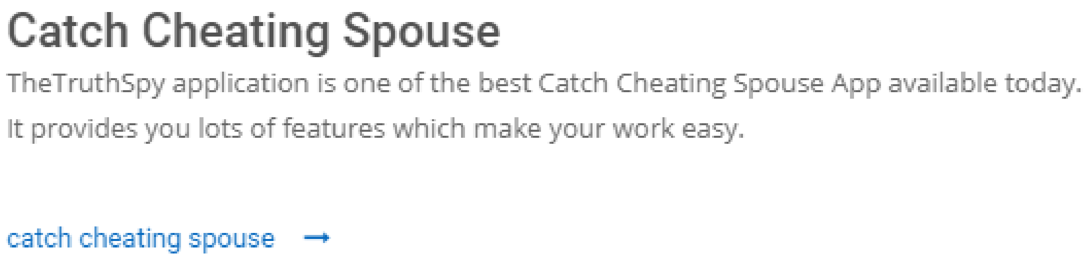
[redacted]
April 26, 2019 22:05

Yes, It will show in the Background Running list, but it shows as Wi-Fi and not the name of the actual app. My wife, who I installed this app on, told me today that her "Wi-Fi" kept telling her that it was not responding. She believes that it is the Wifi in her phone. So the app still won't be noticed unless someone that knows what they are looking for notices something.

Screenshots from the Mobile Tracker Free official website

The next application – Cerberus (Monitor.AndroidOS.Cerberus.a) – is positioned as an anti-theft app. However, it also allows a stalker to work in 'hidden' mode and to prevent its deletion. Among other things, it provides the ability to track the location of the device, take pictures from the camera and screenshots, as well as record audio from the microphone.

The third-placed Monitor.AndroidOS.Nidb.a is in fact a group of similar applications: iSpyoo/TheTruthSpy/Copy9. Unlike the previous two applications, some representatives of this group openly advertise themselves as a means of spying on a partner and even write articles about it.



Catch Cheating Spouse

TheTruthSpy application is one of the best Catch Cheating Spouse App available today. It provides you lots of features which make your work easy.

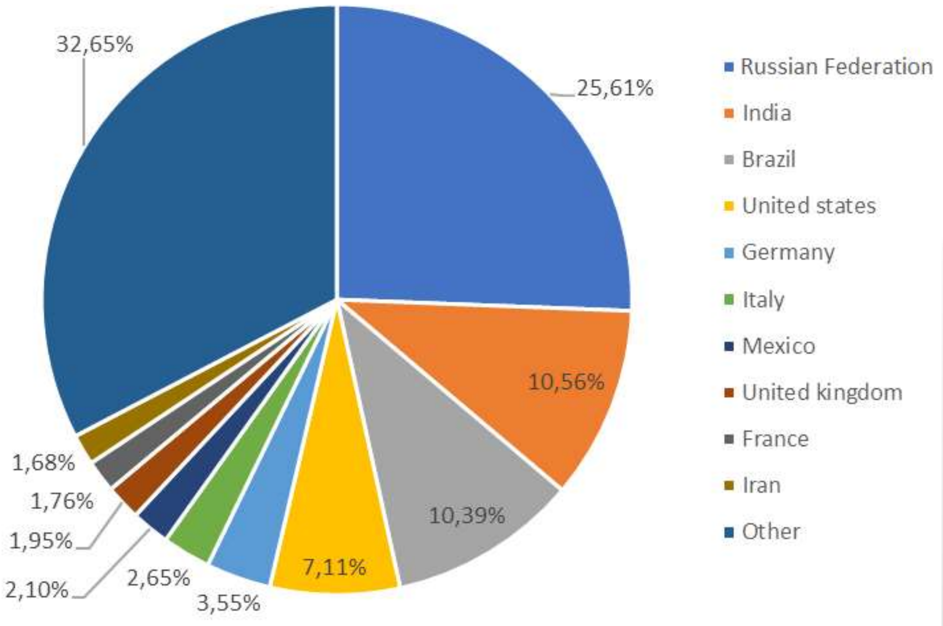
catch cheating spouse →

Screenshot from the TheTruthSpy official website

The set of functions is quite standard for such programs yet still impressive – website tracing, interception of correspondence in SMS and in messenger applications, call tracing and browser history. Like many other similar applications, they require super-user rights (administration rights) to operate some functions. They can work in 'hidden' mode, and their names in the list of installed applications mimic the system processes.

Where is stalkerware found?

There is a global market for legal spyware and stalkerware software, as proven by the diverse range of regions where the most attacks are taking place. The top 10 countries with the largest share of users attacked with stalkerware do not have geopolitical similarities and are not in close proximity.



Geography of users who encountered stalkerware in 2019

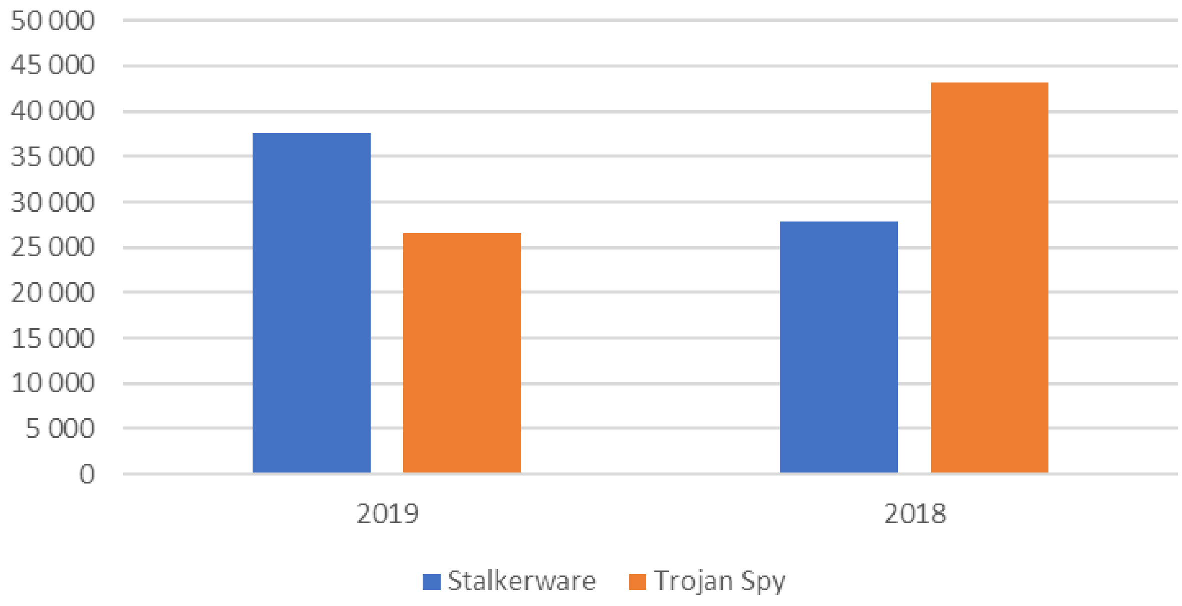
Kaspersky's findings show that Russia is the region where stalkerware activity is peaking. Persistent activity in India has led to the country being the second most prominent region for stalkerware-related incidents from January to August, with 10.56% users affected.

Brazil accounted for 10.39% of attacked users in 2019, while the United States are now fourth (7.11%). There are advocacy groups in the country raising awareness about the dangers of stalkerware and conducting revealing user research. 72 domestic violence shelters were surveyed by National Public Radio, with 85% of domestic violence workers saying they have assisted victims whose abuser tracked them using GPS. Nearly three-quarters (71%) of domestic abusers monitor survivors' computer activities, while 54% tracked survivors' cell phones with stalkerware. The fifth most prevalent country in 2019 was Germany with (3.55%).

Stalkerware on the cyberthreat landscape

When comparing stalkerware and spyware to the rest of the attacks mobile users face – such as adware, riskware and malware – it takes up a big share of less targeted not-a-virus programs. In the first eight months of 2019, Kaspersky detected 2,350,862 users attacked with potentially unwanted threats and just 1.60% of them were related to stalkerware. However, unlike the majority of mass potential threats (like adware), stalkerware requires a specific stalker to act and carry out its operation. Every target is being stalked and chosen on purpose. So, while the numbers are lower, stalkerware takes a more targeted effort to affect a victim and has a disturbing figure of abuse behind each of them.

To get the big picture when assessing the stalkerware development dynamics, we've compared stalkerware to the full scale, illegal survelliance malware for PC that we detect as Trojan Spy. The results have proved, that while illegal spyware is in decline, stalkerware is thriving.



Users attacked by stalkerware and spyware

Our analysis of the first eight months of 2019 shows that the number of users who encountered stalkerware had, in fact, surpassed the figure for Trojan-Spy attacks. While 2018 saw more than 43,000 spyware targets compared to around 28,000 stalkerware targets, in 2019 the picture changed. The number of users that encountered stalkerware grew by 35% to reach over 37,000, while spyware tools accounted for 26,620 of targets.

There has been a notable rise in the number of stalkerware-related incidents registered by Kaspersky products when compared to all threats from the figures in 2018. Between January and August last year, such software made up just 1.01% of the overall number of users who faced any kind of potentially dangerous (adware and others from not-a-virus category) software (2,740,023). It appears that stalkerware is growing in popularity, while more traditional malware attacks are less prolific than they were 12 months ago.

Conclusion and recommendations

It is clear to see that stalkerware is on the rise and becoming much more prominent in the cybersecurity landscape. In accordance with the overall number of detected riskware, adware and spyware attack fluctuations year-on-year, the percentage of stalkerware-related incidents continues to rise. It may take time to discover the role of stalkers on the cyberthreat landscape, but more incidents are now accounted for. Thanks to improved cybersecurity software, there has been a sharp rise since Kaspersky launched its own solution to notify users about stalkerware in April 2019.

There has also been a level of consistency around which countries are the most likely to experience stalkerware-related incidents, with Russia, India, the United States and Germany amongst the most prominent for the last two years.

The good news for users is that functionality and effective solutions are being put in place so they can protect themselves. Practical ways to solve the problem are coming to the fore. IT security companies and advocacy organizations working with domestic abuse victims should join forces to ensure that cybersecurity companies respond better to stalkerware. Such initiatives would help victims through technology and expertise.

We believe that every person has a right to be privacy-protected. That’s why we deliver security expertise, work closely with international organizations and law enforcement agencies to fight cybercriminals, as well as develop technologies, solutions and services that help you stay safe from the cyberthreats.

Source: https://securelist.com/the-state-of-stalkerware-in-2019/93634/

2. Zendesk Security Breach May Impact Orgs Like Uber, Slack, and FCC

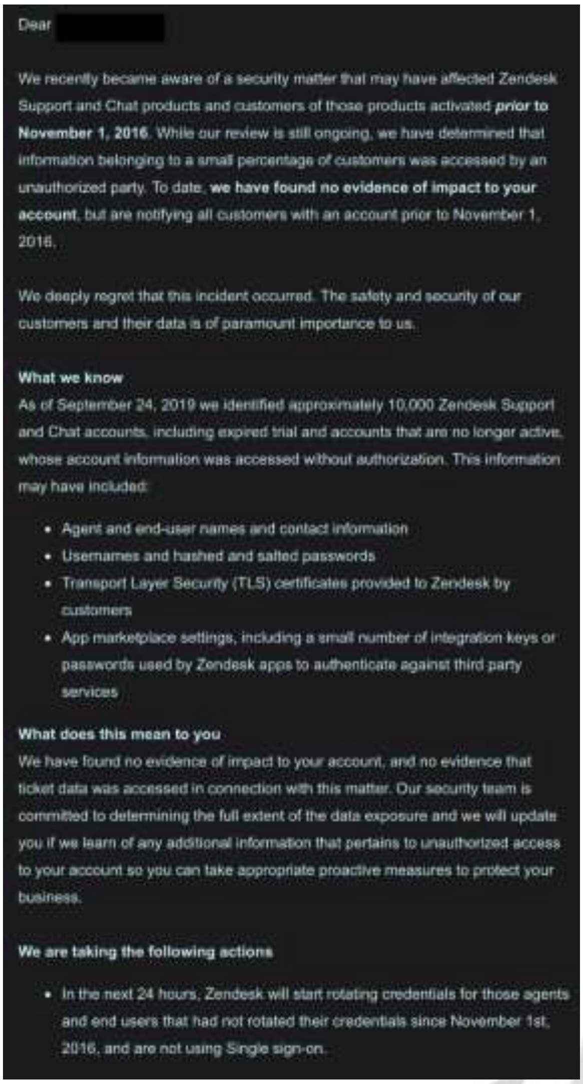
Customer service software company Zendesk has published a blog post today and is sending users notifications regarding a security incident that might have impacted roughly 10,000 Zendesk Support and Chat accounts activated prior to November 1, 2016.

Zendesk's customer support platform is currently used by over 145,000 organizations worldwide according to the company's website, with customers such as Uber, Shopify, Airbnb, and Slack.

"We recently were alerted by a third party regarding a security matter that may have affected the Zendesk Support and Chat products and customer accounts of those products activated prior to November of 2016," says Zendesk.

"While our investigation is still ongoing, on September 24, 2019, we determined that information belonging to a small percentage of customers was accessed prior to November of 2016."

Even though Zendesk found no evidence that all accounts registered before November 1, 2016, were affected, the company says that it has decided to alert all of them nonetheless.



Dear [redacted]

We recently became aware of a security matter that may have affected Zendesk Support and Chat products and customers of those products activated ***prior to* November 1, 2016**. While our review is still ongoing, we have determined that information belonging to a small percentage of customers was accessed by an unauthorized party. To date, **we have found no evidence of impact to your account**, but are notifying all customers with an account prior to November 1, 2016.

We deeply regret that this incident occurred. The safety and security of our customers and their data is of paramount importance to us.

