ESET RESEARCH

Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities

Share Article

ESET researchers discovered a spearphishing campaign targeting Japanese political entities a few weeks before the House of Councillors elections, and in the process uncovered a previously undescribed MirrorFace credential stealer

Dominik Breitenbacher

14 Dec 2022 • 13 min. read

ESET researchers discovered a spearphishing campaign, launched in the weeks leading up to the Japanese House of Councillors election in July 2022, by the APT group that ESET Research tracks as MirrorFace. The campaign, which we have named Operation LiberalFace, targeted Japanese political entities; our investigation revealed that the members of a specific political party were of particular focus in this campaign. ESET Research unmasked details about this campaign and the APT group behind it at the AVAR 2022 conference at the beginning of this month.

Key points of the blogpost:

- *At the end of June 2022, MirrorFace launched a campaign, which we have named Operation LiberalFace, that targeted Japanese political entities.*
- *Spearphishing email messages containing the group's flagship backdoor LODEINFO were sent to the targets.*
- *LODEINFO was used to deliver additional malware, exfiltrate the victim's credentials, and steal the victim's documents and emails.*
- *A previously undescribed credential stealer we have named MirrorStealer was used in Operation LiberalFace.*
- *ESET Research performed an analysis of the post-compromise activities, which suggests that the observed actions were carried out in a manual or semi-manual manner.*
- *Details about this campaign were shared at the AVAR 2022 conference.*

MirrorFace is a Chinese-speaking threat actor targeting companies and organizations based in Japan. While there is some speculation that this threat actor might be related to APT10 (Macnica, Kaspersky), ESET is unable to attribute it to any known APT group. Therefore, we are tracking it as a separate entity that we've named MirrorFace. In particular, MirrorFace and LODEINFO, its proprietary malware used exclusively against targets in Japan, have been reported as targeting

rganizations, and

nd exfiltration of files

these indicators:

ly used by MirrorFace.

rorFace targeting.

server that we track

ce posed as an official

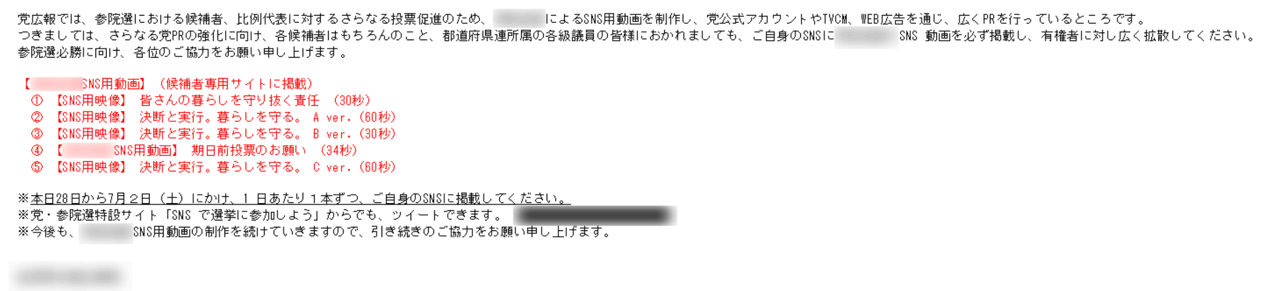
communication from the PR department of a specific Japanese political party, containing a request related to the House of Councillors elections, and was purportedly sent on behalf of a prominent politician. All spearphishing emails contained a malicious attachment that upon execution deployed LODEINFO on the compromised machine.

Additionally, we discovered that MirrorFace has used previously undocumented malware, which we have named MirrorStealer, to steal its target's credentials. We believe this is the first time this malware has been publicly described.

In this blogpost, we cover the observed post-compromise activities, including the C&C commands sent to LODEINFO to carry out the actions. Based on certain activities performed on the affected machine, we think that the MirrorFace operator issued commands to LODEINFO in a manual or semi-manual manner.

Initial access

MirrorFace started the attack on June 29th, 2022, distributing spearphishing emails with a malicious attachment to the targets. The subject of the email was <redacted>SNS用動画 拡散のお願い (translation from Google Translate: `[Important] <redacted> Request for spreading videos for SNS).` Figure 1 and Figure 2 show its content.



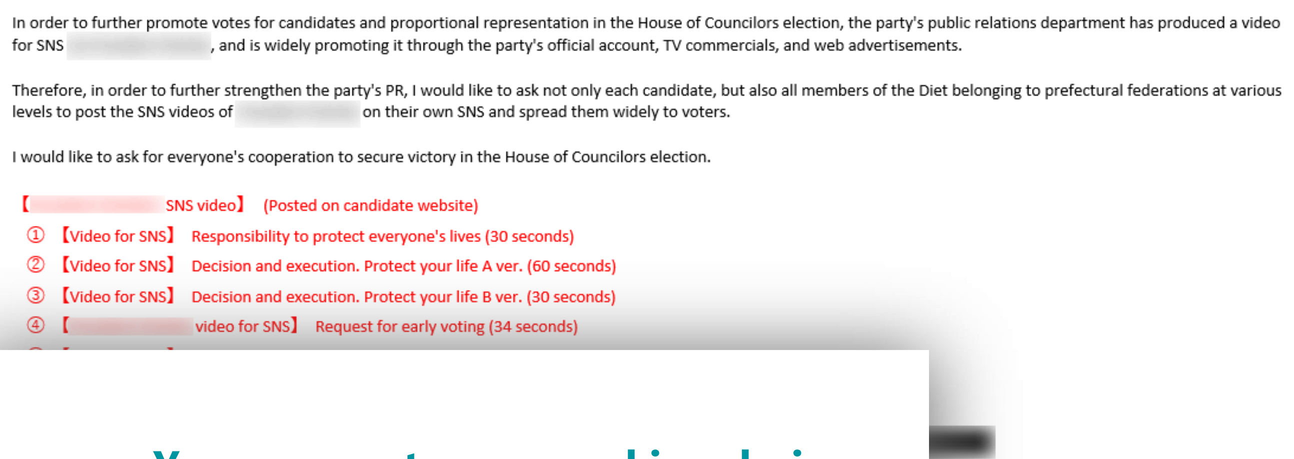
党広報では、参院選における候補者、比例代表に対するさらなる投票促進のため、[redacted]によるSNS用動画を制作し、党公式アカウントやTVCM、WEB広告を通じ、広くPRを行っているところです。
つきましては、さらなる党PRの強化に向け、各候補者はもちろんのこと、都道府県連所属の各級議員の皆様におかれましても、ご自身のSNSに[redacted]SNS 動画を必ず掲載し、有権者に対し広く拡散してください。
参院選必勝に向け、各位のご協力をお願い申し上げます。

