Rewterz Threat Alert - Power Supplier’s Network Infiltrated for 6 Months by “Redfly” Hackers – Active IOCs - Rewterz

Published: 2023-10-13 · Archived: 2026-04-05 13:43:20 UTC

Severity

High

Analysis Summary

A stealthy APT group called “Redfly” hacked a national electricity grid organization in Asia and maintained persistent access to the network for about six months. Researchers discovered evidence for this attack between 28 February and 3 August 2023 after noticing suspicious malware activity within the organization’s network.

The trojan they found is ShadowPad, which is widely used by various APT groups. They also discovered traces of specialized file launchers and keyloggers. Researchers have noticed that Redfly focuses mainly on critical national infrastructure.

The variant of ShadowPad used in these attacks disguises its components as VMware files and drops them on the compromised system. It is also able to achieve persistence by creating services named after VMware, so it can launch malicious executable files and DLL when the system boots.

```
ServiceName: VMware Snapshot Provider Service

DisplayName: VMware Snapshot Provider Service

ServiceType:
SERVICE_WIN32_OWN_PROCESS|SERVICE_INTERACTIVE_PROCESS

StartType: SERVICE_AUTO_START

BinaryPathName:
C:\ProgramData\VMware\RawdskCompatibility\virtual\vmrawdsk.exe
```

ShadowPad is known to be a versatile RAT capable of various features like keylogging, data exfiltration, file searching, and remote command execution. It is difficult to track because a lot of different APTs use it.

Redfly used a different keylogging tool to capture keystrokes in the form of log files, which are then retrieved by the malicious users manually. They also made use of a tool called Packerloader, which loads and executes shellcode inside the AES encrypted files and can avoid detection from antivirus software.

The hackers used this tool to execute code in order to modify a driver file’s permissions and creating credential dumps in the Windows registry to be able to revive it in the future. They also rely on PowerShell to execute commands, helpful for gathering details about the compromised system.

The threat actors utilized DLL side-loading and other legitimate executables, stolen credentials, and executing legitimate binaries for lateral movement. It's common for espionage groups to have a long dwelling period within the compromised networks in order to harvest as much intelligence as they can.

"Attacks against CNI targets are not unprecedented. Almost a decade ago, Symantec uncovered the Russian-sponsored Dragonfly group's attacks against the energy sector in the U.S. and Europe," the researchers concluded in the report.

The exact intent of the attackers to disrupt the power supply is not known, but it still poses a significant threat. This level of disruption could have caused a big damage to the energy provider's reputation and also economic loss for the whole nation.

Impact

- Cyber Espionage
- Information Theft

Indicators of Compromise

Domain Name

websencl.com

MD5

- e1024b0a0c84c798790dba7a68debb88
- db1922cccbf560c6c503dfbac8630033
- 27f636a36207581e75c700c0e36a8031
- a0e9d1463086fed950b51508b826bd5b

SHA-256

- 656582bf82205ac3e10b46cbbcf8abb56dd67092459093f35ce8daa64f379a2c
- ac6938e03f2a076152ee4ce23a39a0bfcd676e4f0b031574d442b6e2df532646
- 231d21ceefd5c70aa952e8a21523dfe6b5aae9ae6e2b71a0cdbe4e5430b4f5b3
- d9438cd2cdc83e8efad7b0c9a825466efea709335b63d6181dfdc57fb1f4a4e3

SHA-1

- 1059ea2d1a62c2e39affd6481578e575755acb09

- 4bba897ee81240b10f9cca41ec010a26586e8c09
- e5091779e52536657eb321a1ccb7cfd0e67bd897
- b9871ce86c29aac05b119c4514cd87ce90956f7b

Remediation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls
- Do not download documents attached in emails from unknown sources and strictly refrain from enabling macros when the source isn’t reliable.
- Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using multi-layered protection is necessary to secure vulnerable assets
- 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.
- Maintain daily backups of all computer networks and servers.
- Keep all software, operating systems, and applications up to date with the latest security patches.
- Continuously monitor network and system logs for unusual or suspicious activities.
- Deploy security information and event management (SIEM) solutions to centralize log analysis.

Source: https://www.rewterz.com/rewterz-news/rewterz-threat-alert-power-suppliers-network-infiltrated-for-6-months-by-redfly-hackers-active-iocs/