MirrorFace Attack against Japanese Organisations

blogs.jpcert.or.jp/en/2024/07/mirrorface-attack-against-japanese-organisations.html

朝長 秀誠 (Shusei Tomonaga)

July 16, 2024

- Python
- APT
- LODEINFO
-
- Email

JPCERT/CC has been observing attack activities by MirrorFace LODEINFO and NOOPDOOR malware (since 2022). The actor's targets were initially media, political organisations, think tanks and universities, but it has shifted to manufacturers and research institutions since 2023. As for the TTPs, they used to send spear phishing emails to infiltrate the target's network, but now they also leverage vulnerabilities in external assets. Figure 1 shows the actor's attack activity transition.

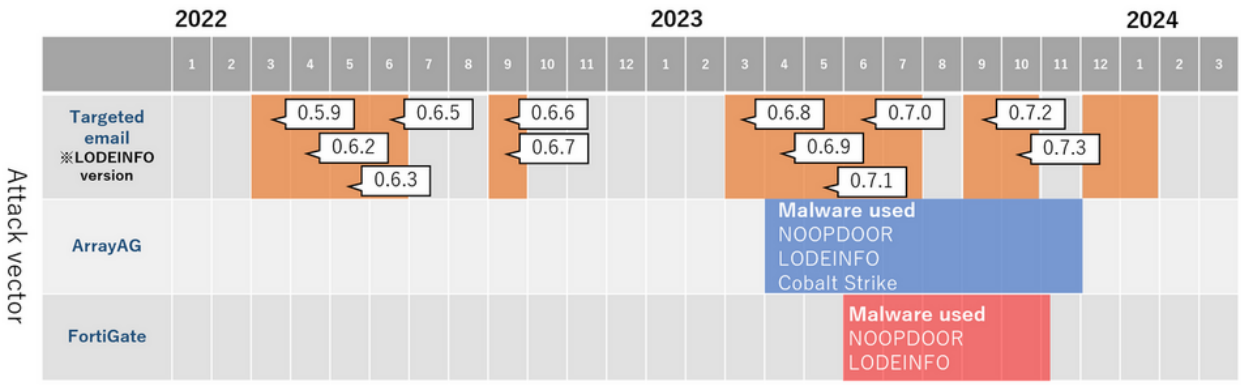


Figure 1: MirrorFace attack activities timeline
(Based on incident reports submitted to JPCERT/CC and publications by other vendors[1] [2])

JPCERT/CC published a security alert (Japanese) on attack activities exploiting vulnerabilities in November 2023. We have confirmed that this actor has leveraged the vulnerabilities in Array AG and FortiGate. Proself may also be exploited, but the cases

mentioned in this blog post focus on those related to Array AG and Fortigate.
This blog describes the malware NOOPDOOR and details of the TTPs and tools the actor used in the victim network.

NOOPDOOR

NOOPDOOR execution flow

NOOPDOOR is a shellcode, and it injects itself into a legitimate application. It runs either by an XML file (Type1) or a DLL file (Type2). The execution flow of each type is illustrated in Figure 2 and 3.

