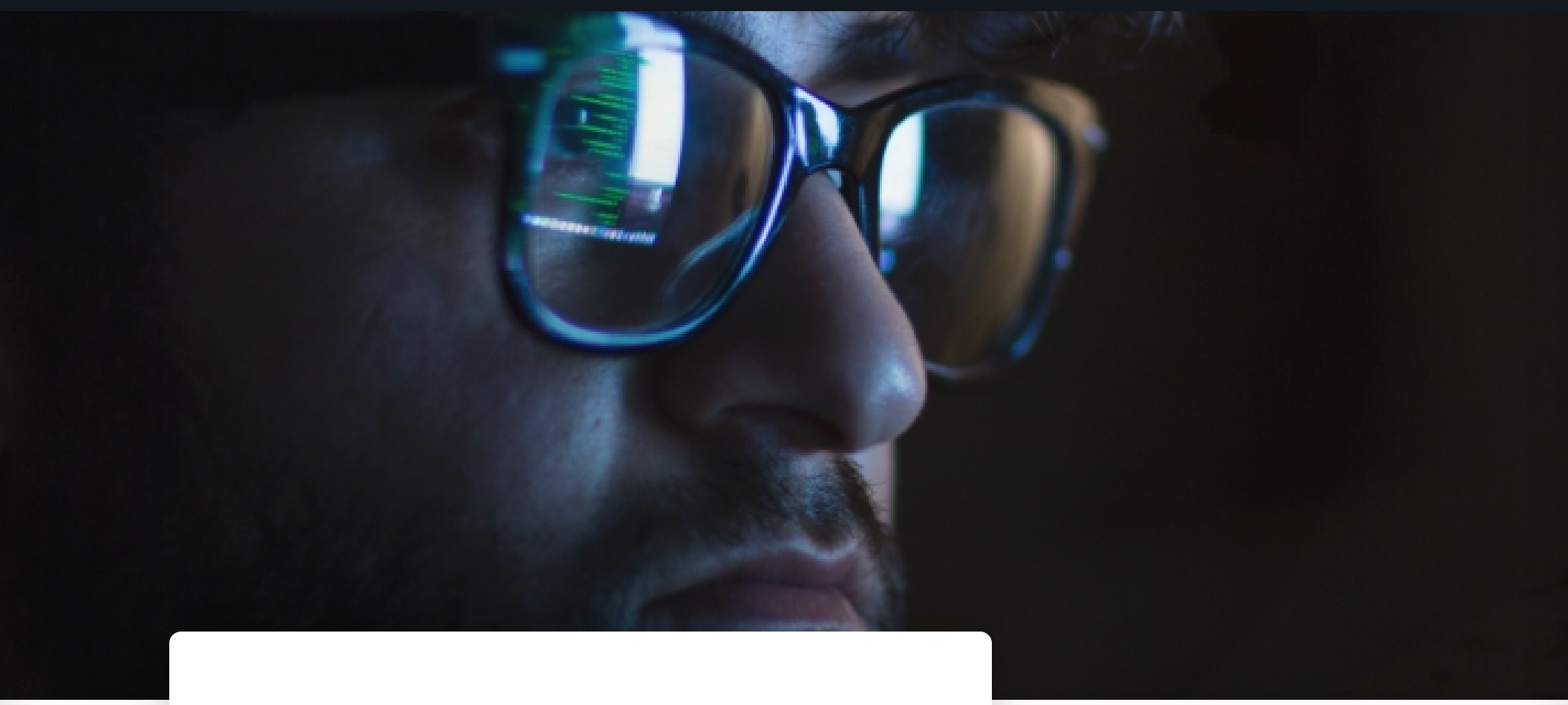

CTI Roundup: CCP-Sponsored APT41 Deploys Google GC2 for Attacks

APT41 leverages Google GC2, ransomware gangs abuse Process Explorer driver to kill security software, and new details regarding 3CX's software supply chain compromise emerge

Emerging Issue

APRIL 25, 2023

This week, CTI analyzes APT41's recent use of Google Command and Control (GC2) during its operations — highlighting a steady increase in the use of publicly available tools by China-nexus APTs. Next up is an overview of a new defense evasion tool — dubbed AuKill — that enables threat actors to disable endpoint detection and response (EDR) solutions before deploying backdoors and ransomware. To wrap things up, CTI explores a new report detailing the true root cause of the high-profile supply chain compromise that began impacting the ubiquitous 3CX Desktop App and its users back in March.

