Redfly: Espionage Actors Continue to Target Critical Infrastructure

Espionage actors are continuing to mount attacks on critical national infrastructure (CNI) targets, a trend that has become a source of concern for governments and CNI organizations worldwide. Symantec's Threat Hunter Team has found evidence that a threat actor group Symantec calls Redfly used the ShadowPad Trojan to compromise a national grid in an Asian country for as long as six months earlier this year. The attackers managed to steal credentials and compromise multiple computers on the organization's network.

The attack is the latest in a series of espionage intrusions against CNI targets. In May 2023, the U.S., UK, Australian, Canadian, and New Zealand governments issued a joint alert about threat actors targeting CNI organizations in the U.S. using techniques that could potentially be replicated against targets in other countries. The alert followed Microsoft's report on Volt Typhoon, an espionage actor that compromised several critical infrastructure organizations in the U.S.

Links to earlier attacks

ShadowPad is a modular remote access Trojan (RAT) that was designed as a successor to the Korplug/PlugX Trojan, and was, for a period of time, sold in underground forums. However, despite its origins as a publicly available tool, it was only sold publicly for a very short time reportedly to a handful of buyers. It has since been closely linked to espionage actors.

While ShadowPad is known to be used by multiple advanced persistent threat (APT) actors, identified tools and infrastructure used in the recent campaign targeting a national power grid overlaps with previously reported attacks attributed to a cluster of APT41 activity (aka Brass Typhoon, Wicked Panda, Winnti, and Red Echo). Symantec tracks this group under as multiple distinct actors such as Blackfly and Grayfly, where links between these groups have been discussed before. The activities identified in this campaign are currently being tracked under a separate group that Symantec has dubbed Redfly, which appears to exclusively focus on targeting CNI.

Tools used: ShadowPad

A distinct variant of the ShadowPad Trojan was used in this attack. It utilized the domain websencl[.]com for command-and-control (C&C) purposes.

It copied itself to disk in the following locations, masquerading as VMware files and directories to mask its purpose (there is no other evident association with VMware products):

- C:\ProgramData\VMware\RawdskCompatibility\virtual\vmrawdsk.exe
- C:\ProgramData\VMware\RawdskCompatibility\virtual\mscoree.dll

Persistence is achieved by creating the following service that is configured to start with Windows on boot-up:

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

Tools used: Packerloader

This is a tool used to load and execute shellcode. The shellcode is stored in a file in an encrypted form. It allows the attackers to deliver and execute arbitrary files or commands on an infected computer.

The tool is a 64-bit dynamic link library (DLL) that has one export, called WorkProc, which accepts an additional command-line argument. This argument is interpreted as a string and can be used as a decryption key. If no key is passed on the command line, the malware attempts to retrieve a key from the following registry location instead:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\HomeGroup\PublishedMessageOfflineCache\

In all cases, the malware checks that the string length of the decryption secret is 0x20 characters.

The malware then loads its payload. It will first check if the following file exists:

- [FILE_DIRECTORY_OF_SAMPLE_BINARY]\tmp.bin

If the file exists, its contents are used as the encrypted payload. Otherwise, the malware attempts to retrieve a payload from the registry at the following location:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\HomeGroup\PublishedMessageOfflineCache\

The malware will then decrypt the loaded payload with the Advanced Encryption Standard (AES) algorithm in Electronic Code Book (ECB) mode using the first 0x10 bytes of the decryption key as the AES key. Finally, it creates a new thread to execute the decrypted payload as shellcode.

Tools used: Keylogger

The attackers also employed a keylogger, which was installed under various file names on different computers, including winlogon.exe and hphelper.exe.

The keylogger was configured to store captured keystrokes in the following location:

- %SYSTEMROOT%\Intel\record.log

Attack outline

The first evidence of intrusion on the targeted network dated from February 28, 2023, when ShadowPad was executed on a single computer. It was executed again on May 17 2023, suggesting that the attackers had maintained a presence in the intervening three months.

A day earlier (May 16), a suspicious Windows batch file (file name: 1.bat) was executed. Shortly afterwards, PackerLoader was executed via rundll32 from the %TEMP% directory with some command-line arguments:

rundll32 %TEMP\%packerloader.dll WorkProc E10ADC3949BA59ABBE56E057F20F883E

Immediately afterwards, permissions were modified for a driver file called dump_diskfs.sys to grant access to all users. It is possible the attackers used this driver to create dumps of the file system for later exfiltration. Four minutes later, credentials were dumped from the Windows registry:

reg save HKLM\SYSTEM system.save

reg save HKLM\SAM sam.sav

reg save HKLM\SECURITY security.save

On May 19, the attackers returned, running PackerLoader and the 1.bat batch file again. Shortly afterwards, a legitimate binary named displayswitch.exe was executed. It was likely being used to perform DLL side-loading. This involves the attackers placing a malicious DLL in a directory where a legitimate DLL is expected to be found. The attacker then runs the legitimate application (having installed it themselves). The legitimate application then loads and executes the payload.