【[redacted]SNS用動画】（候補者専用サイトに掲載）
① 【SNS用映像】 皆さんの暮らしを守り抜く責任 （30秒）
② 【SNS用映像】 決断と実行。暮らしを守る。 A ver.（60秒）
③ 【SNS用映像】 決断と実行。暮らしを守る。 B ver.（30秒）
④ 【[redacted]SNS用動画】 期日前投票のお願い （34秒）
⑤ 【SNS用映像】 決断と実行。暮らしを守る。 C ver.（60秒）

※本日28日から7月２日（土）にかけ、１日あたり１本ずつ、ご自身のSNSに掲載してください。
※党・参院選特設サイト「SNS で選挙に参加しよう」からでも、ツイートできます。[redacted]
※今後も、[redacted]SNS用動画の制作を続けていきますので、引き続きのご協力をお願い申し上げます。

[redacted]

Figure 1. Original text of the email



In order to further promote votes for candidates and proportional representation in the House of Councilors election, the party's public relations department has produced a video for SNS [redacted], and is widely promoting it through the party's official account, TV commercials, and web advertisements.

Therefore, in order to further strengthen the party's PR, I would like to ask not only each candidate, but also all members of the Diet belonging to prefectural federations at various levels to post the SNS videos of [redacted] on their own SNS and spread them widely to voters.

I would like to ask for everyone's cooperation to secure victory in the House of Councilors election.

【[redacted] SNS video】 (Posted on candidate website)
① 【Video for SNS】 Responsibility to protect everyone's lives (30 seconds)
② 【Video for SNS】 Decision and execution. Protect your life A ver. (60 seconds)
③ 【Video for SNS】 Decision and execution. Protect your life B ver. (30 seconds)
④ 【[redacted] video for SNS】 Request for early voting (34 seconds)

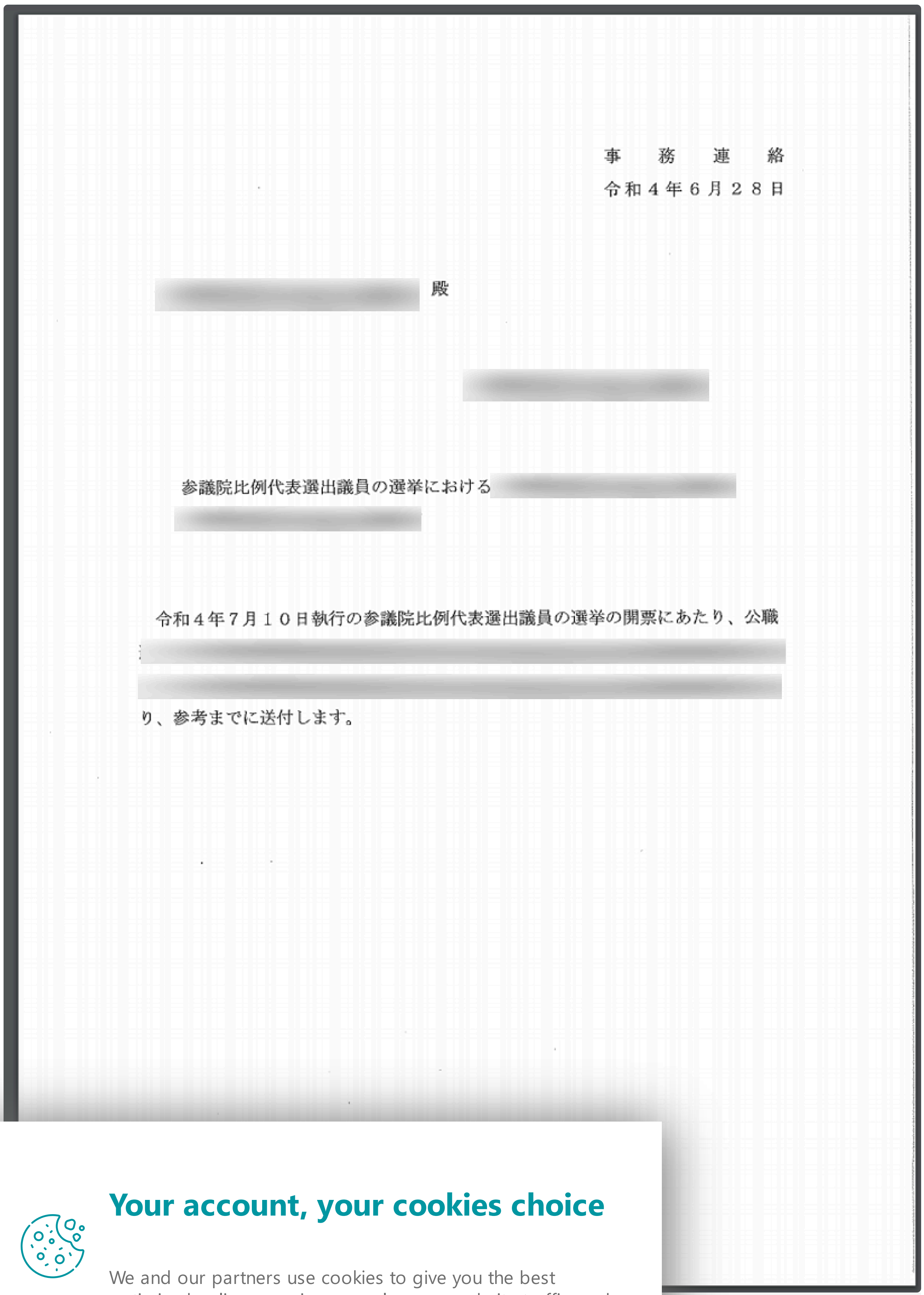
[redacted]

MirrorFace asked the
cial media profiles (SNS
PR and to secure
provides clear

, 2022, this email

clearly indicates that MirrorFace sought the opportunity to attack political entities. Also, specific content in the email indicates that members of a particular political party were targeted.