What we know
As of September 24, 2019 we identified approximately 10,000 Zendesk Support and Chat accounts, including expired trial and accounts that are no longer active, whose account information was accessed without authorization. This information may have included:

- Agent and end-user names and contact information
- Usernames and hashed and salted passwords
- Transport Layer Security (TLS) certificates provided to Zendesk by customers
- App marketplace settings, including a small number of integration keys or passwords used by Zendesk apps to authenticate against third party services

What does this mean to you
We have found no evidence of impact to your account, and no evidence that ticket data was accessed in connection with this matter. Our security team is committed to determining the full extent of the data exposure and we will update you if we learn of any additional information that pertains to unauthorized access to your account so you can take appropriate proactive measures to protect your business.

We are taking the following actions

- In the next 24 hours, Zendesk will start rotating credentials for those agents and end users that had not rotated their credentials since November 1st, 2016, and are not using Single sign-on.

Zendesk user notification (Source: David Jacobus)

In the blog post published today, Zendesk also advises customers who have received the notification email to take the following steps:

- If you installed a Zendesk Marketplace or private app prior to November 1, 2016 that saved authentication credentials such as API keys or passwords during installation, we recommend that you rotate all credentials for the respective app.
- In addition, if you uploaded a TLS certificate to Zendesk prior to November 1, 2016 which is still valid, we recommend you upload a new certificate, and revoke the old one
- While we have no indication at this time that other authentication credentials were accessed, customers may want to consider rotating authentication credentials used in Zendesk products prior to November 1, 2016. API Tokens in Chat do not need to be rotated.

Hashed, salted passwords and usernames exposed

"As of September 24, 2019, we identified approximately 10,000 Zendesk Support and Chat accounts, including expired trial and accounts that are no longer active, whose account information was accessed without authorization," states Zendesk.

Following the investigation, the company discovered that the following customer information might have been accessed during the incident:

- Agent and end-user names and contact information
- Usernames and hashed and salted passwords
- Transport Layer Security (TLS) certificates provided to Zendesk by customers
- App marketplace settings, including a small number of integration keys or passwords used by Zendesk apps to authenticate against third party services

"Our security team is committed to determining the full extent of the data exposure and we will update you if we learn of any additional information that pertains to unauthorized access to your account so you can take appropriate proactive measures to protect your business," adds Zendesk.

The company also says that it will reset the credentials of end-users and agents that don't use Single sign-on or haven't done that one their own since November 1, 2016, during the next 24 hours following the notifications' delivery.

To be safe, customers who accessed Zendesk's customer support platform this month should change their passwords.

Not Zendesk's first rodeo

If you installed a Zendesk Marketplace or private app prior to November 1, 2016 that saved authentication credentials such as API keys or passwords during installation, we recommend that you rotate all credentials for the respective app.

In addition, if you uploaded a TLS certificate to Zendesk prior to November 1, 2016 which is still valid, we recommend you upload a new certificate, and revoke the old one

While we have no indication at this time that other authentication credentials were accessed, customers may want to consider rotating authentication credentials used in Zendesk products prior to November 1, 2016. API Tokens in Chat do not need to be rotated.

BleepingComputer has reached out to Zendesk for more info regarding the security incident but had not heard back at the time of this publication. This article will be updated when a response is received.

Source: https://www.bleepingcomputer.com/news/security/zendesk-security-breach-may-impact-orgs-like-uber-slack-and-fcc/

3. Details of 92 Million Brazilians Auctioned on Underground Forums

Someone is auctioning on underground forums a database allegedly containing personal information of 92 million Brazilian citizens. They claim that every record is real and unique.

The seller also advertises a search service focused on Brazilians, saying that they can dig up details about an individual starting from minimum initial data.

Highest bidder gets the data

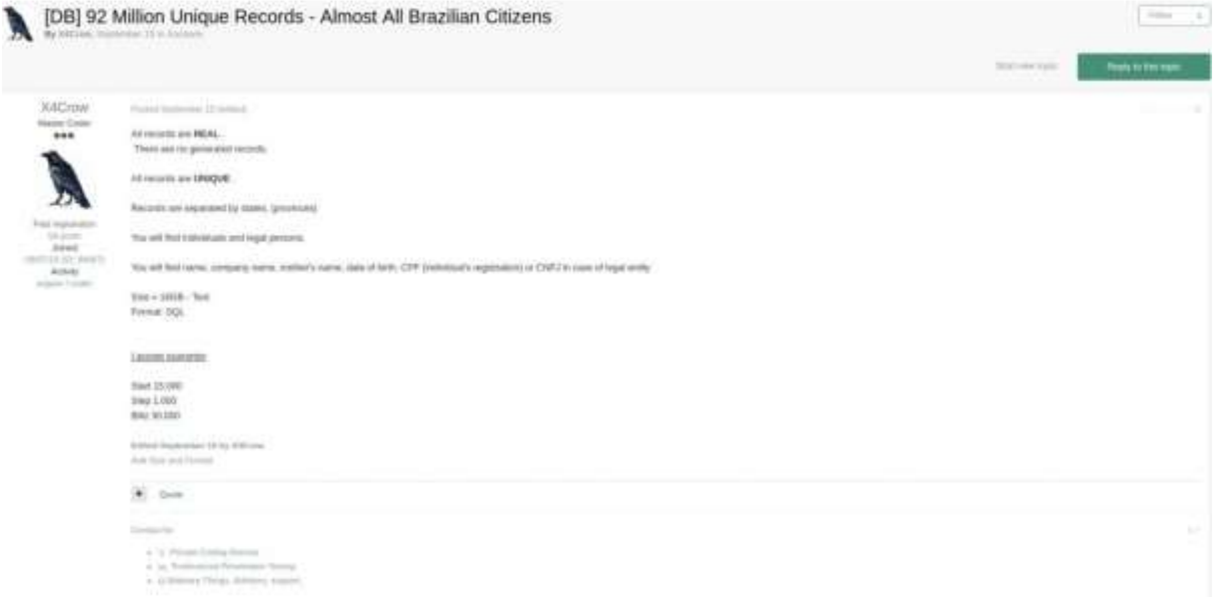
The auction is present on multiple restricted-access underground markets where registration is possible based on an invitation from someone in the community or by paying a fee.

A post on one of the forums seen by BleepingComputer informs that the database is 16GB large, in SQL format. The starting price for the auction is $15,000 with a step up bid of $1,000.

According to the seller, registered as X4Crow, the records are separated per province and include names, dates of birth, and taxpayer ID (CPF - Cadastro de Pessoas Físicas) of individuals. The database also has taxpayer details about legal entities, or the CNPJ (Cadastro Nacional da Pessoa Jurídica), it is stated in the post.

BleepingComputer received a sample of the database and was able to verify that the information on individuals is accurate and also included the mother's name, and gender. We used the CPF lookup service on the Brazilian Federal Revenue website, which also provides the year of death in the case of deceased persons.

Although the origin of the cache is not revealed in the seller's announcement, BleepingComputer was told that it is a government database. X4Crow says that it contains 92 million unique records that cover "almost all Brazilian citizens."



[DB] 92 Million Unique Records - Almost All Brazilian Citizens

By X4Crow, September 15 in Auctions

Posted September 15 (edited)

All records are **REAL**.
There are no generated records.

All records are **UNIQUE**.

Records are separated by states. (provinces)

You will find individuals and legal persons.

You will find name, company name, mother's name, date of birth, CPF (individual's registration) or CNPJ in case of legal entity

Size = 16GB - Text
Format: SQL

Escrow guarantee

Start 15.000
Step 1.000
Blitz 90.000

Edited September 16 by X4Crow
Add Size and Format

Contacts:

- [illegible]
- [illegible]
- [illegible]

Auction posted by the seller

This is highly unlikely since Brazil's population in 2010 had over 190 million people and estimates for 2019 increase that number to more than 210 million. The availability of taxpayer numbers, though, suggests that the records belong to employed citizens.

Multiple statistics estimate that there are around 93 million Brazilians employed, adding weight to this theory.

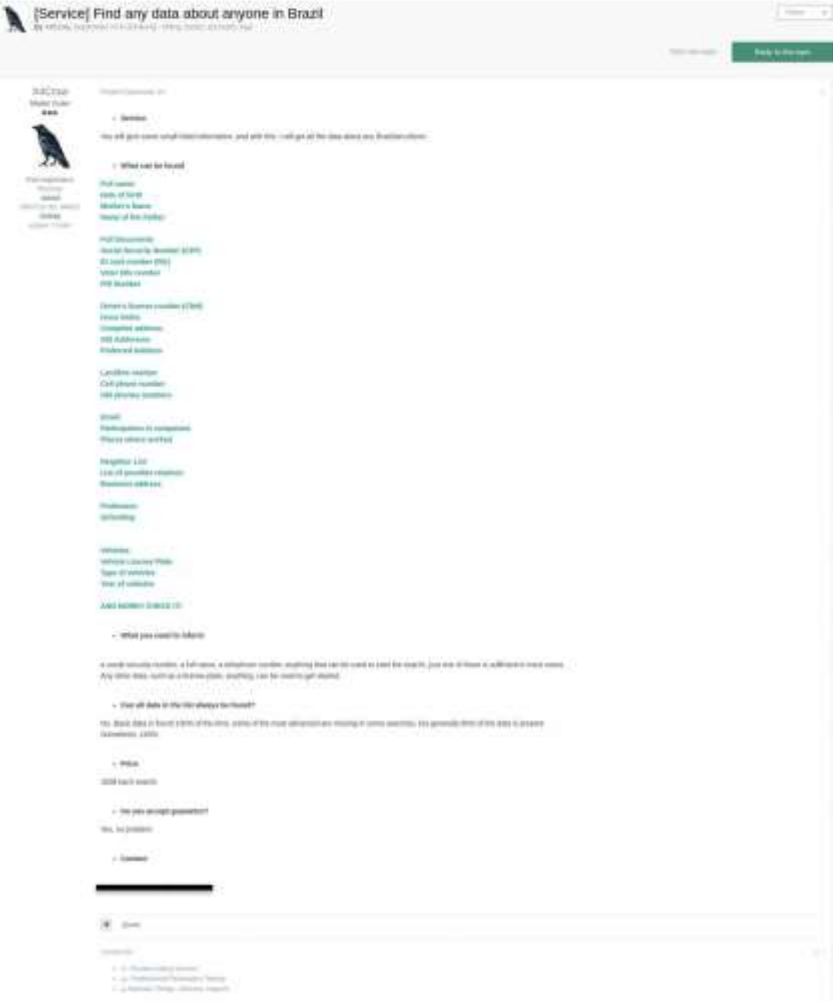
Search service available

From the information we received, the seller may not have received a single bid. However, they also count on making money from another service that promises to return rich information on Brazilian citizens starting from just a few details.

Using input as little as a full name, taxpayer ID, or phone number, X4Crow claims to be able to retrieve data available in national identification documents (ID card, driver's license).

Apart from this, the seller claims that the report may include phone numbers (mobile and landline), old addresses, email address, profession, education level, possible relatives, neighbors, license plates, and vehicle(s).

There is no guarantee that all the details will be retrieved for all individuals but the report may provide, on average, 80% of the specifics listed above.



[Service] Find any data about anyone in Brazil

X4Crow

- Service

[illegible]

- What can be found

Full name
Date of birth
Mother's Name
Name of the Father

Full Documents
Social Security Number (CPF)
ID card number (RG)
Voter title number
PIS Number

Driver's license number (CNH)
[illegible]
Complete address
All Addresses
Preferred Address

Landline number
Cell phone number
All phones numbers

Email
Participations in companies
Places where worked

Neighbor List
List of possible relatives
Business address

Profession
Schooling

Vehicles
Vehicle License Plate
Type of vehicles
Year of vehicles

AND MORE [illegible]

- What you need to inform

[illegible]

- Can all data in the list always be found?

[illegible]

- Price

[illegible] each search

- Do you accept guarantor?

Yes, no problem

- Contact

[redacted]

Quote

Available information for sale

On a freely accessible forum, X4Crow said that they can also get data on any company and its corporate structure. The price for fetching all this is $150, although they offered occasional discounts of $50.

This service may rely only partially on the database they want to sell, an independent security consultant told BleepingComputer. They likely have other data sets to scour for the information.

Not a stranger to cybercrime

Although they don't seem to have long track in the field, X4Crow definitely has enough knowledge of cybercriminal activity to clue others in on how they can solve an issue.

From discussions we've seen X4Crow engage in, they appear to be well informed about various types of operations. They offered possible solutions/advice to problems described by fellow forum members. Some of the topics referred to lateral movement in a LAN and phishing.

One of their profiles lists services that include programming, penetration testing, and malware-related advice and support. Selling databases is not among their skill set, which requires knowing what the market wants and providing it for the right price, typically a fixed one, not an auction.

Source: https://www.bleepingcomputer.com/news/security/details-of-92-million-brazilians-auctioned-on-underground-forums/

4. Tools and Tactics of the Sodinokibi Ransomware Distributors

Using a network of honeypots, researchers from McAfee examined the tools and tactics used by the Sodinokibi Ransomware (REvil) affiliates to infect their victims with ransomware and compromise other machines on the network.

As part of the Sodinokibi ransomware-as-a-service, ransomware executables are tagged with an affiliate's IDs and sub IDs in order to track who infected the victim and which affiliate should earn a commission for a payment.

At the same time, these affiliate IDs allow researchers to track their behavior as well and paint a picture of how they infect their victims and spread laterally throughout a network.