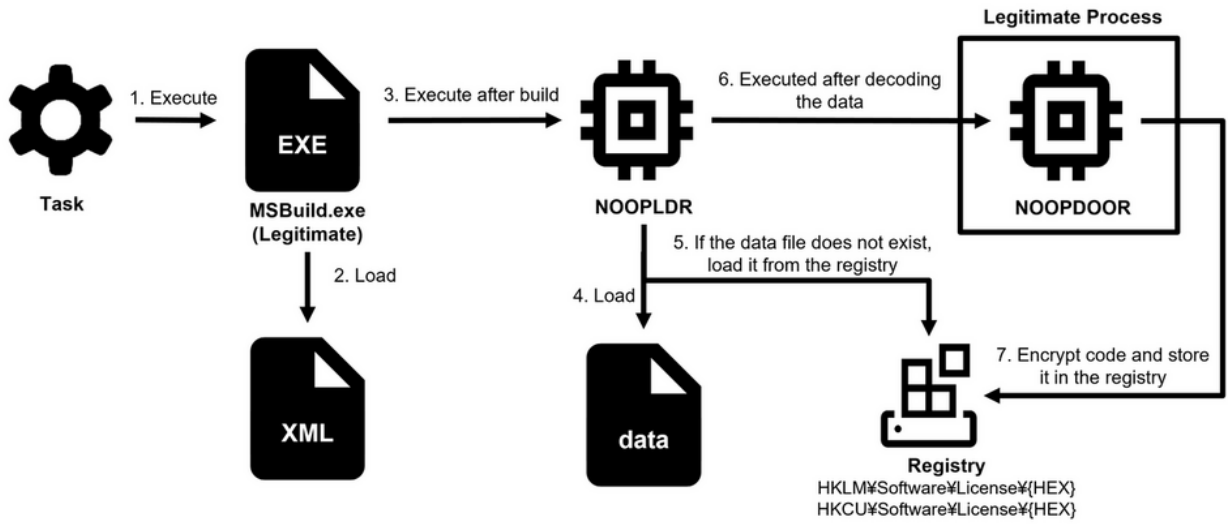


Figure 2: NOOPDOOR launched by an XML file (Type1)

Type1 has its obfuscated C# code in an XML file. It builds the C# code with MSBuild and runs by NOOPDOOR's loader (hereafter 'NOOPLDR'). Once it runs, it reads specific data file or registry value, decrypts the data loaded in AES (CBC mode) based on the machine's unique MachineId and ComputerName, and injects the code into a legitimate application.

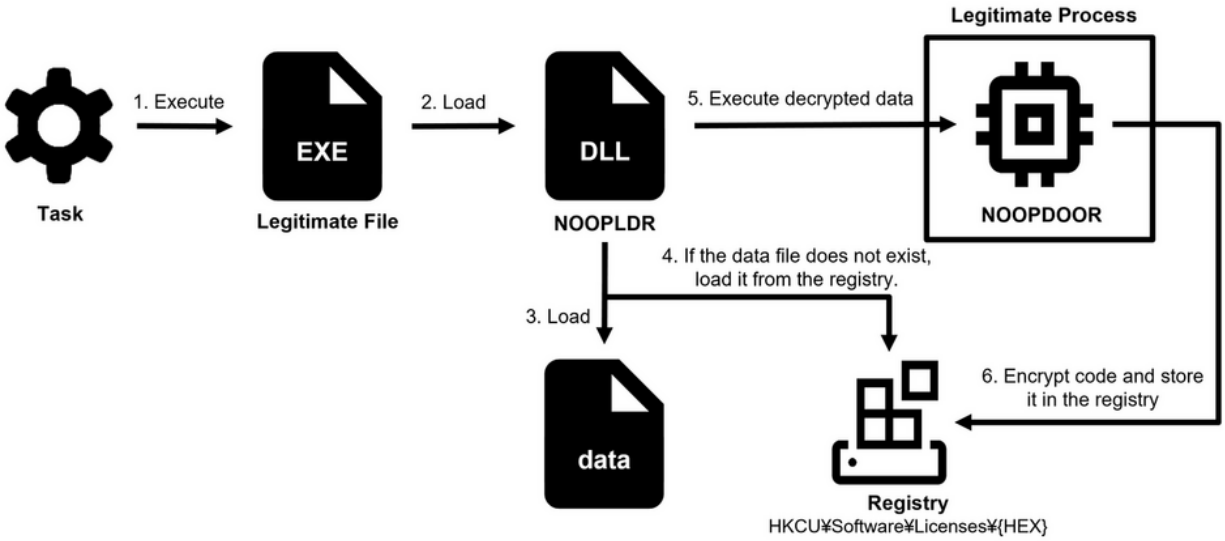


Figure 3: NOOPDOOR launched by a DLL file (Type2)

Type2 launches a legitimate application from Windows tasks, and NOOPLDR is loaded to a legitimate application by DLL side-loading. Similar to Type1, it loads the registry and injects decrypted code into a legitimate application. After NOOPDOOR is executed, both Type1 and Type2 encrypt the code, which is stored in a preset registry so that it is loaded when it runs again.

Types of NOOPLDR

There are several types of NOOPLDR samples with different injection process and functions as follows.