MirrorFace also used another spearphishing email in the campaign, where the attachment was titled 【参考】`220628`<redacted>発・<redacted>選挙管理委員会宛文書（添書分）`.exe` (translation from Google Translate: `[Reference] 220628 Documents from the Ministry of <redacted> to <redacted> election administration committee (appendix).exe`). The attached decoy document (shown in Figure 3) references the House of Councillors election as well.



事　務　連　絡
令和４年６月２８日

[redacted] 殿

[redacted]

参議院比例代表選出議員の選挙における[redacted]
[redacted]

令和４年７月１０日執行の参議院比例代表選出議員の選挙の開票にあたり、公職
[redacted]
り、参考までに送付します。

et

n the form of self-
ed>SNS用動画 拡散のお
`equest for`
redacted>発・
on from Google
Translate: `[Reference] 220628 Documents from the Ministry of`

`<redacted> to <redacted> election administration committee (appendix).exe)` respectively.

These EXEs extract their archived content into the `%TEMP%` folder. In particular, four files are extracted:

- `K7SysMon.exe`, a benign application developed by K7 Computing Pvt Ltd vulnerable to DLL search order hijacking
- `K7SysMn1.dll`, a malicious loader
- `K7SysMon.Exe.db`, encrypted LODEINFO malware
- A decoy document

Then, the decoy document is opened to deceive the target and to appear benign. As the last step, `K7SysMon.exe` is executed which loads the malicious loader `K7SysMn1.dll` dropped alongside it. Finally, the loader reads the content of `K7SysMon.Exe.db`, decrypts it, and then executes it. Note this approach was also observed by Kaspersky and described in their report.

Toolset

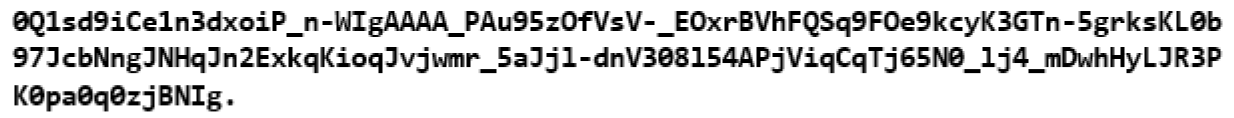
In this section, we describe the malware MirrorFace utilized in Operation LiberalFace.

LODEINFO

LODEINFO is a MirrorFace backdoor that is under continual development. JPCERT reported about the first version of LODEINFO (v0.1.2), which appeared around December 2019; its functionality allows capturing screenshots, keylogging, killing processes, exfiltrating files, and executing additional files and commands. Since then, we have observed several changes introduced to each of its versions. For instance, version 0.3.8 (which we first detected in June 2020) added the command ransom (which encrypts defined files and folders), and version 0.5.6 (which we detected in July 2021) added the command `config`, which allows operators to modify its configuration stored in the registry. Besides the JPCERT reporting mentioned above, a detailed analysis of the LODEINFO backdoor was also

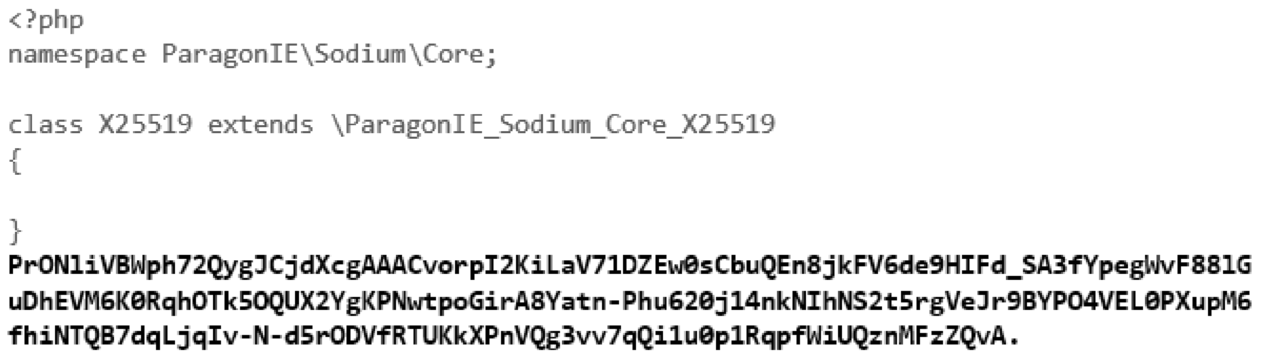
s utilizing both the
EINFO malware. The
ular LODEINFO by
-stage LODEINFO
plemented commands.
C&C command
issing.

en the regular
e LODEINFO, the C&C
ta. See Figure 4, Figure
e the prepended code
nd-stage C&C.



```
0Q1sd9iCe1n3dxoiP_n-WIgAAAA_PAu95zOfVsV-_EOxrBVhFQSq9FOe9kcyK3GTn-5grksKL0b
97JcbNngJNHqJn2ExkqKioqJvjwmr_5aJjl-dnV308154APjViqCqTj65N0_1j4_mDwhHyLJR3P
K0pa0q0zjBNIg.
```