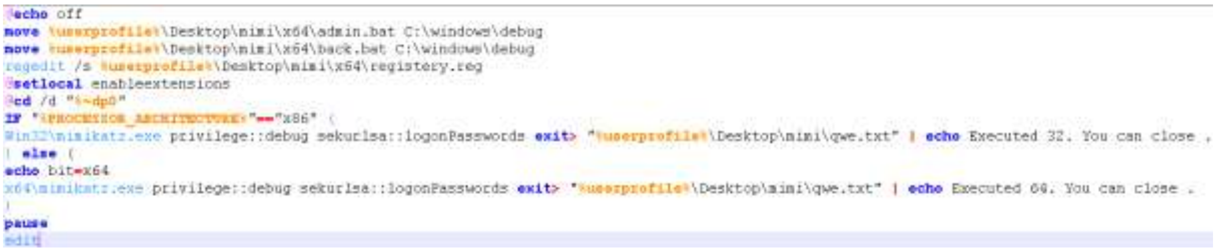
Monitoring the attackers

In a new report shared with BleepingComputer before publication, the McAfee Advanced Threat Research team used a global network of Remote Desktop Protocol (RDP) honeypots was used to track the activities of three Sodinokibi affiliate groups.

These affiliates, known as Group 1, affiliate #34, and affiliate #19, all initially compromised a system via RDP and then use this foothold to try and compromise the rest of the network.

To attempt to spread laterally throughout the network, all of the affiliates used mass port scanning tools to find accessible RDP servers and then used the NLBrute RDP brute forcing tool with custom password lists to try and gain access to servers.

Affiliate #34 and #19, though, showed more skillful tactics such as using custom Mimikatz batch files to harvest network credentials credentials, custom scripts to erase Windows event viewer logs, and the creation of hidden users.



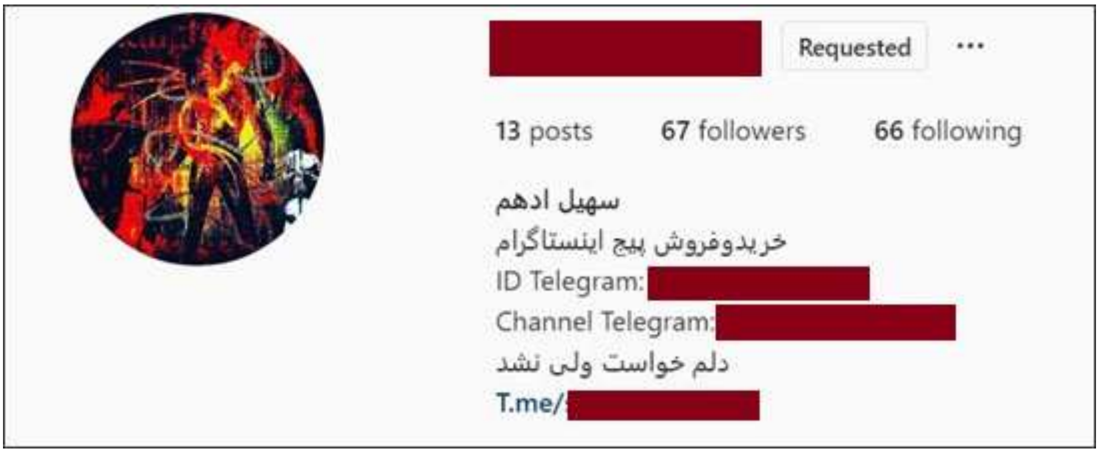
```
@echo off
move %userprofile%\Desktop\mimi\x64\admin.bat C:\windows\debug
move %userprofile%\Desktop\mimi\x64\back.bat C:\windows\debug
regedit /s %userprofile%\Desktop\mimi\x64\registery.reg
@setlocal enableextensions
@cd /d "%~dp0"
IF "%PROCESSOR_ARCHITECTURE%"=="x86" (
Win32\mimikatz.exe privilege::debug sekurlsa::logonPasswords exit> "%userprofile%\Desktop\mimi\qwe.txt" | echo Executed 32. You can close .
) else (
echo bit=x64
x64\mimikatz.exe privilege::debug sekurlsa::logonPasswords exit> "%userprofile%\Desktop\mimi\qwe.txt" | echo Executed 64. You can close .
)
pause
edit
```

Custom Mimikatz batch files

Affiliate #19 appears to be the most skillful, or thorough, as McAfee saw them attempt to utilize local exploits to gain administrative access on a compromised computer. By gaining access to an administrative account, the affiliate could more easily push out and execute the ransomware on other machines on the Windows domain.

In addition to the Sodinokibi Ransomware payload, Affiliate #34 also dropped cryptomining payloads such as MinerGate and XMRig.

From one of the MinerGate configuration files, McAfee was able to learn the email address used by one of the attackers and track it down to a possible Persian-speaking member of an RDP hacking crew.



[redacted] Requested •••

13 posts 67 followers 66 following

سهیل ادهم
خریدوفروش پیج اینستاگرام
ID Telegram: [redacted]
Channel Telegram: [redacted]
دلم خواست ولی نشد
T.me/ [redacted]

Persian-speaking member's social media account

"Based on our analysis, this individual is likely part of some Persian-speaking credential cracking crew harvesting RDP credentials and other types of data. The individual is sharing information related to Masscan and Kport scan results for specific countries that can be used for brute force operations."

Everything search engine deployed to index documents

An interesting program that was deployed by affiliate #34 is the Everything file indexing software.

When installed, Everything will index all of the file and folder names found on the computer so that a user can quickly search for files based on an entered keyword. It is also possible to search for content within the indexed files, though at a much slower speed.

While McAfee was unable to monitor what searches were performed, they did state that a full index of the filesystem was completed.

"Unfortunately we haven’t got information that the actor was searching for specific keywords we did see a complete index of the filesystem," McAfee's John Fokker, Head of Cyber Investigations, told BleepingComputer via email.

BleepingComputer believes that the Everything software was installed so that the attackers could use it to search for sensitive files based on their names.

For example, if files contain the words "secret", "password", "bank accounts", "classified", "military", "10-Q", "10-K", etc, the attackers could then exfiltrate these files in their unencrypted form in order to steal trade secrets, steal financial information, get insider information for stock trades, or threaten to release the documents unless a ransom is payed.

While not common, in the past stolen data of a sensitive nature has been used to threaten victims to make a payment or the data would be publicly released.

The use of Everything as part of a ransomware deployment is an interesting tactic and one that all enterprise customers should be concerned about due to the increased risk of data theft.

Source: https://www.bleepingcomputer.com/news/security/tools-and-tactics-of-the-sodinokibi-ransomware-distributors/

5. Hackers Breach Avast Antivirus Network Through Insecure VPN Profile

Hackers accessed the internal network of Czech cybersecurity company Avast, likely aiming for a supply chain attack targeting CCleaner. Detected on September 25, intrusion attempts started since May 14.

Following an investigation, the antivirus maker determined that the attacker was able to gain access using compromised credentials via a temporary VPN account.

Tiptoeing to higher privileges

From the information collected this far, the attack appears to be "an extremely sophisticated attempt," says Jaya Baloo, Avast Chief Information Security Officer (CISO).

Avast refers to this attempt by the name 'Abiss' and says that the threat actor behind it exercised extreme caution to avoid being detected and hide the traces of their intention.

Logs of the suspicious activity show entries on May 14 and 15, on July 24, on September 11, and on October 4.

The intruder connected from a public IP address in the U.K. and took advantage of a temporary VPN profile that should no longer have been active and was not protected with two-factor authentication (2FA).

In a statement today, Jaya Baloo says that the company received an alert for "a malicious replication of directory services from an internal IP that belonged to our VPN address range;" this had been dismissed as a false positive, though.

However, it turned out that the user whose credentials had been compromised did not have the permissions of a domain administrator, indicating that the attacker achieved privilege escalation.

The logs further showed that the temporary profile had been used by multiple sets of user credentials, leading us to believe that they were subject to credential theft.

CCleaner updates vetted for release

Suspecting CCleaner as the targeted asset, Avast on September 25 stopped the upcoming updates for the software and started to check prior releases for malicious modification.

To ensure that no risk comes to its users, the company re-signed an official CCleaner release and pushed it as an automatic update on October 15. That release updated users still on versions 5.57 through 5.62 of the product so they could benefit from "its enhanced security and improved performance."

Furthermore, the old certificate was revoked, says in a statement today Jaya Baloo, Avast Chief Information Security Officer (CISO).

"It was clear that as soon as we released the newly signed build of CCleaner, we would be tipping our hand to the malicious actors, so at that moment, we closed the temporary VPN profile. At the same time, we disabled and reset all internal user credentials. Simultaneously, effective immediately, we have implemented additional scrutiny to all releases." Jaya Baloo

It is unclear if this is the same threat actor responsible for the CCleaner supply chain attack disclosed in 2017. Chances are low for discovering a connection between these two incidents.

The company tracked the intruder by keeping the VPN profile active and monitoring the access going through it until mitigation actions could be deployed.

Law enforcement has been notified of the intrusion and an external forensics team assisted Avast's efforts to verify the collected data.

Avast will continue to review and monitor its networks for better detection and quicker response in the future.

Investigation in the actions of this threat actor will also continue, to gain intelligence on how they work. Some details, like the IP addresses used for the intrusion, have been shared with law enforcement and the cybersecurity community. The information is marked as TLP:RED, which means that it cannot be shared.

Update [10.21.2019]: When CCleaner 5.63 came out on October 15, BleepingComputer sought comments from Avast about the reason and benefits of the update since it was an unexpected move. The company delayed responding to our questions at the time.

CCleaner General Manager David Peterson explains in a blog post today that the reason for automatically updating all CCleaner installations since 5.57 to the current latest version was a preventative measure to ensure that all users run a genuine release.

"We took these steps preventatively as our investigation is continuing, but we wanted to eliminate the risk of fraudulent software being delivered to our users. Since we have indications that the attempts to infiltrate our systems began in May this year, we automatically updated users on builds released after this time to ensure their safety."

Source: https://www.bleepingcomputer.com/news/security/hackers-breach-avast-antivirus-network-through-insecure-vpn-profile/

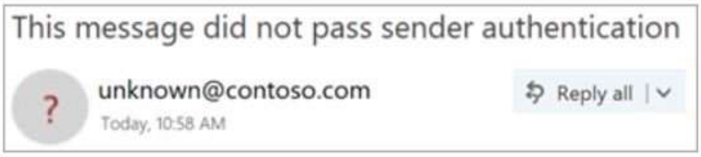
6. Office 365 Now Warns About Suspicious Emails with Unverified Senders

Microsoft is currently rolling out a new Office 365 feature dubbed 'Unverified Sender' and designed to help users identify potential spam or phishing emails that reach their Outlook client's inbox.

"*Unverified sender is a new Office 365 feature that helps end-users identify suspicious messages in their inbox,*" says the company on the new feature's Microsoft 365 roadmap entry.

"*In order to help customers identify suspicious messages in their inbox, we've added an indicator that demonstrates Office 365 spoof intelligence was unable to verify the sender.*"

The new indicators will be shown in the user's Outlook inbox for messages where the client couldn't verify the sender's identity using email authentication techniques.



This message did not pass sender authentication

unknown@contoso.com

Today, 10:58 AM

If Unverified Sender is toggled on, all emails that come from unverified sender will have the sender's photo or initials replaced with a question mark in the people card as shown above. This will make it easier for Office 365 users to quickly detect potential phishing attacks or potential sender spoofing attempts says Microsoft.

When one of the emails in your inbox gets marked by the Office 365 Unverified Sender feature, you should be careful while interacting with them as they could be malicious or being sent by a potential attacker that spoofed the sender.

Microsoft also states that emails will not be analyzed using the Unverified Sender filter if the user has set the sender as a 'Safe Sender' in their inbox or the messages were delivered to the user's Outlook inbox via an admin allow list, including Email Transport Rules (ETRs), Safe Domain List (Anti-Spam Policy), or Safe Sender List.

The suspicious email indicator is going to be automatically tagged with a question mark if the message did not "pass either SPF or DKIM authentication and receive either a DMARC pass, or a composite authentication pass from Office 365 Spoof Intelligence."

Microsoft provides more information on how to properly validate outbound email sent from Office 365 custom domains using DKIM and on how to prevent spoofing by configuring SPF in Office 365.

2048-bit DKIM key sizes

Redmond is also rolling out increased DKIM key sizes to 2048-bit from the current 1024-bit size for all Office 365 customers during October, to enhance security in all environments.

"*If you already have your default or custom domain DKIM enabled in Office 365, it will automatically be upgraded from 1024-bit to 2048-bit at your next DKIM configuration rotation date,*" says Microsoft.

Administrators can manage DKIM configuration using the Get-DkimSigningConfig cmdlet via Exchange PowerShell Admin sessions.

This new 2048-bit key takes effect on the RotateOnDate, and will send emails with the 1024-bit key in the interim. After four days, you can test again with the 2048-bit key (that is, once the rotation takes effect to the second selector). — Microsoft

Both the 2048-bit DKIM key sizes and the new Office 365 Unverified Sender feature are rolling out now and, as a result, might not be available yet for all users.

Microsoft is also rolling out better malicious emails analysis capabilities for Office 365, announced back in late July and allowing Microsoft 365 admins with Threat Explorer access to preview and download malicious emails for further investigation.

Redmond also urged Microsoft Office 365 administrators and users to not bypass the built-in spam filters in a support document published in June and provided guidelines for cases when this can't be avoided.