How it runs	Injection process	Service	Storage registry
XML	lsass.exe	-	HKLM\Software\License\{HEX}, HKCU\Software\License\{HEX}
XML	tabcal.exe	-	HKLM\Software\License\{HEX}, HKCU\Software\License\{HEX}
XML	rdrleakdiag.exe	-	HKLM\Software\License\{HEX}, HKCU\Software\License\{HEX}
XML	svchost.exe	-	HKLM\Software\License\{HEX}, HKCU\Software\License\{HEX}
XML	wuauclt.exe	-	HKLM\Software\License\{HEX}, HKCU\Software\License\{HEX}
XML	vdsldr.exe	-	HKLM\Software\License\{HEX}, HKCU\Software\License\{HEX}

XML	prevhost.exe	-	HKLM\Software\License\{HEX}, HKCU\Software\License\{HEX}
DLL	wuauclt.exe	Yes	HKCU\Software\Microsoft\COM3\{HEX}
DLL	None	-	HKCU\Software\Licenses\{HEX}
DLL	svchost.exe	-	HKCU\Software\Licenses\{HEX}

Table 1: Features in NOOPLDR samples

Some Type2 samples with service registration capability has a function to hide the service by running the following command.

```
sc start [SERVICE_NAME] && sc sdset [SERVICE_NAME] D:(D;;DCLCWPDTSD;;;IU)
(D;;DCLCWPDTSD;;;SU)(D;;DCLCWPDTSD;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:
(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

NOOPLDR obfuscation

NOOPLDR (Type2) uses Control Flow Flattening (CFF) technique as in Figure 4 (left). The code can be partially analysed with D810[3] and other CFF deobfuscator tools, but it is not possible to fully deobfuscate the entire code as it also has many meaningless Windows API calls. To make this process easier, JPCERT/CC developed a tool to help this analysis. The code can be deobfuscated by applying this tool and then D810 and other deobfuscator tools as in Figure 4 (right).

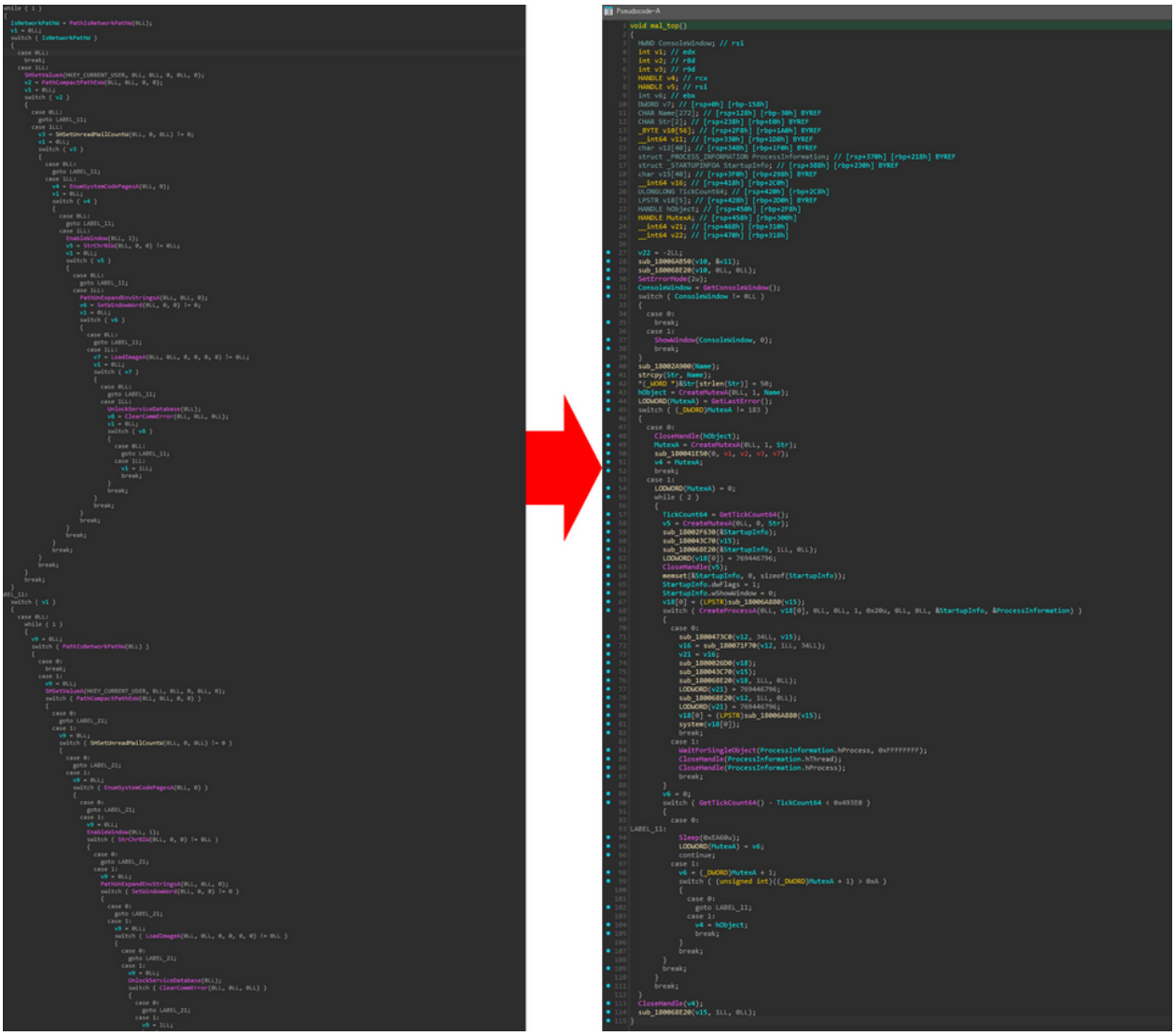


Figure 4: CFF obfuscated function (Left) and deobfuscated function (Right)

JPCERT/CC's tool to support NOOPLDR deobfuscation is available on the below Github repository.

GitHub: JPCERTCC/aa-tools/Deob_NOOPLDR.py
https://github.com/JPCERTCC/aa-tools/blob/master/Deob_NOOPLDR.py

NOOPDOOR functions

NOOPDOOR has several functions such as communicating to Port 443 with the destination generated by the DGA based on the system time and receiving commands by TCP Port 47000. On top of the basic malware behaviour including uploading/downloading files and executing additional commands, it also has commands to alter file time stamps, which may confuse forensic analysis.
