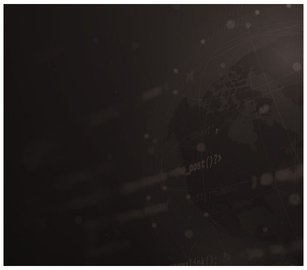
Rewterz Threat Alert – Witchetty APT Group – Active IOCs

rewterz.com/rewterz-news/rewterz-threat-alert-witchetty-apt-group-active-iocs

October 4, 2022

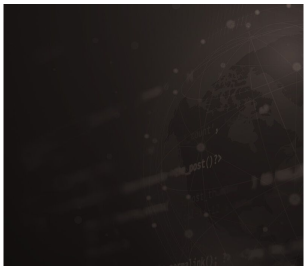
Rewterz Threat Alert – Lazarus APT Group Exploit Dell Driver Vulnerability Using New FudModule Rootkit – Active IOCs

October 5, 2022



Rewterz Threat Update – Recent Microsoft Exchange Server Zero-Day Mitigation Can Be Easily Bypassed

October 4, 2022



Rewterz Threat Alert – Lazarus APT Group Exploit Dell Driver Vulnerability Using New FudModule Rootkit – Active IOCs

October 5, 2022

Severity

High

Analysis Summary

Researchers discovered the Witchetty cyber espionage threat actor group, which employs steganography to conceal backdoor malware in the Windows logo in its latest campaign. The gang attacked governments in the Middle East through the backdoor.

Steganography is the technique of concealing data within non-secret, public information or computer files, such as an image, in order to avoid discovery.

Witchetty is believed to have close links to the Chinese threat actor APT10. The gang is also thought to be part of the TA410 operatives (aka APT10, Stone Panda), the group previously connected to attacks on US energy companies.
The group's current cyberespionage campaign, which targeted two governments in the Middle East and an African stock market, began in February 2022 and is still underway.

The hackers updated their toolset for this campaign to target various vulnerabilities, and they employed steganography to shield their malicious payload from antivirus software.
Two pieces of malware, a first-stage backdoor called X4 and a second-stage modular malware called LookBack, were used in the latest Witchetty activities.

Prior to carrying out malicious actions like stealing credentials, moving lateral across networks, and dropping additional malicious payload, the threat actors first gain initial access to a network by exploiting the Microsoft Exchange ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) and ProxyLogon (CVE-2021-26855 and CVE-2021-27065) attack chains.

The gang launched their campaign by utilizing a previously unidentified implant known as Backdoor.Stegmap, a steganography-based malware that hides the malicious payload in a bitmap picture of an outdated Microsoft Windows logo placed on a GitHub repository. The attackers were able to avoid detection by hiding the malicious code behind a picture uploaded on a trustworthy service.