Source: https://www.bleepingcomputer.com/news/microsoft/office-365-now-warns-about-suspicious-emails-with-unverified-senders/

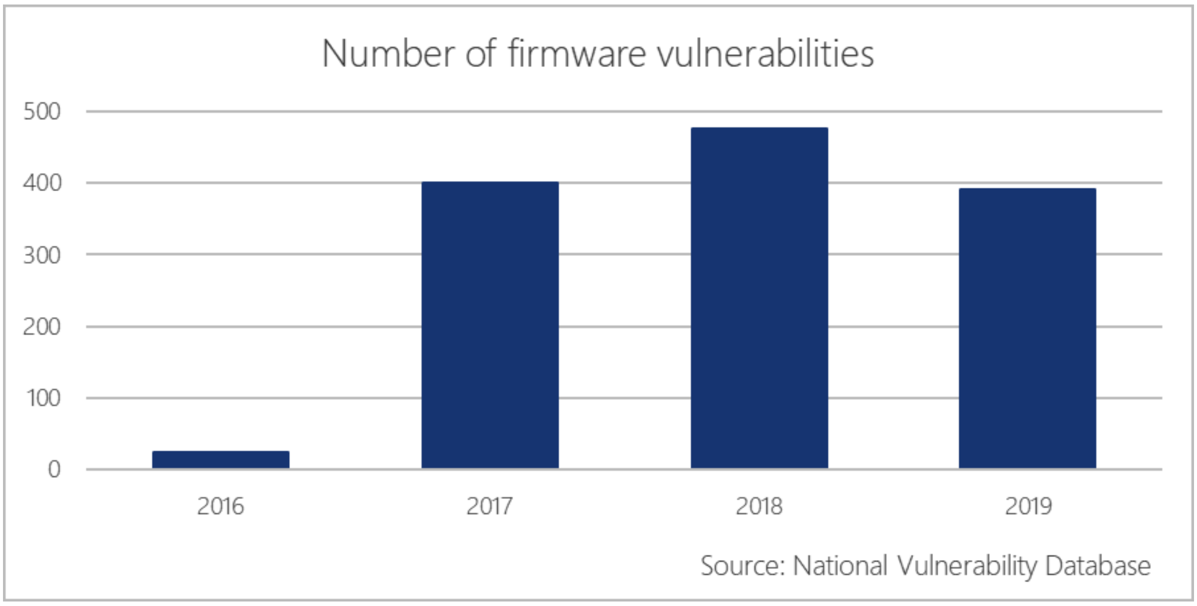
7. New Windows 10 Secured-Core PCs Block Firmware-Level Attacks

Microsoft introduced a new range of devices called Secured-core PCs which come with built-in protection against firmware attacks that have been increasingly used by state-sponsored hacking groups.

The APT28 cyber-espionage group (also tracked as Sednit, Fancy Bear, Strontium, and Sofacy), for instance, used a Unified Extensible Firmware Interface (UEFI) rootkit dubbed LoJax as part of its 2018 operations.

This gave the attackers persistence on the compromised computers not only against operating system reinstallation but also against attempts of replacing the hard drives on infected machines.

"*These devices are designed specifically for industries like financial services, government, and healthcare, and for workers that handle highly-sensitive IP, customer or personal data, including PII as these are higher-value targets for nation-state attackers,*" says Microsoft.



Source: National Vulnerability Database

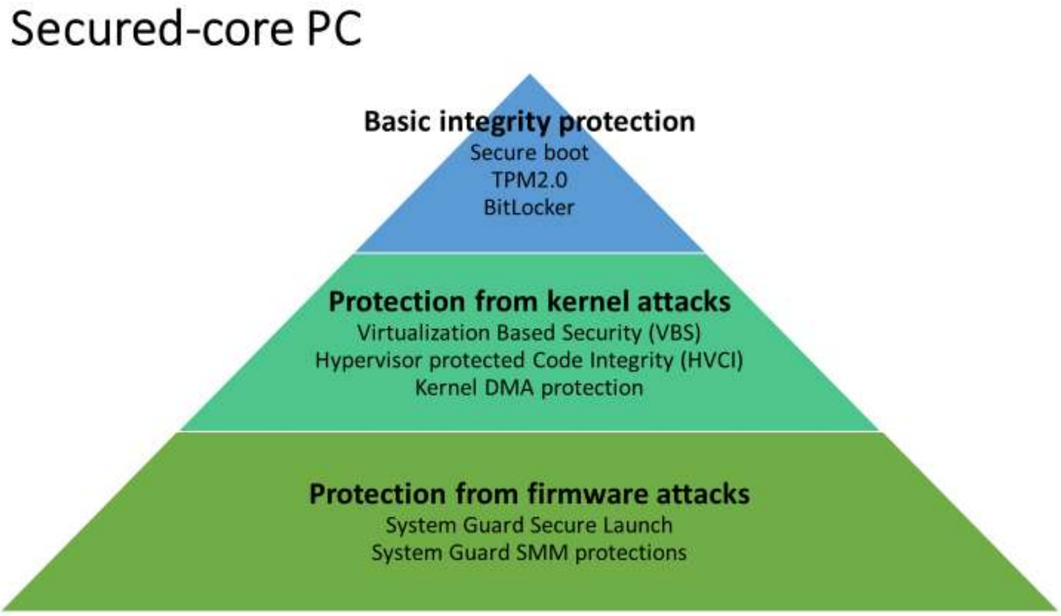
Layers of built-in protection

This new type of secured devices is designed to closely meet an array of software and hardware requirements that will "apply the security best practices of isolation and minimal trust to the firmware layer, or the device core, that underpins the Windows operating system."

Given the deep integration between the hardware, firmware, operating system, and identity features built-in, organized as layers designed to prevent attackers from successfully compromising the system, Secured-core PCs protect from increasing risks of targeted attacks and highly advanced threats out of the box.

"These devices, created in partnership with our OEM and silicon partners, meet a specific set of device requirements that apply the security best practices of isolation and minimal trust to the firmware layer, or the device core, that underpins the Windows operating system," Microsoft adds.

Secured-core PCs come as a solution for the number of increasing firmware vulnerabilities that attackers can exploit to bypass a Windows machine's Secure Boot and the lack of visibility at the firmware level present in today's endpoint security solutions.


Secured-core PC
Basic integrity protection
Secure boot
TPM2.0
BitLocker
Protection from kernel attacks
Virtualization Based Security (VBS)
Hypervisor protected Code Integrity (HVCI)
Kernel DMA protection
Protection from firmware attacks
System Guard Secure Launch
System Guard SMM protections

To protect Secured-core PC users against it, Microsoft and its OEM partners introduced the following array of built-in requirements:

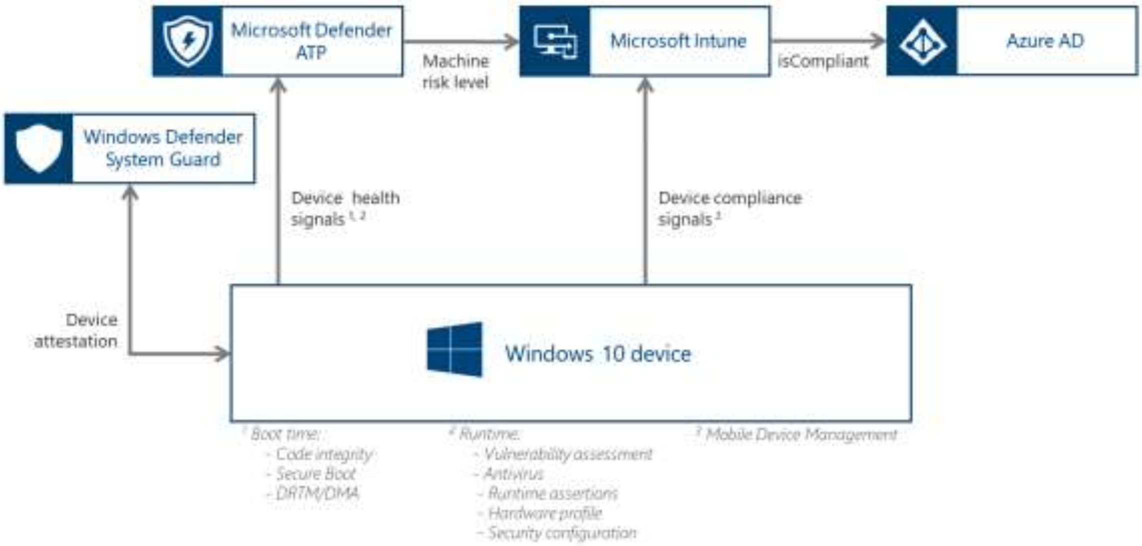
- **Loading Windows securely:** Enabled with Hypervisor Enforced Integrity, a Secured-core PC only starts executables signed by known and approved authorities. Also, the hypervisor sets and enforces permissions to prevent malware from attempting to modify the memory and made executable
- **Firmware protection:** System Guard Secure Launch uses the CPU to validate the device to boot securely, preventing advanced firmware attacks
- **Identity protection:** Windows Hello allows you to sign-in without a password, Credential Guard leverages VBS to prevent identity attacks
- **Secure, hardware-isolated operating environment:** Uses the Trusted Platform Module 2.0 and a modern CPU with dynamic root of trust measurement (DRTM) to boot up your PC securely and minimizes firmware vulnerabilities

These provisions allow Secured-core PCs to boot securely, protect themselves from firmware vulnerabilities, shield their operating system from attacks, prevent unauthorized access, and secure their users' identity and domain credentials.

Windows Defender System Guard is a key requirement

"*Using new hardware capabilities from AMD, Intel, and Qualcomm, Windows Defender now implements System Guard Secure Launch as a key Secured-core PC device requirement to protect the boot process from firmware attacks,*" says Microsoft.

"*System Guard uses the Dynamic Root of Trust for Measurement (DRTM) capabilities that are built into the latest silicon from AMD, Intel, and ARM to enable the system to leverage firmware to start the hardware and then shortly after re-initialize the system into a trusted state by using* *the OS boot loader and processor capabilities to send the system down a well-known and verifiable code path."*



According to Microsoft's announcement, all Secured-core PCs will come with the necessary operating system and hardware support for Windows Defender System Guard's capabilities.

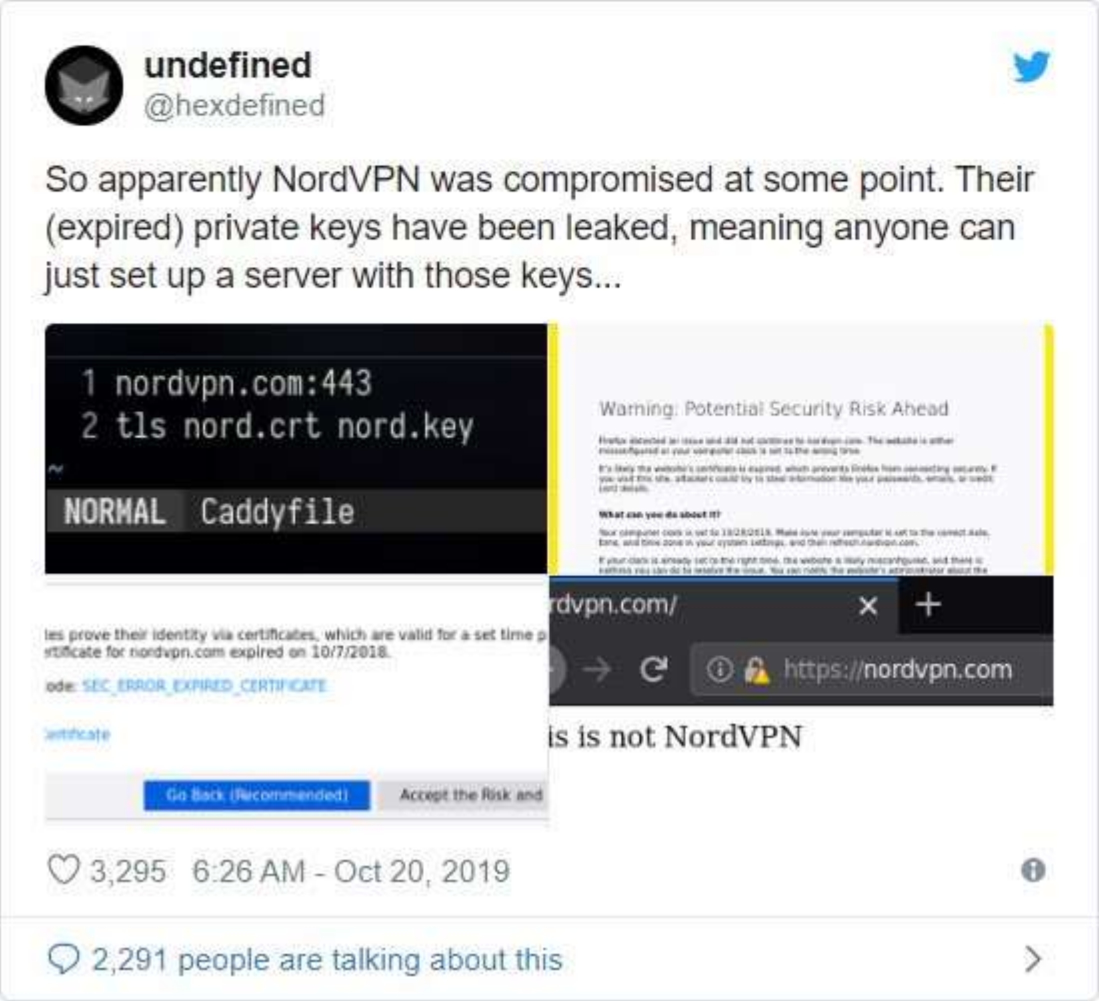
Customers can find more info on devices that are Secured-core PC-verified on this dedicated web page or by going to Dell, Dynabook, HP, Lenovo, and Panasonic, the OEMs involved in this new initiative.

Source: https://www.bleepingcomputer.com/news/security/new-windows-10-secured-core-pcs-block-firmware-level-attacks/

8. Hacker Breached Servers Belonging to Multiple VPN Providers

Servers belonging to the NordVPN and TorGuard VPN companies were hacked and attackers stole and leaked the private keys associated with certificates used to secure their web servers and VPN configuration files.