Please refer to the presentation material[4] by Dominik Breitenbacher at JSAC2024 for more details on the NOOPDOOR command structure and behaviour.

Threat actors activity on the network

The following sections explain the commands, tools and defense evasion techniques used by the attackers.

Access credentials

The attackers attempt accessing Windows network credentials by multiple methods.

(1) From Lsass memory dump

- They aim to extract credentials by accessing the memory dump of a currently running Lsass process by using a tool.
- Access to Lsass memory dump can be detected in an environment with Microsoft Defender. (Event log Windows Defender/Operational: Event ID 1011: Detection name Trojan:Win32/LsassDump)

(2) From NTDS.dit

- They aim to extract credentials by accessing the domain controller database file (NTDS.dit).
- They aim to access NTDS.dit by Vssadmin command etc.
- Access to NTDS.dit is recorded in the event logs. (Please refer to JPCERT/CC's Tool Analysis Result Sheet[5] [6].)

(3) From registry hives

They also aim to access SYSTEM, SAM, SECURITY registry hives to retrieve credentials from SAM database.

These activities can be detected depending on the EDR products.

Lateral Movement

The attackers attempt to access a wide range of clients and servers by leveraging Windows network admin privilege. It is especially recommended to carefully look at servers that are managed by privileged users such as file servers, AD, anti-virus software management servers. Attackers carry out lateral movement by copying the malware via SMB and registering it to the tasks (by schtasks command).
The series of activities can be recorded and monitored by Windows event logs. Creation of a new scheduled task is recorded with the **Event ID 4698**. Additionally, if "Audit Detailed File Share" is enabled, copying the malware via SMB is recorded in the Security event log with the **Event ID 5145**. (Please see Appendix D for setting details.) Below is sample event log recorded when a file is copied by an attacker (Event ID 5145).