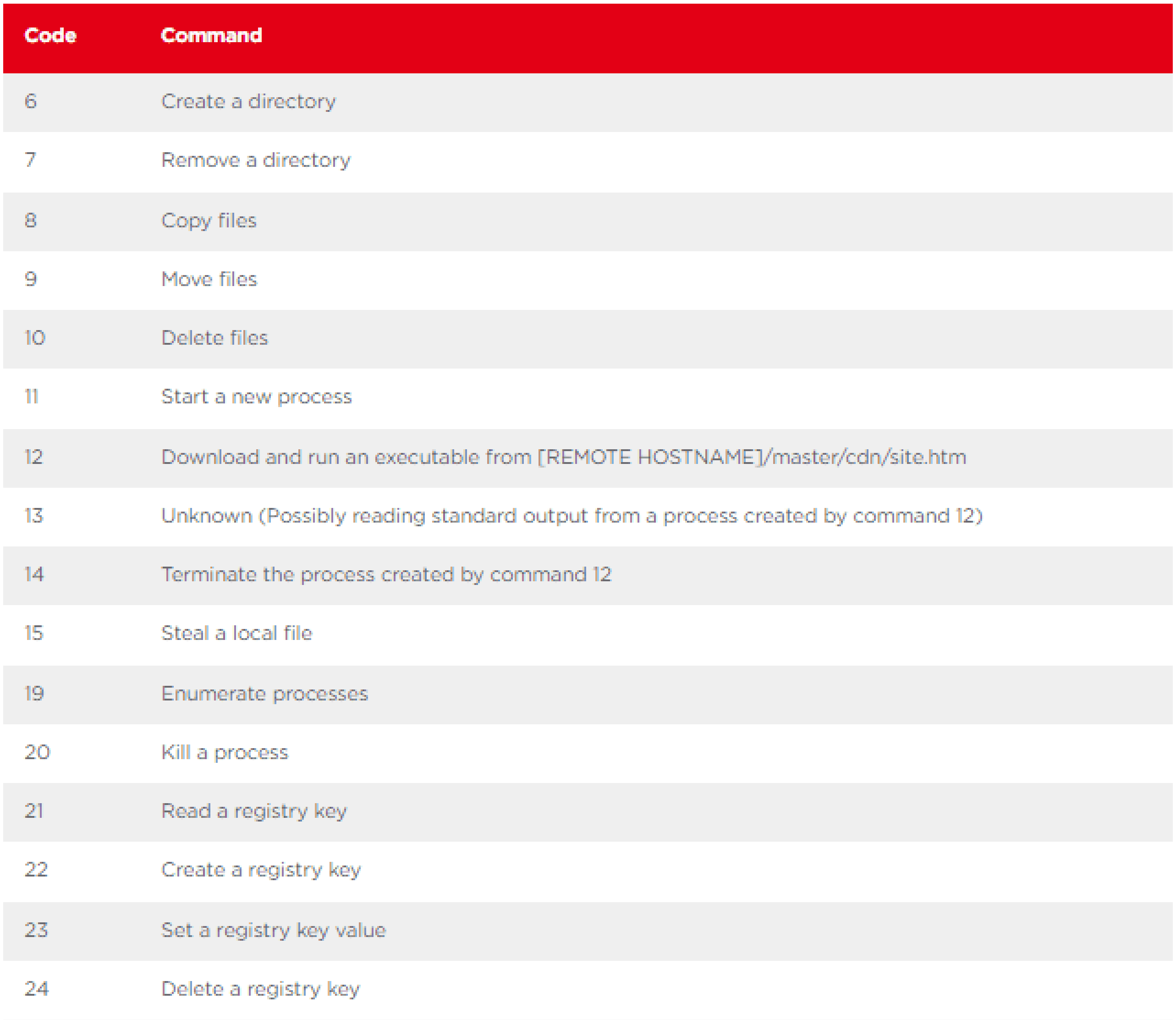
> "A DLL loader downloads a bitmap file from a GitHub repository. The file appears to be simply an old Microsoft Windows logo. However, the payload is hidden within the file and is decrypted with an XOR key."

source: The payload is hidden under the Windows logo.

> “Disguising the payload in this fashion allowed the attackers to host it on a free, trusted service. “

According to them,
“Downloads from reputable domains like GitHub are significantly less likely to trigger red flags than downloads from an attacker-controlled command-and-control (C&C) server.”

The following commands are supported by the implant:



Code	Command
6	Create a directory
7	Remove a directory
8	Copy files
9	Move files
10	Delete files
11	Start a new process
12	Download and run an executable from [REMOTE HOSTNAME]/master/cdn/site.htm
13	Unknown (Possibly reading standard output from a process created by command 12)
14	Terminate the process created by command 12
15	Steal a local file
19	Enumerate processes
20	Kill a process
21	Read a registry key
22	Create a registry key
23	Set a registry key value
24	Delete a registry key

Table 1. Backdoor.Stegmap commands

In the campaign identified, the hackers depend on last year's vulnerabilities to infiltrate the target network and take advantage of the subpar management of publicly accessible servers.

Impact

- Cyber Espionage
- Exploitation of Vulnerabilities
- Network Breach

Indicator Of Compromise

MD5

e3af60f483774014c43a7617c44d05e7

SHA-256

e5f98a1b0d37a09260db033aa09d6829dc4788567beccda9b8fef7e6e3764848

SHA-1

8126ed23cb483c67a454c762178ec7de8536b31a

Remediation

- Block all threat indicators at your respective controls.
- Search for Indicator of compromise (IOCs) in your environment utilizing your respective security controls
- Do not download document ?les attached in emails from unknown sources and strictly refrain from enabling macros when the source isn’t reliable.
- Maintain daily backups of all computer networks and servers.
- Passwords – Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access – limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- WAF – Web defacement must be stopped at the web application level. Therefore, set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Patch – Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Secure Coding – Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- 2FA – Enable two-factor authentication.
- Antivirus – Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using a multi-layered protection is necessary to secure vulnerable assets
- Security Best Practices – Do not open emails and attachments from unknown or suspicious sources.