Over the weekend, security researcher @hexdefined tweeted that NordVPN, of which we are an affiliate, was compromised as the private keys for their web site certificate were publicly leaked on the Internet.



undefined
@hexdefined

So apparently NordVPN was compromised at some point. Their (expired) private keys have been leaked, meaning anyone can just set up a server with those keys...

```
1 nordvpn.com:443
2 tls nord.crt nord.key
~
NORMAL  Caddyfile
```

Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to nordvpn.com. The website is either misconfigured or your computer clock is set to the wrong time.

It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

Your computer clock is set to 10/28/2019. Make sure your computer is set to the correct date, time, and time zone in your system settings, and then refresh nordvpn.com.

If your clock is already set to the right time, the website is likely misconfigured, and there is nothing you can do to resolve the issue. You can notify the website's administrator about the

ies prove their identity via certificates, which are valid for a set time p
rtificate for nordvpn.com expired on 10/7/2018.

ode: SEC_ERROR_EXPIRED_CERTIFICATE

ertificate

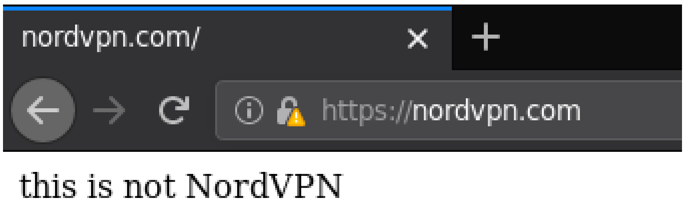
is is not NordVPN

3,295 6:26 AM - Oct 20, 2019

2,291 people are talking about this

While this certificate is now expired, if this certificate was used prior to expiration it could have allowed an attacker to create a convincing site that impersonates NordVPN through the use of their certificate. More advanced attackers could have also used this key to perform man in the middle attack (MiTM) to listen in on encrypted communications.

To illustrate how a fake site could have been made using NordVPN's certificate, hexdefined shared this image.



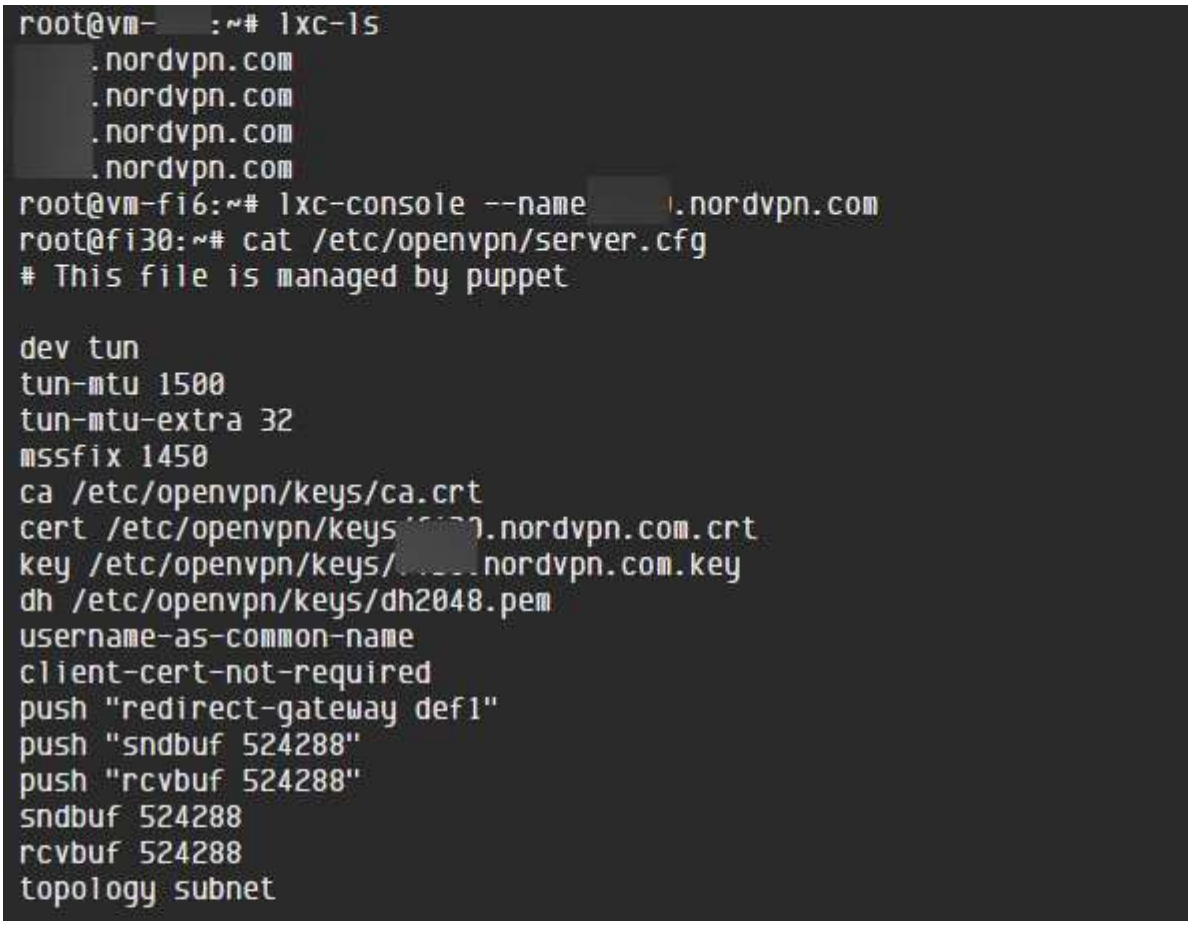
this is not NordVPN

Fake NordVPN Site

Servers for NordVPN, TorGuard, and possibly VikingVPN hacked

In addition to the web site certificate, the Twitter account for OpenVPN provider CryptoStorm.is posted a link to an 8chan post where a person hacker claimed to have full root access to servers belonging to NordVPN, TorGuard, and VikingVPN.

This allowed the attacker to steal OpenVPN keys and configuration files as shown by the image below of the NordVPN hack. CryptoStorm.is stated that by stealing these keys, it could have allowed an attacker to decrypt traffic at the time of the hack.



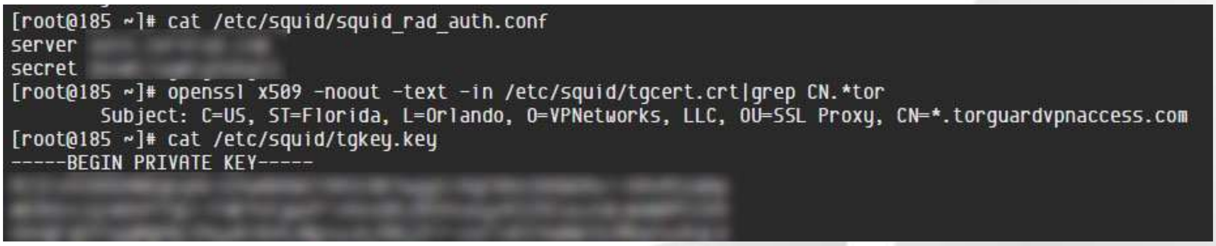
```
root@vm-[redacted]:~# lxc-ls
[redacted].nordvpn.com
[redacted].nordvpn.com
[redacted].nordvpn.com
[redacted].nordvpn.com
root@vm-fi6:~# lxc-console --name [redacted].nordvpn.com
root@fi30:~# cat /etc/openvpn/server.cfg
# This file is managed by puppet

dev tun
tun-mtu 1500
tun-mtu-extra 32
mssfix 1450
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys[redacted].nordvpn.com.crt
key /etc/openvpn/keys/[redacted]nordvpn.com.key
dh /etc/openvpn/keys/dh2048.pem
username-as-common-name
client-cert-not-required
push "redirect-gateway def1"
push "sndbuf 524288"
push "rcvbuf 524288"
sndbuf 524288
rcvbuf 524288
topology subnet
```

NordVPN Hack

Unfortunately, NordVPN was not alone.

This same 8chan post also links to the output of hacks on a server belonging to TorGuard where a Squid proxy certificate and OpenVPN keys and configuration files were stolen.



```
[root@185 ~]# cat /etc/squid/squid_rad_auth.conf
server [redacted]
secret [redacted]
[root@185 ~]# openssl x509 -noout -text -in /etc/squid/tgcert.crt|grep CN.*tor
        Subject: C=US, ST=Florida, L=Orlando, O=VPNetworks, LLC, OU=SSL Proxy, CN=*.torguardvpnaccess.com
[root@185 ~]# cat /etc/squid/tgkey.key
-----BEGIN PRIVATE KEY-----
[redacted]
```

TorGuard Hack

Finally, a third link goes to an alleged hack of a server owned by VikingVPN where the attacker stole OpenVPN keys and configuration files.

NordVPN and TorGuard issue statements

While VikingVPN has not responded to any of our queries, both NordVPN and TorGuard have issued statements.

According to a statement issued by NordVPN, the attacker was able to gain access to their servers through an insecure remote management tool deployed by their datacenter.

"We became aware that on March 2018, one of the datacenters in Finland we had been renting our servers from was accessed with no authorization. The attacker gained access to the server by exploiting an insecure remote management system left by the datacenter provider while we were unaware that such a system existed. The server itself did not contain any user activity logs; none of our applications send user-created credentials for authentication, so usernames and passwords couldn't have been intercepted either. The exact configuration file found on the internet by security researchers ceased to exist on March 5, 2018. This was an isolated case, and no other datacenter providers we use have been affected."

NordVPN further states that the TLS key taken by the attacker was already expired and contrary to what Cryptostorm.io stateed, no VPN traffic could have been decrypted at the time of the attack.

In a statement by TorGuard, the VPN provider states that as they utilize "secure PKI management", none of their VPN users were affected by this breach and their CA key was not stolen as it was not present on the compromised server

"TorGuard was the only one using secure PKI management, meaning our main CA key was not on the affected VPN server."

They further state that the stolen TLS certificate for *.torguardvpnaccess.com is for a "squid proxy cert which has not been valid on the TorGuard network since 2017."

While, they do not go into details as to how the server was hacked, they do state that there was "repeated suspicious activity" at the reseller they were renting the server from and that they no longer work with them.

TorGuard further stated that the compromised server is related to a lawsuit they filed against NordVPN in 2019.

"TorGuard first became aware of this disclosure during May of 2019 and in a related development we filed a legal complaint against NordVPN in the Middle District of Florida on June 27, 2019."

More information about this lawsuit can be read at TorGuard and NordVPN.

As previously stated, VikingVPN has not responded to our queries regarding their server.

Never advertise that you can't be hacked

While using these certificates to perform a MiTM attack against TorGuard and NordVPN visitors would be difficult, one thing we have learned over time is that nothing is unhackable.

In fact, anyone who states they are unhackable or are immune to hackers are quickly proven false.

This was clearly shown, as the unveiling of this VPN hacking escapade came just hours after NordVPN decided to run a Twitter ad that stated "Ain't no hacker can steal your online life. (If you use VPN). Stay safe."

This ad was taken down soon after.

Disclosure: BleepingComputer is an affiliate of NordVPN.

Source: *https://www.bleepingcomputer.com/news/security/hacker-breached-servers-belonging-to-multiple-vpn-providers/*

9. Credential-Stuffing Attacks Are Just the Tip of the Iceberg

It’s no secret that passwords just aren’t very secret these days. Poor password hygiene and an overwhelming volume of digital accounts has influenced far many consumers to routinely reuse passwords across multiple accounts. As you might imagine, businesses have been hearing more and more about credential-stuffing attacks in the news.

Credential-stuffing attacks happen when a malicious actor obtains a list of stolen usernames and passwords and tests them at various other sites using a bot. The credentials themselves could come from anywhere: data breaches, phishing attacks, etc. Because so many consumers reuse the same credentials over and over again, a username and password stolen from a data breach at a major retailer could help a fraudster access that consumer’s online accounts.

To Detect Credential-Stuffing Attacks, Look for the Bots

While businesses can’t reasonably force a user to not reuse a password from another site, bot detection solutions can help detect and mitigate credential-stuffing activity. Detecting bot activity — and thereby reducing credential stuffing attacks — is helpful. Bot detection in the application layer can also help reduce denial-of-service-attacks. Bot detection that is further down, analyzing things such as behavioral biometrics, can recognize additional markers for scripted attacks and nonhuman activity.

Account Takeover: Addressing the Root Problem

Despite its utility, focusing efforts solely on bot detection to address credential-stuffing attacks is a bit like taking an aspirin for a headache when the true problem is a brain tumor. Credential stuffing is only step one; generally speaking, the ultimate goal of these attacks is account takeover. That is when a malicious actor actually gains access to an account and can begin to monetize it.

Holistic Fraud and Authentication Strategies

Business leaders should consider holistic, multilayered strategies for dealing with credential stuffing attacks and account takeovers. This means detecting bot activity and understanding the full context of the user and their activity on a site or app. By examining the user's behavior, device, network and other behind-the-scenes factors, organizations can get a true understanding of the risk of each of their site visitors — including those that are nonhuman — and modify their authentication strategy accordingly, adapting the digital experience to match the risk.

Just as credential-stuffing attacks are indicative of the much larger issue of account takeover, this adaptive authentication is a small part of a much larger effort to actually improve the digital experience for low-risk users. This is because businesses can modify the authentication process for low-risk users as well — perhaps even embracing a passwordless strategy. Thus, organizations can move toward a world where they not only detect credential-stuffing attacks, but move the rest of us slowly away from the problem that created them in the first place.

Source: http://feedproxy.google.com/~r/SecurityIntelligence/~3/oz_JS2a_L1Y/

10. Malicious Apps on Alexa or Google Home Can Spy or Steal Passwords

Google and Amazon smart speakers can be leveraged to record user conversation or to phish for passwords through malicious voice apps, security researchers warn.