```
A network share object was checked to see whether client can be granted desired
access

Subject:
       Security ID:  [ID]
       Account Name:  [User name]
       Account Domain:  [Domain name]
       Logon ID:  [Logon ID]

Network Information:
       Object Type:  File
       Source Address:  [IP address]
       Source Port:  [Port]

Share Information:
       Share Name:  \\*\C$
       Share Path:  \??\C:\
       Relative Target Name: WINDOWS\SYSTEM32\UIANIMATION.XML

Access Request Information:
    Access Mask:    0x120089
    Accesses:       READ_CONTROL
                SYNCHRONIZE
                ReadData (or ListDirectory)
                ReadEA
                ReadAttributes
```

Reconnaissance command

After the intrusion, the attackers were carrying out reconnaissance activities by using Windows commands as below. This includes commands that are not used by general users, which may be a clue to detect malicious activities.

```
at
auditpol
bitsadmin
del
dir
dfsutil
dsregcmd
hostname
ipconfig
nbtstat
net
netstat
ntfrsutl
nslookup
mountvol
ping
powercfg
qprocess
quser
qwinsta
reg
sc
setspn
schtasks
systeminfo
tasklist
vdsldr
ver
vssadmin
wevtutil
whoami
wmic
```

Information exfiltration

Aside from NOOPDOOR, the attackers used the following tools to exfiltrate information.

- WinRAR
- SFTP

The attackers attempt to exfiltrate information after reviewing file contents. We have confirmed that they ran `dir /s` commands to see the list of files in the file server and stored the results in a RAR file. In addition, the attackers also used the following commands to see the list of files, including the folders in OneDrive, Teams, IIS, etc.

```
cmd.exe /c dir c:\
cmd.exe /c dir c:\users\
cmd.exe /c dir c:\users\\Desktop
cmd.exe /c dir c:\users\\Documents
cmd.exe /c dir "c:\users\\OneDrive"  /s /a
cmd.exe /c dir "c:\users\\OneDrive\Microsoft Teams\"
cmd.exe /c dir "c:\users\\OneDrive\Microsoft Teams チャット ファイル\[redacted].docx"
cmd.exe /c dir "c:\Program Files\"
cmd.exe /c dir "c:\Program Files (x86)"
cmd.exe /c dir c:\Intel
cmd.exe /c dir c:\inetpub
cmd.exe /c dir c:\inetpub\wwwroot
```

Other tools

The attackers also use tools other than LODEINFO and NOOPDOOR. In some cases, we confirmed that GO Simple Tunnel (GOST), a HTTP/SOCKS5 proxy tool, was leveraged.

GitHub: ginuerzh/gost
https://github.com/ginuerzh/gost

We also saw cases where GOST was running on Linux servers. Also, Linux servers may also be infected with TinyShell-based malware.

Defense Evasion

The attackers used various techniques for defense evasion including the following. (Please see Appendix C for more details on TTPs.)

(1) Leverage MSBuild

Execute a malicious XML file (NOOPLDR) by using a legitimate MSBuild

(2) Store malicious data in a registry

Load encrypted malware file, store the data in the registry and delete the original file

(3) Alter time stamp

Change the creation date of the malware and tools older than the actual attack date

(4) Add a rule to a firewall

- Add a new setting to allow communication to specific ports that NOOPDOOR uses
- Recorded in Event log Firewall With Advanced Security/Firewall with the **Event ID 2004**

(5) Hide registered services

Set access control so that the registered services are not displayed

(6) Delete Windows Event logs

- Delete system logs
- Recorded with **Event ID 1102**

(7) Disable Windows Defender

Recorded in Windows Defender/Operational with the **Event ID 5001**

(8) Delete files

Delete the malware file

After completing the series of reconnaissance activities, the attackers deleted the malware and stopped its own processes. This is supposed to be conducted for a purpose of covering up the traces to allow long-term persistence.