Figure 4. Data received from the first-stage LODEINFO C&C

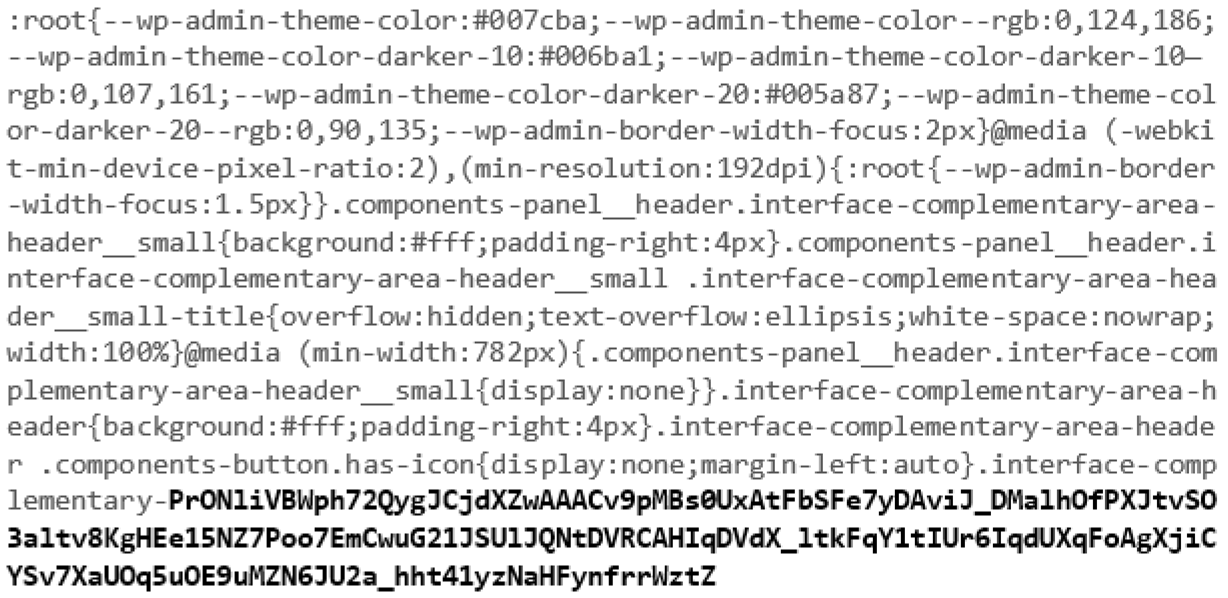


```
<?php
namespace ParagonIE\Sodium\Core;

class X25519 extends \ParagonIE_Sodium_Core_X25519
{

}
PrONliVBWph72QygJCjdXcgAAACvorpI2KiLaV71DZEw0sCbuQEn8jkFV6de9HIFd_SA3fYpegWvF881G
uDhEVM6K0RqhOTk5OQUX2YgKPNwtpoGirA8Yatn-Phu620j14nkNIhNS2t5rgVeJr9BYPO4VEL0PXupM6
fhiNTQB7dqLjqIv-N-d5rODVfRTUKkXPnVQg3vv7qQi1u0p1RqpfWiUQznMFzZQvA.
```

Figure 5. Data received from the second-stage C&C



```
:root{--wp-admin-theme-color:#007cba;--wp-admin-theme-color--rgb:0,124,186;
--wp-admin-theme-color-darker-10:#006ba1;--wp-admin-theme-color-darker-10—
rgb:0,107,161;--wp-admin-theme-color-darker-20:#005a87;--wp-admin-theme-col
or-darker-20--rgb:0,90,135;--wp-admin-border-width-focus:2px}@media (-webki
t-min-device-pixel-ratio:2),(min-resolution:192dpi){:root{--wp-admin-border
-width-focus:1.5px}}.components-panel__header.interface-complementary-area-
header__small{background:#fff;padding-right:4px}.components-panel__header.i
nterface-complementary-area-header__small .interface-complementary-area-hea
der__small-title{overflow:hidden;text-overflow:ellipsis;white-space:nowrap;
width:100%}@media (min-width:782px){.components-panel__header.interface-com
plementary-area-header__small{display:none}}.interface-complementary-area-h
eader{background:#fff;padding-right:4px}.interface-complementary-area-heade
r .components-button.has-icon{display:none;margin-left:auto}.interface-comp
lementary-PrONliVBWph72QygJCjdXZwAAACv9pMBs0UxAtFbSFe7yDAviJ_DMalhOfPXJtvSO
3altv8KgHEe15NZ7Poo7EmCwuG21JSUlJQNtDVRCAHIqDVdX_ltkFqY1tIUr6IqdUXqFoAgXjiC
YSv7XaUOq5uOE9uMZN6JU2a_hht41yzNaHFynfrrWztZ
```

Figure 6. Another data stream received from the second-stage C&C

MirrorStealer

e, is a credential
been publicly
various applications
targeted applications
pan. All the stolen
rorStealer doesn't have
her malware to do it.

commands that were

Initial environment observation

Once LODEINFO was launched on the compromised machines and they had successfully connected to the C&C server, an operator started issuing commands (see Figure 7).