Unless the two companies take measures to improve the review process and the restrictions for apps integrating with their smart devices, malicious developers could exploit the weakness to capture audio from users.

Modified intents

Called 'skills' for Amazon Alexa and 'actions' for Google Home, voice apps for these smart speakers are activated using a phrase ('invocation name') designated by the developer to start the app, which is typically the name of the app.

"*Hey Google/Alexa, turn on my Horoscope*" - invoking the Horoscope app

Functions of a skill or an action are called via an 'intent' - a set phrase that can have slot values for custom variables. In many cases, these reach the developer's server.

"*Tell me my horoscope for today*" - intent with the slot value '*today*'

Users can tell the smart speaker to stop a skill or action, but security researchers at Germany's Security Research Labs demonstrated that an app can bypass this intent and keep on listening.

They show that a malicious app behaving this way can receive the security approval stamp from both Google and Amazon and put user privacy at risk as the converted audio reaches a third-party server.

A malicious Amazon skill used for eavesdropping could come with a modified deactivation intent that does not turn it off. Instead, the session could stay open for a defined period.

SRLabs achieved this by changing the 'stop' intent to keep the skill running instead of turning it off. Users will still hear the 'Goodbye' message signaling the end of the skill, though.

To keep the speaker silent during the eavesdropping session, the researchers added the Unicode character sequence ". " (U+D801, dot, space) after the intent.

The sequence cannot be pronounced and the speaker will stay quiet for a few more seconds while the malicious app listens to the conversation. The eavesdrop time can be extended by adding the characters multiple times.

With a second intent triggered by specific words, an attacker can record sentences as slot values. This would act as a backup method to spy on users.

Eavesdropping on Google Home

Actions for Google Home could monitor for user speech for much longer, because of its design. By putting the user in a loop, the device sends a continuous stream of recognized speech to the attacker without making a peep to signal its activity.

The speaker is designed to wait for about nine seconds for vocal input and stops for a brief moment. This is repeated three times before the action is deactivated. When speech is detected, the count is reset.

This hack is possible by changing the main intent to end with the 'Bye' earcon sound, normally used to mark the end of a voice app.

Multiple 'noInputPrompts' with SSML element or the unpronounceable Unicode character sequence will silence the speaker silent while the eavesdropping action continues its speech-to-text activity.

Changing the malicious intent occurred after the apps passed the initial review from Amazon and Google, and the modifications did not trigger a second verification.

Phishing the password

Using similar tricks, SRLabs demonstrated another attack scenario that could fool users into giving up their passwords.

For this purpose, the silence given by the Unicode characters is cut short to play a phishing message.

"An important security update is available for your device. Please say start update followed by your password," could pass for a genuine request. However, neither Google nor Amazon asks for passwords this way.

Anything the user says after this message is turned into text and delivered to the attacker's server. SRLabs created two additional videos to show how this would work.

The German researchers recommend that unpronounceable characters be removed and allowing sensitive output that could be used to extract secret information should be considered more carefully.

Source: https://www.bleepingcomputer.com/news/security/malicious-apps-on-alexa-or-google-home-can-spy-or-steal-passwords/

11. Open Redirect Bug in Bridge Theme Plugin Opens Admins to Spearphishing

The Qode Instagram Widget and Qode Twitter Feed both have bugs that could allow redirects to malicious sites.

Two open-redirect vulnerabilities in Bridge, a commercial WordPress theme purchased more than 120,000 times, would allow an attacker to mount spearphishing attacks against site administrators.

An open redirect vulnerability can be used to hide malicious links behind URLs for legitimate domains. For instance, a victim could be sent a link to https://legitimatesite.com/redirect.php?url=https://evilsite.com. If they hover over the link, they see only the legitimatesite.com domain — but if they click on it, they would be taken to evilsite.com without their permission.

“This is commonly used in phishing scams, since a link to a trustworthy site is much more likely to be clicked than a typical phishing domain,” explained researchers at Wordfence, who discovered the vulnerability, in a Tuesday posting. In the case of these specific flaws, “an administrator could receive a link to their own website and be taken to a WordPress login page, not knowing they were redirected to a phishing site built to harvest their credentials.”

The bugs exist in two of theme’s prepackaged helper plugins, called Qode Instagram Widget and Qode Twitter Feed (Qode Interactive is Bridge’s developer). Users are prompted to install these when installing the Bridge theme itself.

Both contain redirect scripts which allow open redirects. For Qode Instagram Widget, a script found at lib/instagram-redirect.php takes the GET parameters redirect_uri and code, and combines them into an eventual redirect location.

The offending code in Qode Twitter Feed is found at lib/twitter-redirect.php and is nearly identical to the Instagram Widget script, researchers said: “Not counting the interchange of ‘URI’ and ‘URL’ in the variable names, the only differences are the additional GET parameters required to trigger the redirect.”

Qode, which said that the scripts were artifacts of a demonstration mode included in the plugins, has released a patch for both plugins, available in version 2.0.2, which can be applied after users update the Bridge theme itself to version 18.2.1. Unfortunately, Wordfence researchers said that applying the patch is far from intuitive, given that the theme update isn’t available via WordPress’s built-in update notification system.

"Updating these plugins first requires users to update the Bridge theme. This is done either by manually downloading and installing an updated copy of the theme from ThemeForest, or by using the Envato Market plugin which also comes bundled with the Bridge theme to update from within the WordPress dashboard," they explained in the posting. "Once the Envato Market plugin is installed, you can open its menu in the dashboard and set up your site's API access to the Envato Marketplace. This will require you to log in to the account you used to purchase the Bridge theme and generate an access token using the steps they provide."

Once Bridge has been updated, the individual plugin entries will show an "Update Required" link.

Users can also simply delete instagram-redirect.php and twitter-redirect.php from their sites, which takes care of the problem – but WordPress users should probably keep their plugins updated anyway given that these are a prime attack vector for cybercriminals.

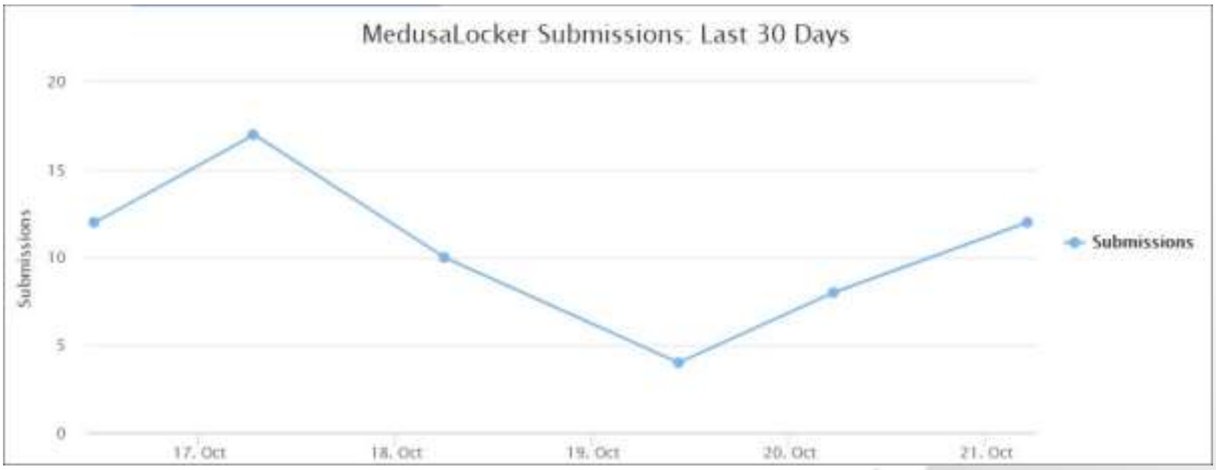
Wordfence researchers said that Qode users aren't very good about patching, with its analysis showing that 38 percent of active Qode Instagram Widget installations haven't been updated in more than two years; that number jumps to 68 percent for Qode Twitter Feed users.

Source: https://threatpost.com/open-redirect-bug-bridge-theme/149437/

12. MedusaLocker Ransomware Wants Its Share of Your Money

A new ransomware called MedusaLocker is being actively distributed and victims have been seen from all over the world. It is not known at this time, how the attacker is distributing the ransomware.

This new ransomware was found by MalwareHunterTeam at the end of September 2019, and while it is not currently known how the ransomware is being distributed, there has been a steady amount of submissions to the ID Ransomware site since then.



ID Ransomware submissions

When the ransomware is installed, it will perform various startup routines in order to prep the computer for encryption.

It will create the Registry value **EnableLinkedConnections** under the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** registry key and set it to **1**. This is done to make sure mapped drives are accessible even in a UAC launched process.

It will also restart the LanmanWorkstation service in order to make sure that Windows networking is running and that mapped network drives are accessible.

It will then look for and terminate the following processes in order to shut down security programs and to make sure all data files are closed and accessible for encrypting:

wrapper, DefWatch, ccEvtMgr, ccSetMgr, SavRoam, sqlservr, sqlagent, sqladhlp, Culserver, RTVscan, sqlbrowser, SQLADHLP, QBIDPService, Intuit.QuickBooks.FCS, QBCFMonitorService, sqlwriter, msmdsrv, tomcat6, zhudongfangyu, SQLADHLP, vmware-usbarbitator64, vmware-converter, dbsrv12, dbeng8

wxServer.exe, wxServerView, sqlservr.exe, sqlmangr.exe, RAgui.exe, supervise.exe, Culture.exe, RTVscan.exe, Defwatch.exe, sqlbrowser.exe, winword.exe, QBW32.exe, QBDBMgr.exe, qbupdate.exe, QBCFMonitorService.exe, axlbridge.exe, QBIDPService.exe, httpd.exe, fdlauncher.exe, MsDtSrvr.exe, tomcat6.exe, java.exe, 360se.exe, 360doctor.exe, wdswfsafe.exe, fdlauncher.exe, fdhost.exe, GDscan.exe, ZhuDongFangYu.exe

Finally, it clears the Shadow Volume Copies so that they cannot be used to restore files, removes backups made with Windows backup, and disables the Windows automatic startup repair using the following commands:

vssadmin.exe Delete Shadows /All /Quiet

wmic.exe SHADOWCOPY /nointeractive

bcdedit.exe /set {default} recoveryenabled No

bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures

wbadmin DELETE SYSTEMSTATEBACKUP

wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest

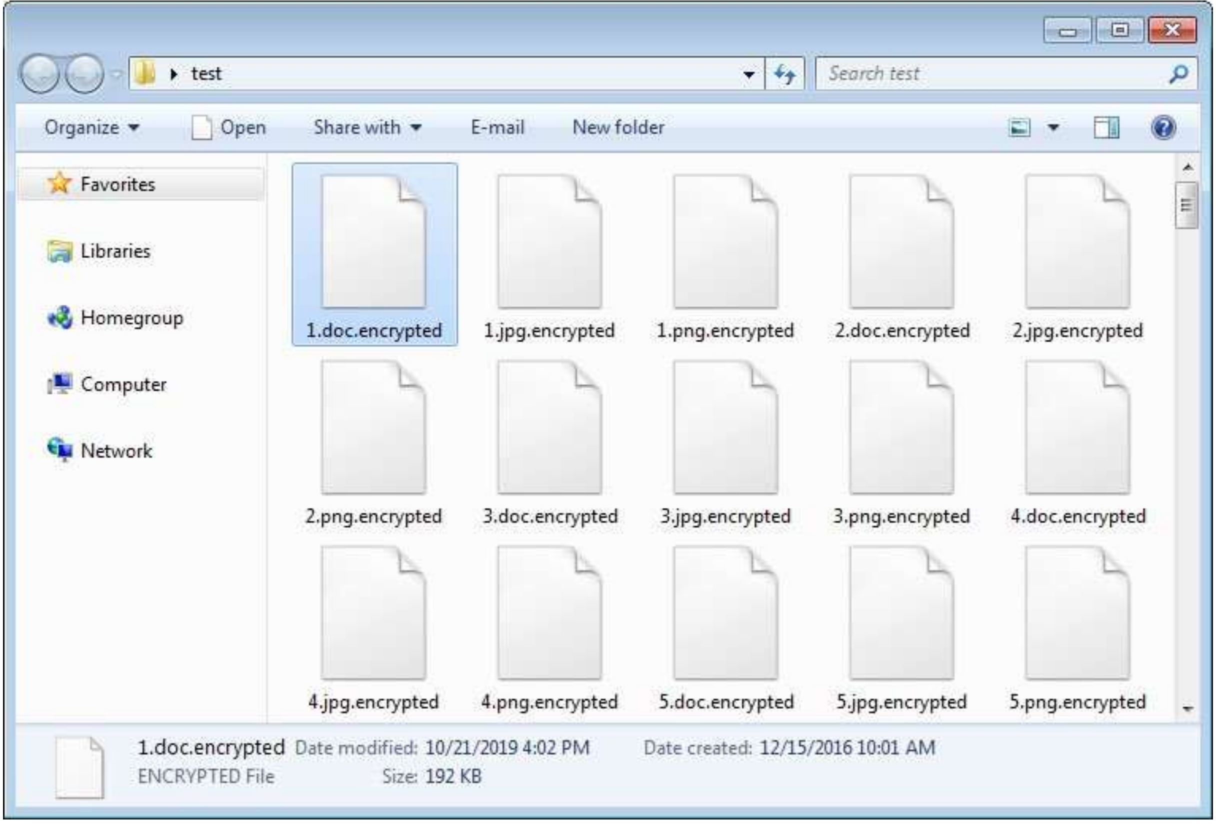
MedusaLocker will now begin to scan the computer's drives for files to encrypt. When encrypting files, it will skip all files that have the extensions .exe, .dll, .sys, .ini, .lnk, .rdp, .encrypted (or other extension used for encrypted files) as well as files in the following folders.