```
cmd.exe /c del c:\Windows\system32\UIAnimation.xml /f /q
taskkill.exe
```

In closing

MirrorFace has been conducting attacks against Japanese organisations for a long period of time. Activities related to this actor is expected continue, and it is advised to continuously look out for information on this actor. Please refer to Appendix A for detailed IoC information. In some cases, early detection based on IoCs may be difficult. In order to detect this kind of incidents with security products and services in an early stage, we believe it is crucial to maintain information sharing among security vendors about malware and TTPs for some extent. JPCERT/CC is committed to continue working with partner organisations and security vendors for timely information sharing about such attack activities.

Acknowledgement

JPCERT/CC would like to acknowledge the support by the organisations for this publication.

Security vendors who supported this publication

- ITOCHU Cyber & Intelligence Inc.
- Macnica, Inc.
- Secureworks, Inc.

We also referred to the report from the following companies:

- LAC Co., Ltd.
- Trend Micro Incorporated

Yuma Masubuchi, Kota Kino, Shusei Tomonaga
(Translated by Yukako Uchida)

Reference

[1] JSAC2024: Spot the Difference: An Analysis of the New LODEINFO Campaign by Earth Kasha
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf

[2] ITOCHU Cyber & Intelligence Inc.: 分析官と攻撃者の解析回避を巡る終わりなき戦い: LODEINFO v0.6.6 - v0.7.3 の解析から (Japanese)
https://blog.itochuci.co.jp/entry/2024/01/24/134047

[3] GitHub: D-810
https://github.com/joydo/d810

[4] JSAC2024: Unmasking HiddenFace: MirrorFace's most complex backdoor yet
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_8_Breitenbacher_en.pdf

[5] JPCERT/CC: Tool Analysis Result Sheet ntdsutil
https://jpcertcc.github.io/ToolAnalysisResultSheet/details/ntdsutil.htm

[6] JPCERT/CC: Tool Analysis Result Sheet vssadmin
https://jpcertcc.github.io/ToolAnalysisResultSheet/details/vssadmin.htm

Appendix A: IoC

- 45.66.217.106
- 89.233.109.69
- 45.77.12.212
- 108.160.130.45
- 207.148.97.235
- 95.85.91.15
- 64.176.214.51
- 168.100.8.103
- 45.76.222.130
- 45.77.183.161
- 207.148.90.45
- 207.148.103.42
- 2a12:a300:3600::31b5:2e02