Several hours later a suspicious PowerShell command was executed and used to gather information on the storage devices attached to the system. Specifically it was designed to look for DriveType=3 (Read/Write Supported) and gather details on available space.

powershell -executionpolicy ByPass -command "$disks = Get-WmiObject Win32_LogicalDisk -Filter \" DriveType = 3\" ; foreach ($disk in $disks) { $freeSpace = \"{0:N2}\" -f ($disk.FreeSpace/1GB) ; Write-Host \"Drive Free Space: $($disk.DeviceID) $freeSpace\"; }"

Several hours later, a similar set of activity occurred again.

On May 26, displayswitch.exe was executed from the %TEMP% directory via the command prompt. Less than an hour later, several commands were executed via displayswitch.exe to dump credentials from the registry and clear the Windows security event logs:

CSIDL_SYSTEM\cmd.exe

reg save HKLM\SAM sam.save

reg save HKLM\SYSTEM system.save

reg save HKLM\SYSTEM system.save

reg save HKLM\SYSTEM system.save

reg save HKLM\SECURITY security.save

reg save HKLM\SAM sam.save

reg save HKLM\SECURITY security.save

wevtutil cl security

On May 29, the attackers returned and used a renamed version of ProcDump (file name: alg.exe) to dump credentials from LSASS.

alg.exe -accepteula -ma lsass.exe z1.dmp

On May 31, a scheduled task is used to execute oleview.exe, mostly likely to perform side-loading and laterally movement. Use of Oleview by ShadowPad has been previously documented by Dell Secureworks and was also reported to have been used in attacks against industrial control systems. The command specified that Oleview was to be executed on a remote machine using the task name (TendView) at 07:30 a.m. It appears the attackers likely used stolen credentials in order to spread their malware onto other machines within the network.

schtasks /create /s \\[REMOVED] /u [REMOVED] /P [REMOVED] /tr "CSIDL_PROFILE\[REMOVED]\appdata\local\temp\oleview.exe" /tn TrendView /st 07:30 /sc once /ru " " /f

Malicious activity appeared to cease until July 27, when a keylogger (file name: winlogon.exe) was installed on a machine.

The final evidence of malicious activity came on August 3, when the attackers returned and attempted to dump credentials again using a renamed version of ProcDump (file name: yara32.exe):

yara32.exe -accepteula -ma lsass.exe z1.dmp

Minutes later, the attackers also attempted to dump credentials from the Windows registry:

reg save HKLM\SAM sam.save

reg save HKLM\SAM sam.save

reg save HKLM\SYSTEM system.save

reg save HKLM\SYSTEM system.save

reg save HKLM\SYSTEM system.save

reg save HKLM\SECURITY security.save

reg save HKLM\SECURITY security.save

Source of concern

Attacks against CNI targets are not unprecedented. Almost a decade ago, Symantec uncovered the Russian-sponsored Dragonfly group's attacks against the energy sectors in the U.S. and Europe. More recently, the Russian Sandworm group mounted attacks against the electricity distribution network in Ukraine, which were directed at disrupting electricity supplies.

However, the frequency at which CNI organizations are being attacked appears to have increased over the past year and is now a source of concern. Threat actors maintaining a long-term, persistent presence on a national grid presents a clear risk of attacks designed to disrupt power supplies and other vital services in nation-states during times of increased political tension. While Symantec has not seen any disruptive activity by Redfly, the fact that such attacks have occurred in other regions means they are not outside the bounds of possibility.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

Type	IOC	Description
SHA256	73993d3b9aebf8dee50a144cf7e56b49d222a42600171df62c13d3f96824db60	DiskDumpDriver
SHA256	01f4e6f32070234b4203507be22cfb9d3d73b4bbd5100f62271e2161ec8813b7	DisplaySwitch (clean)
SHA256	8dbc8b756cb724e2d6dc9c7c40f22c48022a8ee48da6685c4ccf580c6b5183cf	Keylogger
SHA256	2e642afdd36c129e6b50ae919ca608ac0006ce337f2a5a7a6fb1eef6a4ad99e7	Oleview (clean)
SHA256	32d709d8d41e4ede6861ce27c9e2bb86d83be8336b45a17f567bab1869c6600a	PackerLoader
SHA256	16f413862efda3aba631d8a7ae2bfff6d84acd9f454a7adaa518c7a8a6f375a5	ProcDump
SHA256	656582bf82205ac3e10b46cbbcf8abb56dd67092459093f35ce8daa64f379a2c	Shadowpad
SHA256	ac6938e03f2a076152ee4ce23a39a0bfcd676e4f0b031574d442b6e2df532646	Shadowpad
SHA256	231d21ceefd5c70aa952e8a21523dfe6b5aae9ae6e2b71a0cdbe4e5430b4f5b3	Shadowpad
SHA256	d9438cd2cdc83e8efad7b0c9a825466efea709335b63d6181dfdc57fb1f4a4e3	Shadowpad
Domain	websencl[.]com	Shadowpad
Filepath	%SYSTEMROOT%\Intel\record.log	Keylogger