USERPROFILE
PROGRAMFILES(x86)
ProgramData
\AppData
WINDIR
\Application Data
\Program Files

\Users\All Users
\Windows
\intel
\nvidia
When encrypting files, it will use AES encryption to encrypt the file and then the AES key will be encrypted by a RSA-2048 public key included in the ransomware executable.

For each file that is encrypted, it will append one of the following extensions depending on the variant of the ransomware.

.encrypted, .bomber, .boroff, .breakingbad, .locker16, .newlock, .nlocker, .skynet

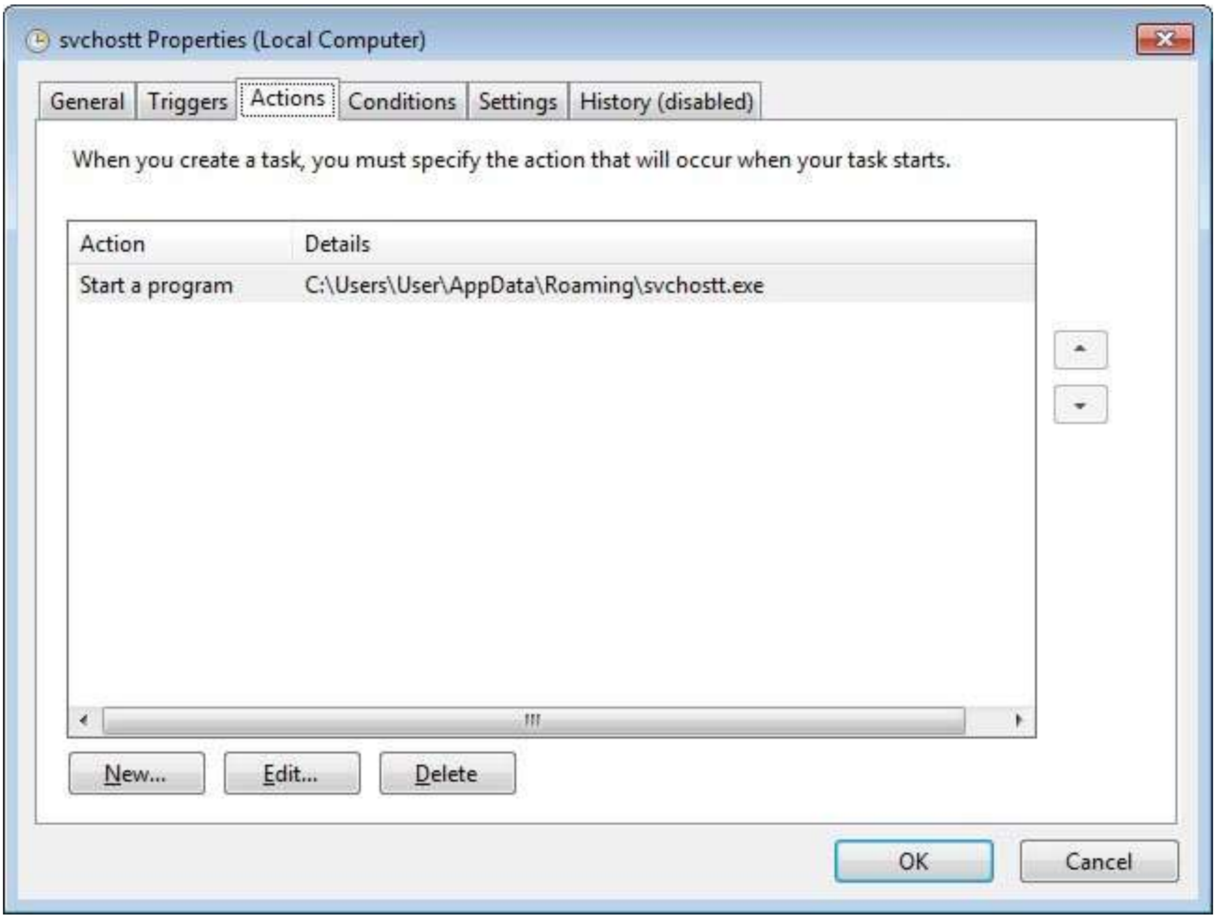


1.doc.encrypted Date modified: 10/21/2019 4:02 PM Date created: 12/15/2016 10:01 AM
ENCRYPTED File Size: 192 KB

Encrypted MedusaLocker files

When done, the ransomware will sleep for 60 seconds and then scan the drives again for new files to encrypt.

When installed, this ransomware will also copy itself to %UserProfile%\AppData\Roaming\svchostt.exe and create a scheduled task that launches the program every 30 minutes in order to remain resident.



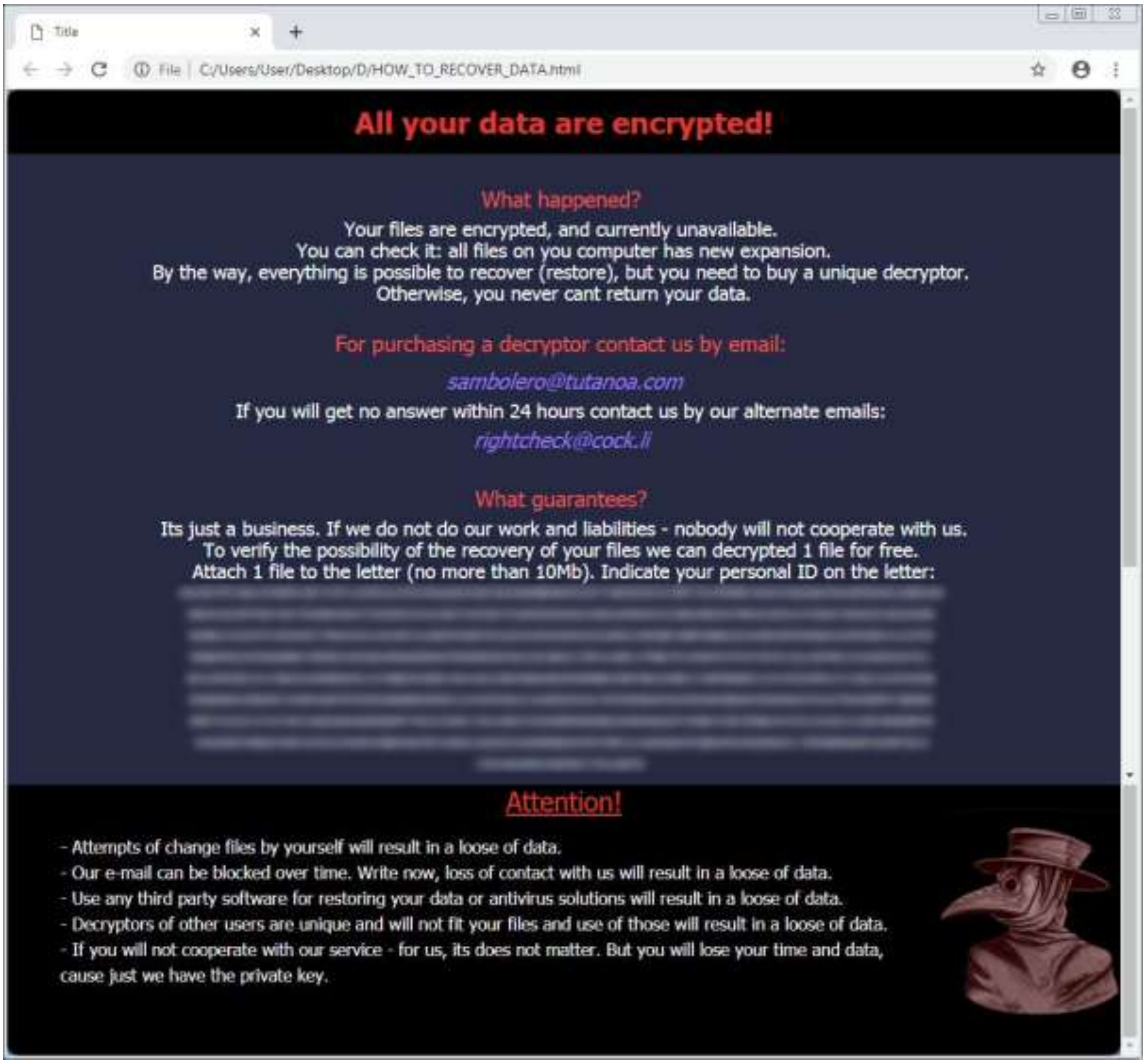
svchostt Properties (Local Computer)

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Users\User\AppData\Roaming\svchostt.exe

Scheduled Task for MedusaLocker

In each folder that a file is encrypted, MedusaLocker will create a ransom note named HOW_TO_RECOVER_DATA.html or Readme.html that contains two email addresses to contact for payment instructions.



All your data are encrypted!

What happened?

Your files are encrypted, and currently unavailable.
You can check it: all files on you computer has new expansion.
By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.
Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:

sambolero@tutanoa.com

If you will get no answer within 24 hours contact us by our alternate emails:

rightcheck@cock.li

What guarantees?

Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.
To verify the possibility of the recovery of your files we can decrypted 1 file for free.
Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:

[redacted]

Attention!

- Attempts of change files by yourself will result in a loose of data.
- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.
- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.
- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.
- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.

MedusaLocker Ransom Note

It is not known at this time how much the attackers are demanding for a decryptor or if they actually provide one after paying.

This ransomware is still being researched, so it is not known if it can be decrypted at this time.

For now, if you have any questions or need help with this ransomware, you can leave a comment here or in our MedusaLocker Support & Help topic.

IOCs

Hashes:

dde3c98b6a370fb8d1785f3134a76cb465cd663db20dffe011da57a4de37aa95

Associated Files:

HOW_TO_RECOVER_DATA.html

%UserProfile%\AppData\Roaming\svchostt.exe

C:\Windows\System32\Tasks\svchostt

Associated Registry keys:

HKCU\SOFTWARE\Medusa

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ "EnableLinkedConnections" = 1

Associated emails:

sambolero@tutanoa.com

rightcheck@cock.li

Ransom note text:

All your data are encrypted!

What happened?

Your files are encrypted, and currently unavailable.

You can check it: all files on you computer has new expansion.

By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.

Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:

sambolero@tutanoa.com

If you will get no answer within 24 hours contact us by our alternate emails:

rightcheck@cock.li

What guarantees?

Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.

To verify the possibility of the recovery of your files we can decrypted 1 file for free.

Attach 1 file to the letter (no more than 10Mb). Indicate your personal ID on the letter:

[id]

Attention!

- Attempts of change files by yourself will result in a loose of data.

- Our e-mail can be blocked over time. Write now, loss of contact with us will result in a loose of data.

- Use any third party software for restoring your data or antivirus solutions will result in a loose of data.

- Decryptors of other users are unique and will not fit your files and use of those will result in a loose of data.

- If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.

Source: https://www.bleepingcomputer.com/news/security/medusalocker-ransomware-wants-its-share-of-your-money/

13. 15 Years Later, Metasploit Still Manages to be a Menace

A fresh look at the penetration testing tool Metasploit reveals the 15-year old hacking tool still has some tricks up its sleeves, even against modern defenses.

The popular penetration testing and hacking framework Metasploit may be getting long in the tooth, but it hasn’t lost its bite in the hands of bad actors. According to researchers, hackers are still using the tool and a highly effective technique called Shikata Ga Nai (Japanese for “nothing can be done”) to slip past modern day endpoint protections.

Stopping attacks that use this technique still remain a challenge, according to a fresh analysis by FireEye researchers Steve Miller, Evan Reese and Nick Carr posted Monday.

“Despite Metasploit’s over 15 year existence, there are still core techniques that go undetected, allowing malicious actors to evade detection,” researchers wrote. Metasploit was created in 2003 by network security expert (and hacker) H D Moore. In 2009, Rapid7 hired Moore and acquired Metasploit. Moore designed the tool as a way to make the job of penetration testers easier. And, like many similar tools, it was coopted by black hat hackers who have used it, as recently as last week, to attack computer systems.

Today, Metasploit is on its fifth version and billed by Rapid7 as “penetration testing software to help you act like the attacker.”

Metasploit, and especially Shikata Ga Nai, has also found a home with a cadre of bad guys.

FireEye said Shikata Ga Nai has been used by suspected Chinese nation-state sponsored threat group APT20, along with recent attacks involving cybercrime groups identified by FireEye as UNC902, TA505 and APT41. In 2018, ESET Research identified the Turla APT group using the Shikata Ga Nai encoder in a campaign called Mosquito.

“The encoding utility that Shikata Ga Nai provides is typically found in first stage backdoors,” Reese told Threatpost. This type of malware would be used to gain an initial foothold within an environment during an attack, he said.

"One of [Metasploits] core techniques is the Shikata Ga Nai (SGN) payload-encoding scheme," FireEye wrote. "Modern detection systems have improved dramatically over the last several years and will often catch plain vanilla versions of known malicious methods. In many cases though, if a threat actor knows what they are doing they can slightly modify existing code to bypass detection."

According to researchers, skilled code tweaks, via the Metasploit SGN technique, are still highly lethal. They credit the SGN encoder's unique "polymorphic XOR additive feedback encoder" for its success. Researchers break down that jargon as such:

"It is polymorphic in that each creation of encoded shellcode is going to be different from the next," researchers wrote. SGN will make the payload appear benign via encoding the malware with "dynamic instruction substitution, dynamic block ordering, randomly interchanging registers, randomizing instruction ordering, inserting junk code, using a random key, and randomization of instruction spacing between other instructions."

A XOR, or XOR cipher, is an encryption algorithm that operates on a set of known principles. Encryption and decryption can be performed by applying and reapplying the XOR function.

In the context of Metasploit and SGN, "The XOR additive feedback piece in this case refers to the fact the algorithm is XORing future instructions via a random key and then adding that instruction to the key to be used again to encode the next instruction. Decoding the shellcode is a process of following the steps in reverse."