Hackers abuse Google command-and-

Tanium CTI

Tanium's Cyber Threat Intelligence (CTI) analysts process and extract trends from the daily cyber landscape to curate and deliver current intel to stakeholders around threats impacting business and security.

Google Cloud's **2023 Threat Horizons Report** reveals that the Chinese state-sponsored espionage group APT41 is now abusing Google's GC2 red-teaming tool in its attacks.

specifically for red team activities. Google's Threat Analysis Group (TAG) disrupted **APT41's latest phishing attack**, during which the actors attempted to distribute the GC2 agent amid broader abuse of Google's infrastructure.

APT41 — also known as Wicked Panda and HOODOO — occasionally engages in financially motivated operations. The group has been active since at least 2007, and several members have been indicted by the U.S. Department of Justice. The group has historically targeted government and private organizations in the U.S., Taiwan, India, Thailand, China, Hong Kong, Mongolia, and more. APT41 is also known for its ability to leverage vulnerability exploitation, particularly when it comes to applications vulnerable to SQL injection attacks.

Campaign details

In October 2022, Google's TAG disrupted an APT41 campaign targeting a Taiwanese media organization with **phishing emails containing links to password-protected files** hosted on Drive. The payload of this campaign was GC2; an open-source red team tool.

This tool, written in Go, gets its commands from Google Sheets to hide its malicious activity. The data is then exfiltrated to Google Drive. After installation on the victim's machine, the malware queried Google Sheets for its commands.GC2 also enables the threat actor to download additional files from Drive onto the victim's system. The use of Google infrastructure and collaborative applications increases the likelihood of malicious traffic going largely unnoticed within enterprise environments.

Google has noted that this threat actor previously utilized a similar workflow last year to target an Italian job search website.

Analyst comments from Tanium's Cyber Threat Intelligence Team

"Google's TAG hasn't released many details about this campaign, so there isn't much to work with in terms of indicators of compromise (IOC). However, the campaign does reveal this Chinese APT's increased use of publicly available tools like GC2."

versions of publicly available tools. APT41's use of GC2 — supposedly in its original state with no custom modifications — certainly marks a shift towards out-of-the-box, publicly available tooling. Is this a tactic to confuse attribution efforts,

Ransomware gangs abuse Process Explorer driver to kill security software

A new Sophos report explores a **defense evasion tool** called "AuKill" currently being leveraged by threat actors to disable **endpoint detection and response (EDR)** software before deploying backdoors and ransomware. The tool abuses an outdated version of Process Explorer and has been used in at least three ransomware incidents this year.

Sophos has reportedly investigated multiple incidents in which the threat actor attempted to disable EDR clients via the new AuKill tool. This tool abuses an outdated version of the driver used by version 16.32 of Microsoft's Process Explorer utility. In January and February, the threat actors deployed Medusa Locker ransomware after leveraging AuKill. In February, the threat actor was again observed using AuKill before deploying LockBit ransomware.

This is of course not the first time that threat actors have been observed deploying software designed to kill EDR agents. Security research teams from Microsoft, Mandiant, SentinelOne, and Sophos have all previously reported on attacks involving custom-built drivers to disable EDR products. What sets these recent incidents apart from previous attacks is the fact that AuKill abuses a legitimate, but out-of-date and exploitable driver.

Sophos has collected six different variants of the AuKill malware, finding similarities between AuKill and another open-source tool, Backstab, including debug strings exhibiting seemingly derivative characteristics and nearly identical code flow logic used to interact with the driver. Sophos researchers believe that AuKill was built around multiple code snippets from Backstab.

Legitimate driver abuse and procexp.sys

To get around driver security measures, threat actors need to either figure out a way to get a malicious driver signed by a trusted/legitimate certificate or figure out how to abuse a legitimate commercial software driver. In the campaigns observed by Sophos, the threat actors took advantage of a driver both created – and signed – by Microsoft.

legitimate Process Explorer driver is normally found in this same location and is called procexp152.sys. Both drivers can exist on a machine that has a copy of Process Explorer running. The AuKill installer also drops an executable copy of itself to

service.

Abusing this process requires the threat actor to use administrative privileges on the system. However, critical Windows processes are under additional protection to prevent threat actors from disabling them. To circumvent these features, the threat actors need to go one step further and run a driver in kernel mode. In this case, AuKill abused the legitimate driver behind Process Explorer to overcome these features.

It's important to note that the use of AuKill requires the threat actor to have administrative privileges, but it cannot, itself, give the threat actor those privileges.