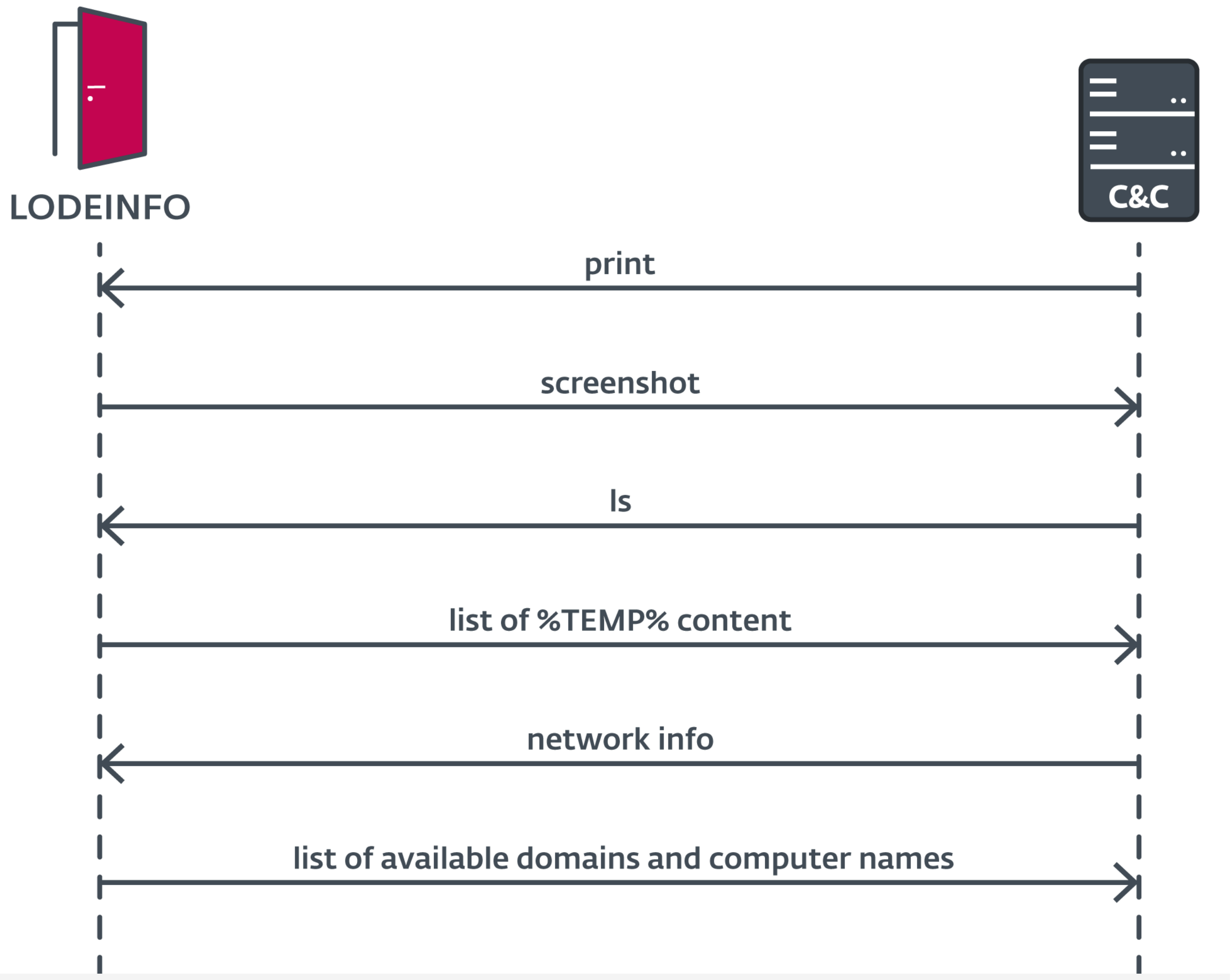
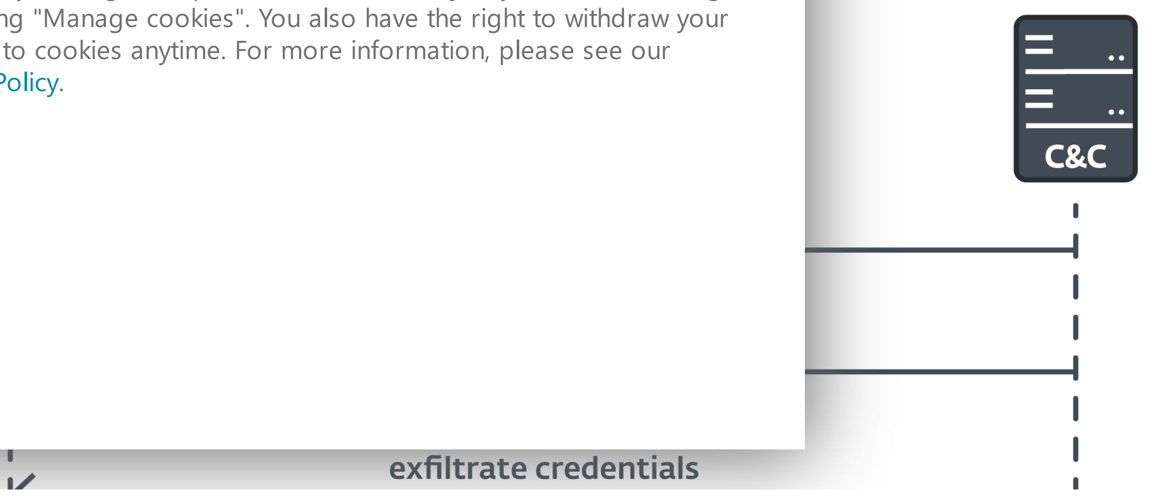


Figure 7. Initial environment observation by the MirrorFace operator via LODEINFO

First, the operator issued one of the LODEINFO commands, `print`, to capture the screen of the compromised machine. This was followed by another command, `ls`, to see the content of the current folder in which LODEINFO resided (i.e., `%TEMP%`). Right after that, the operator utilized LODEINFO to obtain network information by running `net view` and `net view /domain`. The first command returns the list of computers connected to the network, while the second returns the list of available domains.

Credential and browser cookie stealing

to the next phase (see



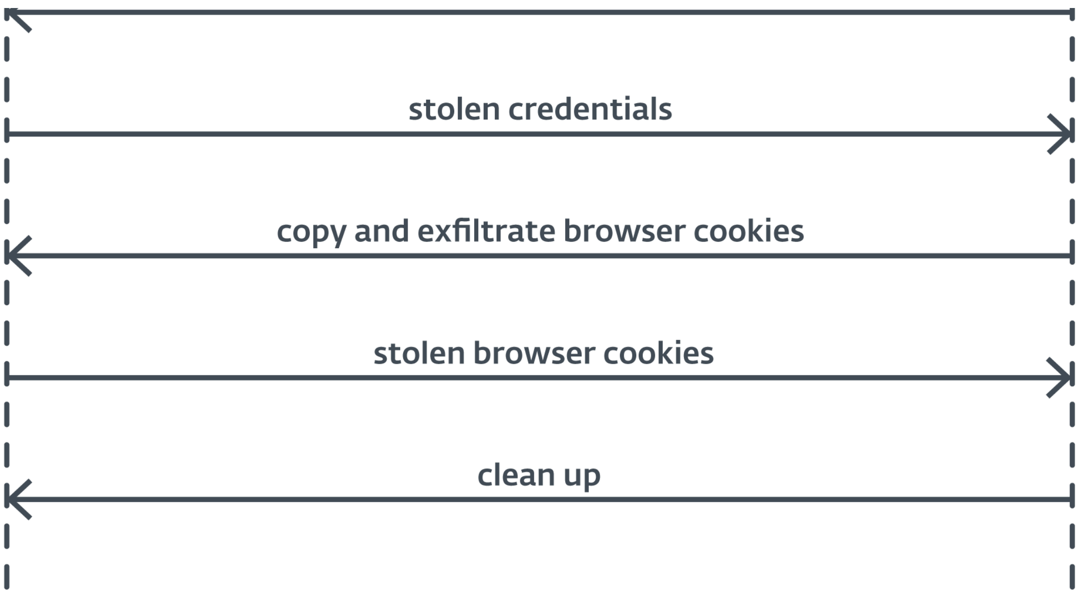


Figure 8. Flow of instructions sent to LODEINFO to deploy credential stealer, collect credentials and browser cookies, and exfiltrate them to the C&C server

The operator issued the LODEINFO command send with the subcommand –memory to deliver `MirrorStealer` malware to the compromised machine. The subcommand `–memory` was used to indicate to LODEINFO to keep MirrorStealer in its memory, meaning the MirrorStealer binary was never dropped on disk. Subsequently, the command `memory` was issued. This command instructed LODEINFO to take MirrorStealer, inject it into the spawned `cmd.exe` process, and run it.