- 2001:19f0:7001:2ae2:5400:4ff:fe0a:5566
- 2400:8902::f03c:93ff:fe8a:5327
- 2a12:a300:3700::5d9f:b451

Appendix B: Malware hash values

NOOPLDR Type1

- 93af6afb47f4c42bc0da3eedc6ecb9054134f4a47ef0add0d285404984011072
- bcd34d436cbac235b56ee5b7273baed62bf385ee13721c7fdcfc00af9ed63997
- 43349c97b59d8ba8e1147f911797220b1b7b87609fe4aaa7f1dbacc2c27b361d
- 4f932d6e21fdd0072aba61203c7319693e490adbd9e93a49b0fe870d4d0aed71
- 0d59734bdb0e6f4fe6a44312a2d55145e98b00f75a148394b2e4b86436c32f4c
- 9590646b32fec3aafd6c648f69ca9857fb4be2adfabf3bcaf321c8cd25ba7b83
- 572f6b98cc133b2d0c8a4fd8ff9d14ae36cdaa119086a5d56079354e49d2a7ce

NOOPLDR Type2

- 7a7e7e0d817042e54129697947dfb423b607692f4457163b5c62ffea69a8108d
- 5e7cd0461817b390cf05a7c874e017e9f44eef41e053da99b479a4dfa3a04512
- b07c7dfb3617cd40edc1ab309a68489a3aa4aa1e8fd486d047c155c952dc509e

Appendix C: MITRE ATT&CK

Techniques	ID	Name	Description
Initial Access	T1133	External Remote Services	Exploit VPN product vulnerability and access network
Execution	T1053.005	Scheduled Task/Job: Scheduled Task	Execute NOOPLDR by a scheduled task
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task	Set a scheduled task to execute malware automatically
	T1543.003	Create or Modify System Process: Windows Service	Register a service and execute malware automatically
Privilege Escalation	T1134.002	Access Token Manipulation: Create Process with Token	Manipulate access tokens to create a process
Defense Evasion	T1055	Process Injection	Use a legitimate EXE file under C:\windows\system32, perform NOOPDOOR process injection and execute
	T1070.001	Clear Windows Event Logs	Delete system logs
	T1070.004	File Deletion	Delete malware and tools

	T1070.006	Timestomp	Change the file creation date
	T1112	Modify Registry	Store NOOPDOOR in a registry
	T1127.001	Trusted Developer Utilities Proxy Execution: MSBuild	Use a legitimate MSBuild.exe to run a malicious XML file
	T1140	Deobfuscate/Decode Files or Information	Decrypt NOOPDOOR and execute in the injected process
	T1562.001	Disable or Modify Tools	Disable Windows Defender
	T1562.004	Disable or Modify System Firewall	Add a rule to allow communication to the ports that NOOPDOOR uses