Researchers said SGN has managed to elude endpoint protection that relies too heavily on static and dynamic detection. The decoding of the payload in memory necessary to determine the code's malicious intent is too taxing on system, making it impractical. Detection via behavioral indicators and sandboxes can also be imprecise, Reese explains.

"Different engines will fall into the static or dynamic detection categories, including machine learning, but it is important to spread detections across engines within these categories. Relying on a single detection or engine is a single point of failure," he said. "It is entirely possible to detect SGN without machine learning, and we even included a YARA rule in the blog, but the addition of a machine learning engine… is a great approach for adding detection depth."

Researchers said, SGN encoded payloads vary. "Looking forward, we expect to see continued usage of SGN encoded payloads," they said.

Source: https://threatpost.com/metasploit-still-a-menace/149448/

14. PHP Bug Allows Remote Code-Execution on NGINX Servers

CVE-2019-11043 is trivial to exploit — and a proof of concept is available.

A buffer underflow bug in PHP could allow remote code-execution (RCE) on targeted NGINX servers.

First discovered during a hCorem Capture the Flag competition in September, the bug (CVE-2019-11043) exists in the FastCGI directive used in some PHP implementations on NGINX servers, according to researchers at Wallarm.

PHP powers about 30 percent of modern websites, including popular web platforms like WordPress and Drupal – but NGINX servers are only vulnerable if they have PHP-FPM enabled (a non-default optimization feature that allows servers to execute scripts faster). The issue is patched in PHP versions 7.3.11, 7.2.24 and 7.1.33, which were released last week.

In a Monday posting, Wallarm researchers said that the bug can be exploited by sending specially crafted packets to the server by using the "fastcgi_split_path" directive in the NGINX configuration file. That file is configured to process user data, such as a URL. If an attacker creates a special URL that includes a "%0a" (newline) byte, the server will send back more data than it should, which confuses the FastCGI mechanism.

"In particular, [the bug can be exploited] in a fastcgi_split_path directive and a regexp trick with newlines," according to Wallarm security researcher Andrew Danau, who found the bug. "Because of %0a character, NGINX will set an empty value to this variable, and fastcgi+PHP will not expect this….[as a result], it's possible to put [in] arbitrary FastCGI variables, like PHP_VALUE."

Another security researcher participating in the CTF exercise, Emil Lerner, offered more details in the PHP bug tracker: "The regexp in `fastcgi_split_path_info` directive can be broken using the newline character (in encoded form, %0a). Broken regexp leads to empty PATH_INFO, which triggers the bug," he said.

Lerner posted a zero-day proof-of-concept exploit for the flaw that works in PHP 7 to allow code execution. The exploit, which is trivial, makes use of an optimization used for storing FastCGI variables, _fcgi_data_seg.

"Usually, that sort of [buffer underflow] response is related to memory-corruption attacks and we expected to see an attack on the type of information disclosure," Wallarm researchers said. "Information disclosure is bad enough as it can result in leaking sensitive or financial data. Even worse, from time to time, although quite rarely, such behavior can indicate a remote code execution vulnerability."

Researchers added that without patching, this issue can be a dangerous entry point into web applications given the trivial nature of mounting an exploit.

Admins can identify vulnerable FastCGI directives in their NGINX configurations with a bash command, “egrep -Rin –color ‘fastcgi_split_path’ /etc/nginx/,” according to Wallarm.

Source: https://threatpost.com/php-bug-rce-nginx-servers/149593/

15. UniCredit Suffers Third Breach Despite Investing Billions in Cybersecurity

UniCredit was also hit with hacking incidents in September-October 2016 and June-July 2017.

Despite investing 2.4 billion euros since 2016 to upgrade its cybersecurity profile, Italian banking institution UniCredit has suffered its third recent data breach, this time impacting 3 million customers.

The company said in a short data breach announcement on its website that names, telephone numbers, email addresses and cities where clients were registered were exposed via unauthorized access to a file generated in 2015. Bank account details were not included. UniCredit told Reuters that it wouldn’t release information on how the access occurred, but it did say that has launched an internal investigation and has informed all the relevant authorities, including the police.

UniCredit was also hit with hacking incidents in September-October 2016 and June-July 2017, affecting 400,000 Italian customers. Those hacks were carried out via the network of a commercial partner, the bank said at the time.

“The incident at UniCredit shows that spending money alone isn’t enough to safeguard an organization from data breaches,” Jelle Wieringa, technical evangelist at KnowBe4, said via email. “After the breach in 2016, the bank invested an additional Euro 2.4 billion in its security. That is an awful lot of money to spend only to find out it wasn’t enough to stop the bad guys from getting in and stealing information.”

Its cybersecurity investment, which it calls “Transform 2019,” included the June 2019 implementation of a strong identification process featuring two-factor authentication (via a onetime password or biometric identification) for access to its web and mobile services, as well as for payment transactions.

“There isn’t very much known about the way the UniCredit breach took place. But there is still a lesson which can be learned from this. Even at this early stage,” Wieringa said. “In this instance, a file from 2015 was stolen. Under GDPR, it counts as a data breach, since it’s likely that most of the data is still valid. People tend to forget the value of data over time, especially if they are confronted with large amounts of it every day, and information fatigue is a real thing.”

ZeroFOX’ recent Financial Services Digital Threat Report showed a 56 percent annual increase in digital threat activity targeting the financial services sector this year. System and information exploitation specifically grew 26 percent within the past year.

“Attackers are increasingly adept at compromising systems, and social media has increasingly become the conduit,” according to the report. “They also blatantly market their heists both publicly and privately, across all digital channels. Malicious domains top the list of attack techniques at 57 percent share, with another 18 percent coming from information disclosures found on paste sites, most of which are accessible to the public.”

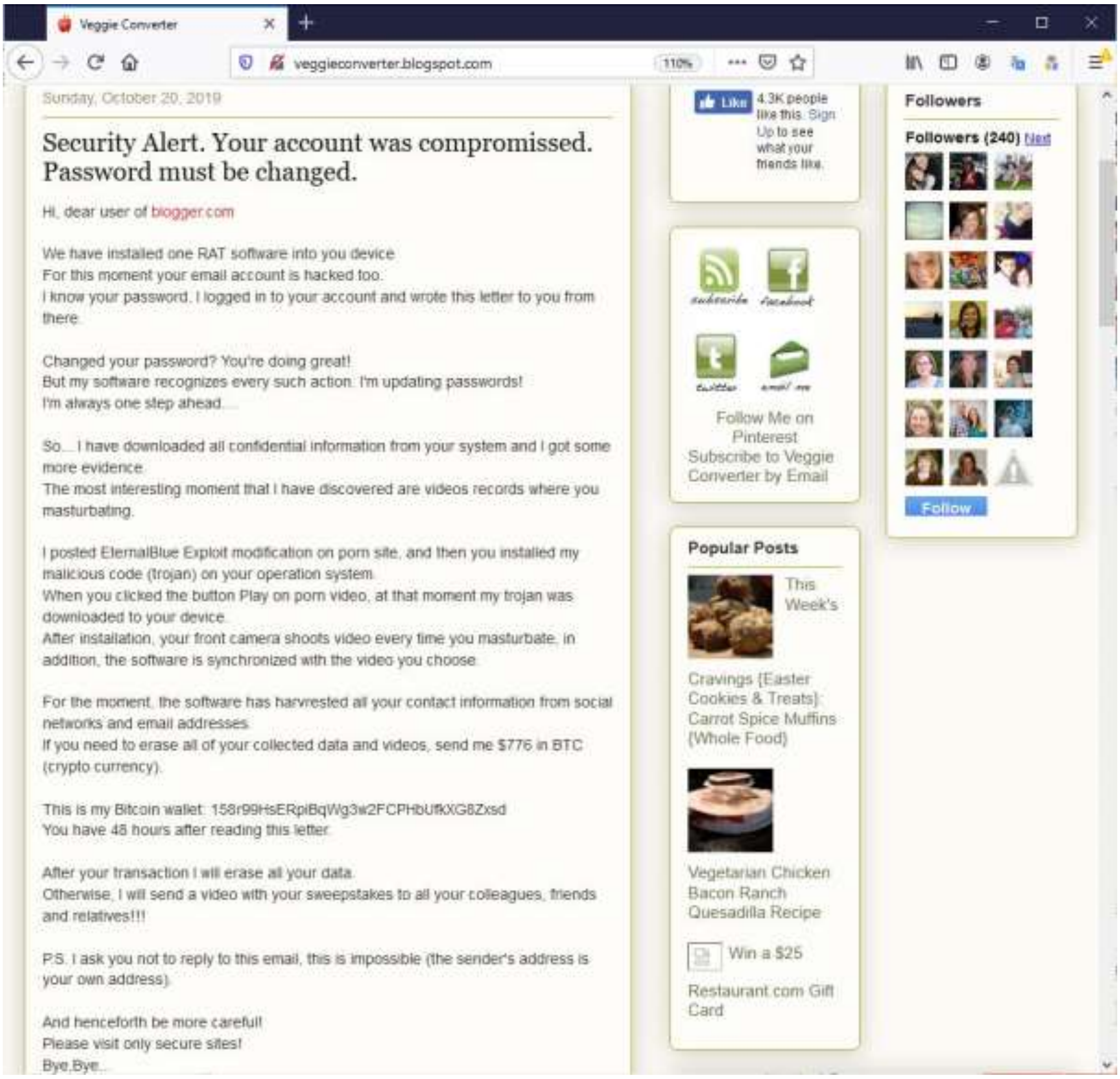
Source: https://threatpost.com/unicredit-suffers-third-breach/149617/

16. Blogger and WordPress Sites Hacked to Show Sextortion Scams

Scammers are hacking into WordPress and Blogger sites and using the hacked accounts to create posts stating that the blogger's computer has been hacked and that they were recorded while using adult web sites.

These types of threats is called sextortion and are typically send via email to recipients whose information was disclosed in data breaches. These scam emails then threaten the recipient that their video will be released to everyone on the their contact list unless an extortion demand is paid.

While performing some related searches, BleepingComputer has noticed that attackers are also hacking into the accounts of popular blogging platforms such as Blogger and WordPress. Once they gain access to an account, they create a new blog post containing a similar extortion threat that users typically receive via email.



Veggie Converter
veggieconverter.blogspot.com
110%
Like
4.3K people like this. Sign Up to see what your friends like.
subscribe
facebook
twitter
email me
Follow Me on Pinterest
Subscribe to Veggie Converter by Email
Popular Posts
This Week's Cravings {Easter Cookies & Treats}: Carrot Spice Muffins (Whole Food)
Vegetarian Chicken Bacon Ranch Quesadilla Recipe
Win a $25 Restaurant.com Gift Card
Followers
Followers (240) Next
Follow

Sunday, October 20, 2019

Security Alert. Your account was compromissed. Password must be changed.

Hi, dear user of blogger.com

We have installed one RAT software into you device.
For this moment your email account is hacked too.
I know your password. I logged in to your account and wrote this letter to you from there.

Changed your password? You're doing great!
But my software recognizes every such action. I'm updating passwords!
I'm always one step ahead...

So... I have downloaded all confidential information from your system and I got some more evidence.
The most interesting moment that I have discovered are videos records where you masturbating.

I posted ElernalBlue Exploit modification on porn site, and then you installed my malicious code (trojan) on your operation system.
When you clicked the button Play on porn video, at that moment my trojan was downloaded to your device.
After installation, your front camera shoots video every time you masturbate, in addition, the software is synchronized with the video you choose.

For the moment, the software has harvrested all your contact information from social networks and email addresses.
If you need to erase all of your collected data and videos, send me $776 in BTC (crypto currency).

This is my Bitcoin wallet: 158r99HsERpiBqWg3w2FCPHbUfkXG8Zxsd
You have 48 hours after reading this letter.

After your transaction I will erase all your data.
Otherwise, I will send a video with your sweepstakes to all your colleagues, friends and relatives!!!

P.S. I ask you not to reply to this email, this is impossible (the sender's address is your own address).

And henceforth be more careful!
Please visit only secure sites!
Bye.Bye...

Sextortion scam posted to Blogger

It is not known how the attacker's are gaining access to a user's site, but it is most likely through credentials stuffing attacks using credentials from leaked data breaches.

Sextortion is profitable

Hacking into a user's blog and using their credentials to create a new post with the extortion demand makes threats more convincing. This is because the attacker is really hacking into the user's blogging account, this is proven by the existence of the blog post, and thus it adds more legitimacy that the attacker may have hacked the user's computer as well.

While we all know this is purely a scam and no one has hacked your computer to record a video, after reviewing some of the over 1,500 hacked Blogger accounts and over 200 hacked WordPress accounts, it is clear that users are paying sextortion demands.

From just three bitcoin addresses that BleepingComputer commonly saw listed in the blog post sextortion posts, the attackers have generated approximately 12 bitcoins. This is equal to over $110,000 USD at current prices.

Bitcoin Address	BTC Payments	Value
1N6dubqFmnyQ2qDWvi32ppVbc3kKMTYcGW	4.38393994	$41,303.11
15yF8WkUg8PRjJehYW4tGdqcyzc4z7dScM	3.95021411	$37,216.78
1H1K8MfLEJgjCCfDEkTJmv9GJjD3XzEFGR	3.81985447	$35,988.61

As these bitcoin addresses are also used in traditional email sextortion scams, it is not clear whether it's the blog posts or the emails generating these payments.

It does, though, show that sextortion, regardless of how it is delivered, offers an easy way to generate revenue with little to no overhead. This is why these scams have become common and will continue to be so in the future.

Source: https://www.bleepingcomputer.com/news/security/blogger-and-wordpress-sites-hacked-to-show-sextortion-scams/

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.