Once MirrorStealer had collected the credentials and stored them in `%temp%\31558.txt`, the operator used LODEINFO to exfiltrate the credentials.

The operator was interested in the victim's browser cookies as well. However, MirrorStealer doesn't possess the capability to collect those. Therefore, the operator exfiltrated the cookies manually via LODEINFO. First, the operator used the LODEINFO command `dir` to list the contents of the folders `%LocalAppData%\Google\Chrome\User Data\` and `%LocalAppData%\Microsoft\Edge\User Data\`. Then, the operator copied all the identified cookie files into the `%TEMP%` folder. Next, the operator exfiltrated all the collected cookie files using the LODEINFO command `recv`. Finally, the operator deleted the copied cookie files from the `%TEMP%` folder in an attempt to remove the traces.

Document and email stealing

ous kinds as well as

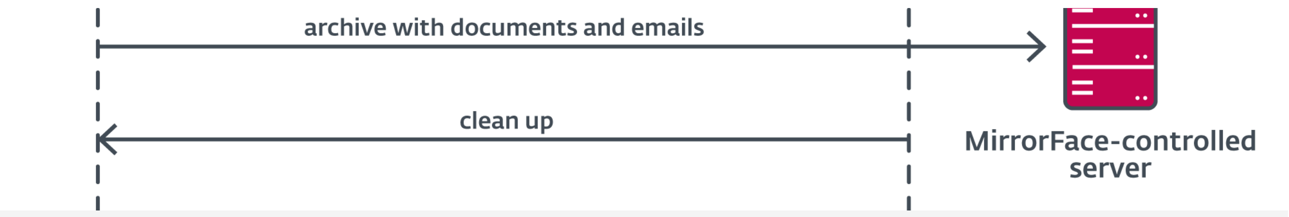

archive with documents and emails
clean up
MirrorFace-controlled server

Figure 9. Flow of the instructions sent to LODEINFO to exfiltrate files of interest

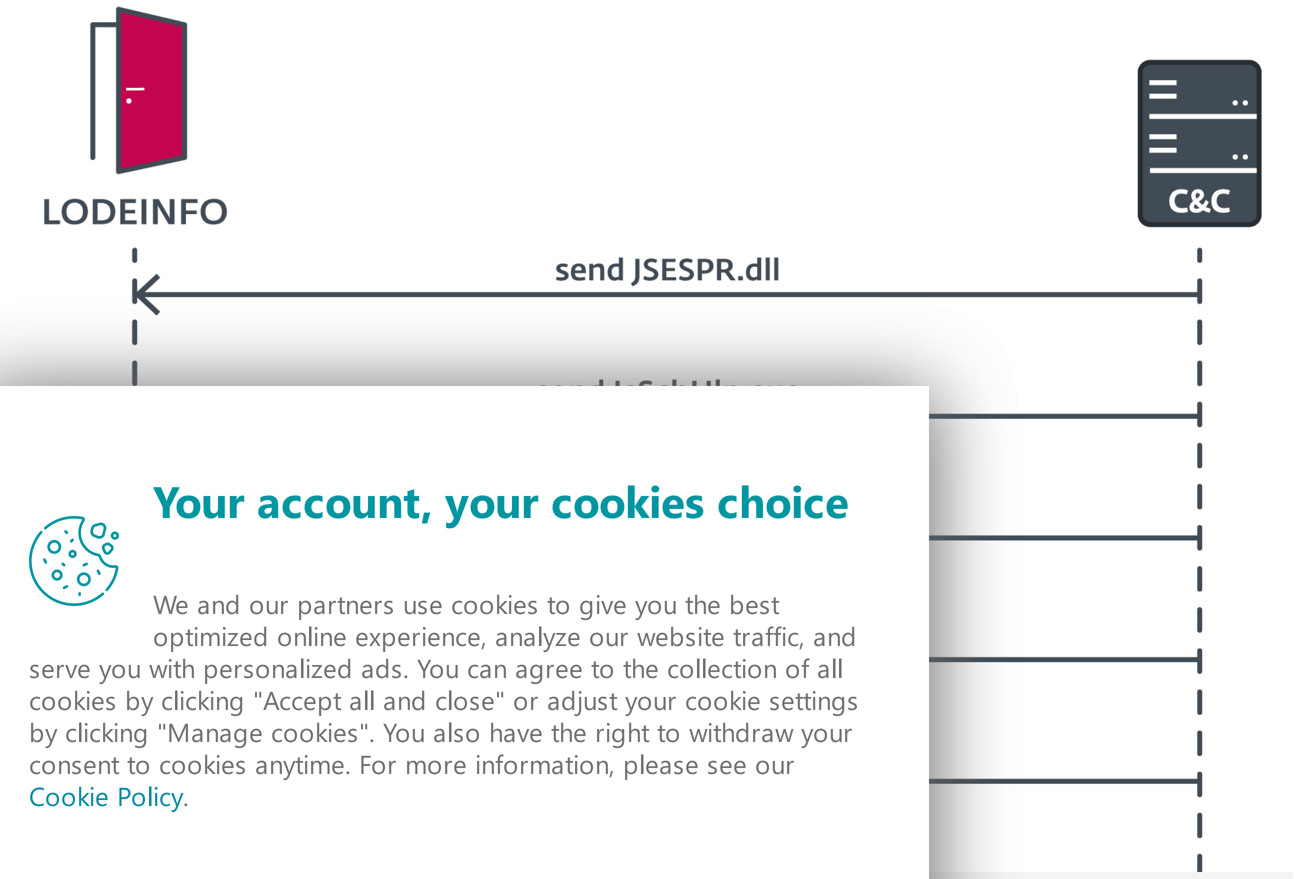
For that, the operator first utilized LODEINFO to deliver the WinRAR archiver (`rar.exe`). Using `rar.exe`, the operator collected and archived files of interest that were modified after 2022-01-01 from the folders `%USERPROFILE%\ and C:\$Recycle.Bin\`. The operator was interested in all such files with the extensions `.doc*`, `.ppt*`, `.xls*`, `.jtd`, `.eml`, `.*xps`, and `.pdf`.