Aukill malware's evolution

Sophos collected six versions of AuKill malware over the course of a few months and tracked functionality changes between each version. Most notably, the compiler and targeted security components changed.

Sophos primarily focused on v1 and v6 samples as those were most frequently observed. V6 appears to Sophos' researchers to be an experimental version. The comparison between these two versions gives researchers insight into where future versions could potentially go.

- **Phase 1:** Installing the service: Once executed, the malware confirms whether it has administrator privileges. It also requires the threat actor to run the file with a keyword, or a password of sorts, as the first argument of the command line and, if not, aborts execution. AuKill first starts the Trusted Installer service – a Windows Modules installer component. It then duplicates the token of TrustedInstaller[.]exe and passes the token to elevate itself to SYSTEM when the process restarts. It finally copies itself to C:\Windows\system32, installs itself as a service, and starts the service.
- **Phase 2:** Disabling security: After establishing persistence by creating the service entry, it drops procexp.sys onto disk. The driver is embedded in AuKill as a resource.

To prevent components of EDR clients from restarting, AuKill starts several threads to ensure that these processes and services stay disabled. Each of the threads targets a different component and continuously probes them to determine

AuKill has four functions it uses to disable EDR components: Terminate via Procexp, terminate forcefully, disable services, and unload drivers. Sophos goes into detail on each of these four functions in their report.

Analyst comments from Tanium's Cyber Threat Intelligence Team

"While AuKill appears to be a precursor to further malicious activity and any indication of AuKill in a network should be taken seriously, it's worth remembering that AuKill cannot run if the threat actor does not already have administrator privileges. Nonetheless, observation of AuKill activity in a network likely signals the pending deployment of another dangerous payload, such as LockBit ransomware; therefore proving that AuKill can still pose a serious threat."

3CX software supply chain compromise initiated by a prior software supply chain compromise

Intelligence firm Mandiant has concluded that the initial infection vector for the high-profile 3CX supply chain compromise which affected that company's ubiquitous Desktop App software back in March was malicious software downloaded from a third-party website onto 3CX's network.

Mandiant notes that this is the first time it has observed one software supply chain attack lead to another software supply chain attack in what can only be described as an Inception-style, Russian-nesting-doll-type of cyber nightmare.

Here's a refresher, courtesy of Mandiant:

> *In late March 2023, a software supply chain compromise spread malware via a **trojanized version of 3CX's legitimate software** that was available to download from their website. The affected software was 3CX DesktopApp 18.12.416 and earlier, which contained malicious code that ran a downloader, SUDDENICON, which in turn received additional command and control (C2) servers from encrypted icon files hosted on GitHub. The decrypted C2 server was used to download a third stage identified as ICONICSTEALER, a dataminer that steals browser information.*

Mandiant Consulting also claims to have uncovered the initial intrusion vector as a result of its ongoing investigation of the

installer for X_TRADER, a legitimate software package provided by Trading Technologies.

Mandiant determined that a fairly sophisticated loading malware (which Mandiant describes as a "multi-stage modular backdoor") as well as its accompanying modules.

Analyst comments from Tanium's Cyber Threat Intelligence Team

"Mandiant attributes the malicious activity described above to the threat group tracked as UNC4736 — an actor which Mandiant believes with a moderate degree of confidence to be related to the financially-motivated North Korean cybercrime activity dubbed AppleJeus by CISA."

"This is corroborated by reporting from Google's TAG which reported the compromise of www.tradingtechnologies[.]com in February 2022, preceding the distribution of compromised X_TRADER updates from the site. Further infrastructure overlaps are apparent between UNC4736 and APT43, another North Korean threat actor for which CTI maintains an active Threat Actor Profile (TAP)."

"As pointed out by Mandiant, APT43 frequently targets cryptocurrency users and related services, highlighting such campaigns are widespread across North Korea-nexus cyber operators."

"It is significant that North Korean state-backed groups may be responsible for the first software supply chain attack that led directly to another software supply chain attack. It is also likely that security researchers may have underestimated cyber threat actors with a DPRK-nexus in the past. This incident serves as a reminder that the Hermit Kingdom still poses a formidable threat."

---

*Do you have insight into these stories that you want to share? Head over to **Tanium's discussion forum** to start a conversation.*

For further reading, catch up on our recent **cyber threat intelligence roundups.**

CTI Roundup: Gophish Toolkit Phishing, Malicious Virtual Hard...

CTI Roundup: Callback Phishing, Time-to-Exploit Trends, and PureLogs...

Reducing the Fog of War by Increasing Cybersecurity...