	T1564	Hide Artifacts	Set access restriction so that the services related to autorun NOOPDOOR are not visible
Credential Access	T1003	OS Credential Dumping	Dump credentials from lsass and ntds.dit
Discovery	T1087	Account Discovery	Collect account information
	T1083	File and Directory Discovery	Collect file information
Lateral Movement	T1021.002	SMB/Windows Admin Shares	Spread malware to other systems via SMB
Collection	T1560.001	Archive Collected Data: Archive via Utility	Compress data witih WinRAR
	T1039	Data from Network Shared Drive	Collect data stored in Network Shared Drive
Command and Control	T1568.002	Dynamic Resolution: Domain Generation Algorithms	Change destination based on DGA

Table C-1: MirrorFace ATT&CK mapping

Appendix D: Enable "Audit Detailed File Share"

The audit policy on Windows OS can be configured in Group Policy Editor (gpedit.msc). Please enable it from Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Object Access >> "Audit

Detailed File Share".

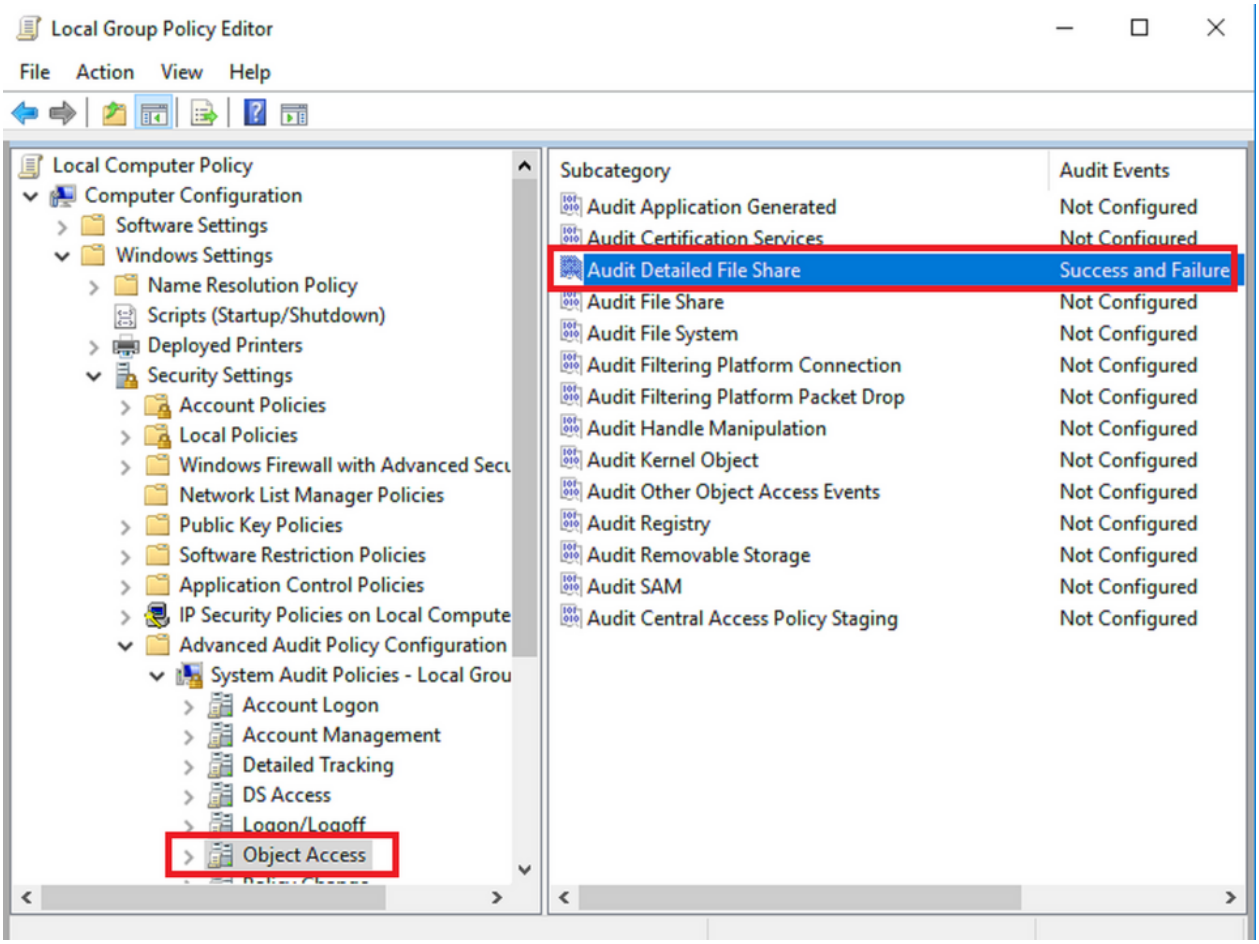
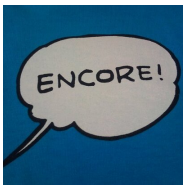


Figure 5: Group Policy Editor configuration

-
- Email

Author



朝長 秀誠 (Shusei Tomonaga)

Since December 2012, he has been engaged in malware analysis and forensics investigation, and is especially involved in analyzing incidents of targeted attacks. Prior to joining JPCERT/CC, he was engaged in security monitoring and analysis operations at a foreign-affiliated IT vendor. He presented at CODE BLUE, BsidesLV, BlackHat USA Arsenal, Botconf, PacSec and FIRST Conference. JSAC organizer.

Was this page helpful?

0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

please change the setting of your browser to set JavaScript valid. Thank you!

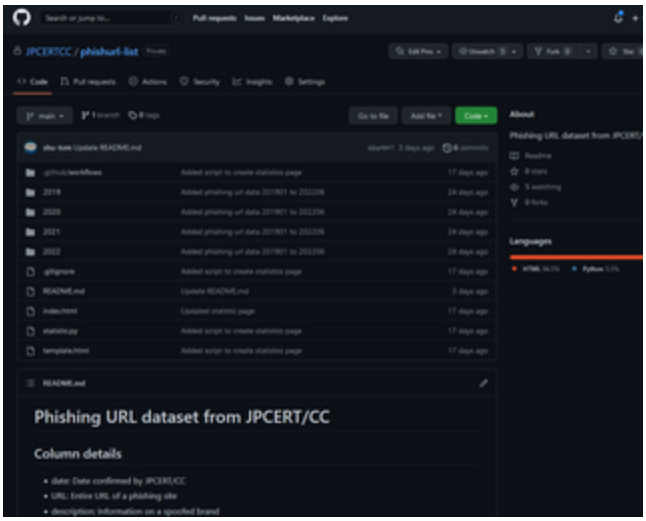
Related articles

- 

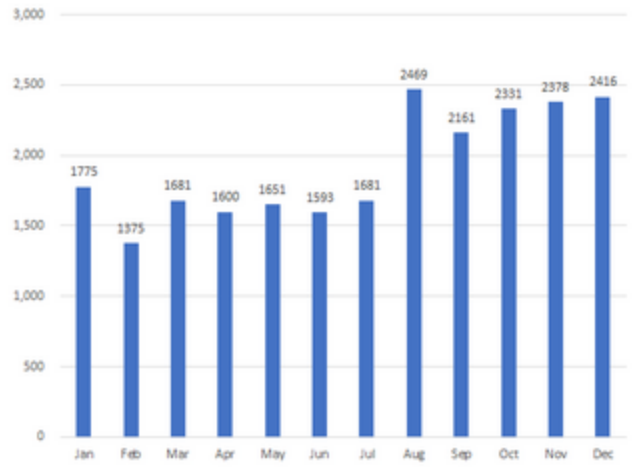
  Credential Theft and Domain Name Hijacking through Phishing Sites

- 

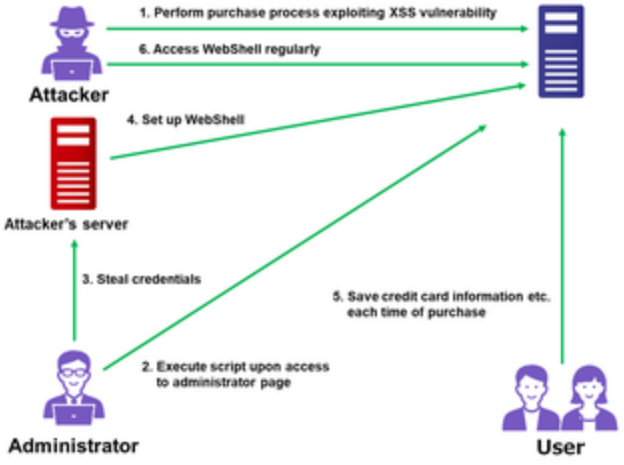
  F5 BIG-IP Vulnerability (CVE-2022-1388) Exploited by BlackTech

- 

  JPCERT/CC Releases URL Dataset of Confirmed Phishing Sites

- 

  Trends of Reported Phishing Sites and Compromised Domains in 2021

- 

  Attack Exploiting XSS Vulnerability in E-commerce Websites

Back
Top

Next