Notice that besides the common document types, MirrorFace was also interested in files with the `.jtd` extension. This represents documents of the Japanese word processor Ichitaro developed by JustSystems.

Once the archive was created, the operator delivered the Secure Copy Protocol (SCP) client from the PuTTY suite (`pscp.exe`) and then used it to exfiltrate the just-created RAR archive to the server at `45.32.13[.]180`. This IP address had not been observed in previous MirrorFace activity and had not been used as a C&C server in any LODEINFO malware that we have observed. Right after the archive was exfiltrated, the operator deleted `rar.exe`, `pscp.exe`, and the RAR archive to clean up the traces of the activity.

Deployment of second-stage LODEINFO

The last step we observed was delivering the second-stage LODEINFO (see Figure 10).



nd-stage LODEINFO

`JsSchHlp.exe`, and `vcruntime140.dll` to the compromised machine. The original `JsSchHlp.exe` is vcruntime140.dll to the compromised machine. The original JsSchHlp.exe is a benign application signed by JUSTSYSTEMS CORPORATION (makers of the previously mentioned Japanese word processor, Ichitaro). However, in this case the MirrorFace operator abused a known Microsoft digital signature verification issue and appended RC4 encrypted data to the JsSchHlp.exe digital signature. Because of the mentioned issue, Windows still considers the modified JsSchHlp.exe to be validly signed.

JsSchHlp.exe is also susceptible to DLL side-loading. Therefore, upon execution, the planted JSESPR.dll is loaded (see Figure 11).

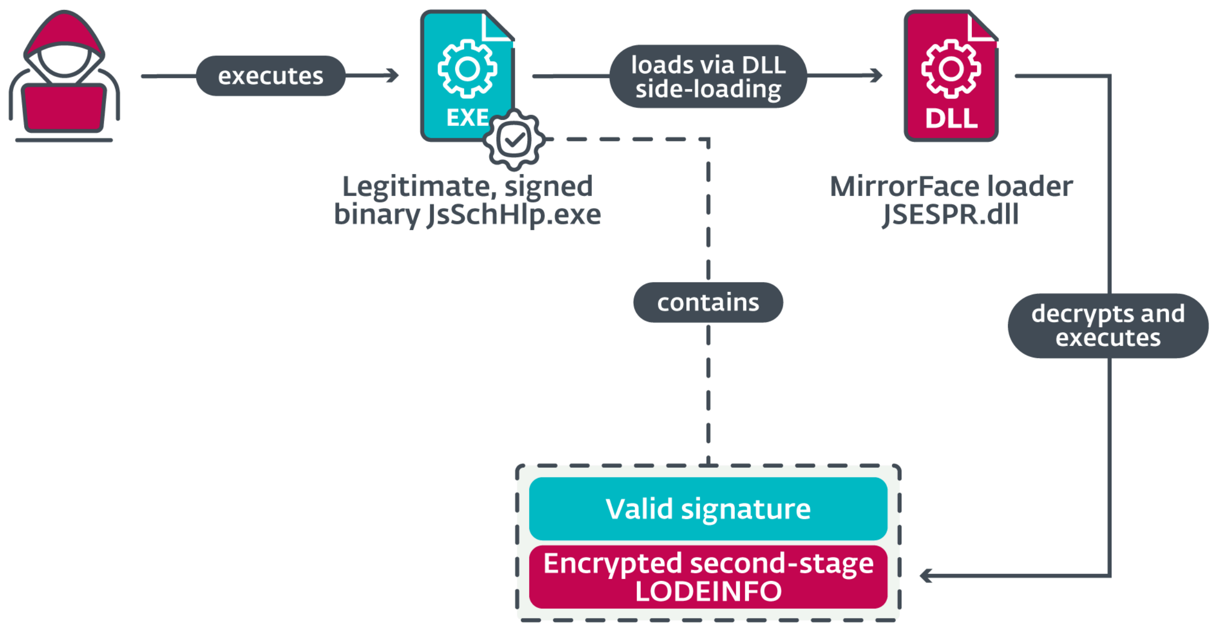

executes
EXE
Legitimate, signed binary JsSchHlp.exe
loads via DLL side-loading
DLL
MirrorFace loader JSESPR.dll
contains
decrypts and executes
Valid signature
Encrypted second-stage LODEINFO

Figure 11. Execution flow of second-stage LODEINFO

JSESPR.dll is a malicious loader that reads the appended payload from JsSchHlp.exe, decrypts it, and runs it. The payload is the second-stage LODEINFO, and once running, the operator utilized the regular LODEINFO to set the persistence for the second-stage one. In particular, the operator ran the reg.exe utility to add a value named JsSchHlp to the Run registry key holding the path to JsSchHlp.exe.

However, it appears to us the operator didn't manage to make the second-stage LODEINFO communicate properly with the C&C server. Therefore, any further steps of the operator utilizing the second-stage LODEINFO remain unknown to us.

ations. One of them is
g commands to
/c dir "c:\use\" to
dir "c:\users\".

FO in a manual or

ormed a few cleanups
delete
tials. Thus, at least this
us that the operator
was not thorough in the cleanup process.

Conclusion

MirrorFace continues to aim for high-value targets in Japan. In Operation LiberalFace, it specifically targeted political entities using the then-upcoming House of Councillors election to its advantage. More interestingly, our findings indicate MirrorFace particularly focused on the members of a specific political party.

During the Operation LiberalFace investigation, we managed to uncover further MirrorFace TTPs, such as the deployment and utilization of additional malware and tools to collect and exfiltrate valuable data from victims. Moreover, our investigation revealed that the MirrorFace operators are somewhat careless, leaving traces and making various mistakes.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
ESET Research also offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IoCs

Files

SHA-1	Filename	ESET detection
F4691FF3B3ACD15653684F372285CAC36C8D0AEF	K7SysMn1.dll	Win32/Agent.ACLP
DB81C8719DDAAE40C8D9B9CA103BBE77BE4FCE6C	K7SysMon.Exe.db	N/A
A8D2BE15085061B753FDEBBDB08D301A034CE1D5	JsSchHlp.exe	Win32/Agent.ACLP
		Win32/Agent.ACLP
		Win32/Agent.ACLP

Details

`5.8.95[.]174`	G-Core Labs S.A.	2022-06-13	LODEINFO C&C server.
`45.32.13[.]180`	AS-CHOOPA	2022-06-29	Server for data exfiltration.
`103.175.16[.]39`	Gigabit Hosting Sdn Bhd	2022-06-13	LODEINFO C&C server.
`167.179.116[.]56`	AS-CHOOPA	2021-10-20	`www.ninesmn[.]com`, second-stage LODEINFO C&C server.
`172.105.217[.]233`	Linode, LLC	2021-11-14	`www.aesorunwe[.]com`, second-stage LODEINFO C&C server.

MITRE ATT&CK techniques

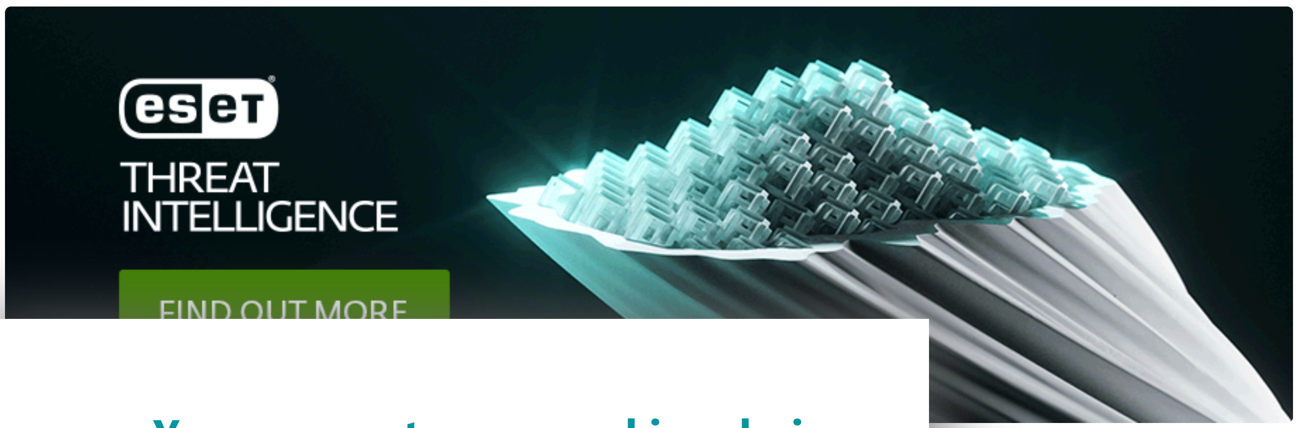
This table was built using version 12 of the MITRE ATT&CK framework**.**

Note that although this blogpost does not provide a complete overview of LODEINFO capabilities because this information is already available in other publications, the MITRE ATT&CK table below contains all techniques associated with it.

Tactic	ID	Name	Description
Initial Access	T1566.001	Phishing: Spearphishing Attachment	A malicious WinRAR SFX archive is attached to a spearphishing email.
	T1106	Native API	LODEINFO can execute files using the `CreateProcessA` API.
			rFace operators rely on a n opening a malicious chment sent via email.
			EINFO can execute mands via Component ct Model.
			EINFO adds an entry to `HKCU Run` key to ensure stence.
		Keys / Startup Folder	bserved MirrorFace ators manually adding an entry to the `HKCU Run` key to

			ensure persistence for the second-stage LODEINFO.
Defense Evasion	T1112	Modify Registry	LODEINFO can store its configuration in the registry.
	T1055	Process Injection	LODEINFO can inject shellcode into `cmd.exe`.
	T1140	Deobfuscate/Decode Files or Information	LODEINFO loader decrypts a payload using a single-byte XOR or RC4.
	T1574.002	Hijack Execution Flow: DLL Side-Loading	MirrorFace side-loads LODEINFO by dropping a malicious library and a legitimate executable (e.g., `K7SysMon.exe`).
Discovery	T1082	System Information Discovery	LODEINFO fingerprints the compromised machine.
	T1083	File and Directory Discovery	LODEINFO can obtain file and directory listings.
	T1057	Process Discovery	LODEINFO can list running processes.
	T1033	System Owner/User Discovery	LODEINFO can obtain the victim's username.
	T1614.001	System Location Discovery: System Language Discovery	LODEINFO checks the system language to verify that it is not running on a machine set to use the English language.
			bserved MirrorFace ators archiving collected using the RAR archiver.
			bserved MirrorFace ators collecting stored l messages.
			EINFO performs gging.
			EINFO can obtain a screenshot.

	T1005	Data from Local System	We observed MirrorFace operators collecting and exfiltrating data of interest.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	LODEINFO uses the HTTP protocol to communicate with its C&C server.
	T1132.001	Data Encoding: Standard Encoding	LODEINFO uses URL-safe base64 to encode its C&C traffic.
	T1573.001	Encrypted Channel: Symmetric Cryptography	LODEINFO uses AES-256-CBC to encrypt C&C traffic.
	T1001.001	Data Obfuscation: Junk Data	Second-stage LODEINFO C&C prepends junk to sent data.
Exfiltration	T1041	Exfiltration Over C2 Channel	LODEINFO can exfiltrate files to the C&C server.
	T1071.002	Application Layer Protocol: File Transfer Protocols	We observed MirrorFace using Secure Copy Protocol (SCP) to exfiltrate collected data.
Impact	T1486	Data Encrypted for Impact	LODEINFO can encrypt files on the victim's machine.



Related Articles

ESET RESEARCH
CloudScout: Evasive Panda scouting cloud services

ESET RESEARCH
ESET Research Podcast: CosmicBeetle

ESET RESEARCH
Embargo ransomware: Rock'n'Rust

Discussion

What do you think?
0 Responses

👍 Upvote 😝 Funny 😍 Love 😯 Surprised 😤 Angry 😢 Sad

0 Comments 1 **Login ▾**

Start the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS ?

Best **Newest** **Oldest**