APT & Targeted Attacks

Earth Lusca Uses Geopolitical Lure to Target Taiwan Before Elections

During our monitoring of Earth Lusca, we noticed a new campaign that used Chinese-Taiwanese relations as a social engineering lure to infect selected targets.

By: Cedric Pernet, Jaromir Horejsi
February 26, 2024
Read time: 7 min (1993 words)

Introduction

Trend Micro previously published a number of entries discussing the operations of a China-linked threat actor we track as Earth Lusca. The group, which has been active since at least 2020 and has regularly changed its modus operandi, has been known to launch several different campaigns at the same time.

During our monitoring of this threat actor, we noticed a new campaign that used Chinese-Taiwanese relations as a social engineering lure to infect selected targets. We attribute this campaign to Earth Lusca with high confidence based on the tools, techniques, and procedures (TTPs) we observed in previous research.

document discussing Chinese-Taiwanese geopolitical issues. This file was created just two days before the Taiwanese national elections and the document seems to be a legitimate document stolen from a geopolitical expert from Taiwan.

Note that a recent leak of private documents provides a new attribution path to a Chinese company called I-Soon. We discuss these connections in a separate section in this entry. There is significant overlap between the victims, malware used, and probable location of Earth Lusca and I-Soon. This suggests, at the very least, a significant connection between these groups. Our research is continuing at this time.

Earth Lusca attack chain

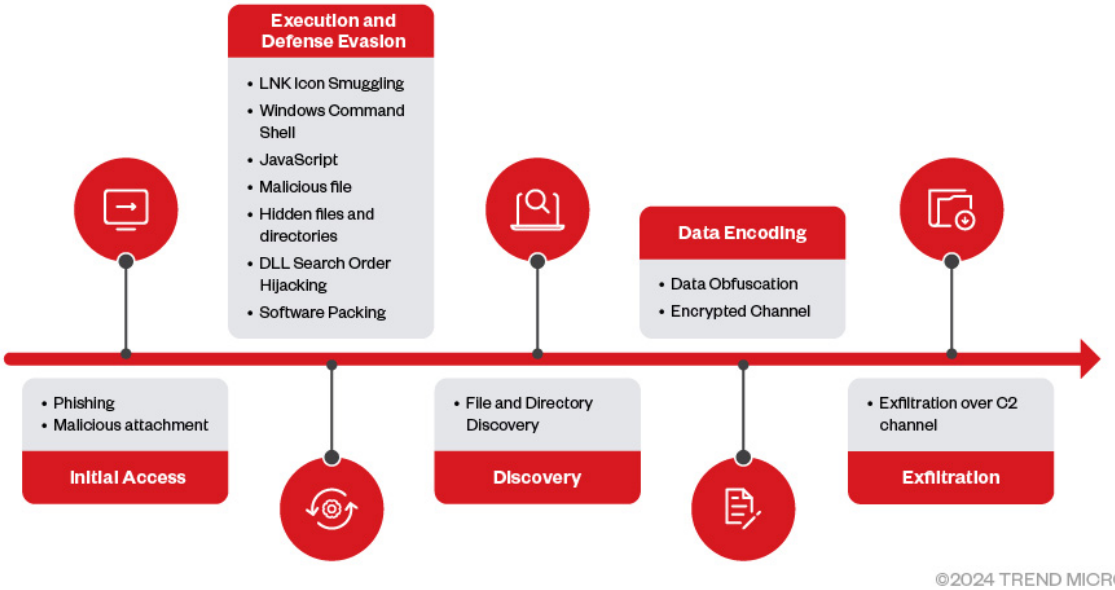

Figure 1. The infection chain used in the campaign

Initial access via spear phishing

an archive (.7z), named China's gray zone warfare against Taiwan. Based on the threat actor's previous activities, we suspect this file was sent to the targets via email, either embedded as an attachment or as a link.

The archive consists of a folder named "China's gray zone warfare against Taiwan" that contains two different Windows shortcut files (.LNK) and a subfolder named "__MACOS".

```
1520427 Jan 11 07:33 China's_gray_zone_warfare_against_Taiwan.doc.lnk
1737269 Jan 11 07:34 China_paper.pdf.lnk
    128 Jan 11 07:34 __MACOS/
```

Figure 2. The content of the 7-Zip archive

The __MACOS subfolder name resembles the legitimate __MACOSX folder name created by macOS, which is hidden by default and is used to store each folder's various settings. In the case we analyzed, the __MACOS folder does not contain any metadata but instead hides another stage of the malicious payload.

The __MACOS subfolder contains two files named "*_params.cat.js*" and "*_params2.cat.js*".

All the files show metadata indicating that the files were last modified on Jan. 11, 2024.

First stage: Shortcut (LNK) file with hidden target attribute

The LNK files, once selected, executes the JavaScript code stored in the __MACOS folder.

followed by space characters, as can be seen in Figures 3 and 4.

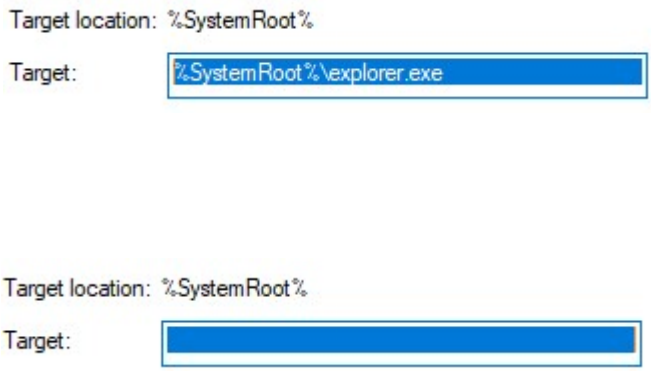

Figure 3. Beginning (top) and end (bottom) of the "target" property field (space characters are in blue)

The threat actor inserted 255 space characters in the "arguments" attribute before including the actual path to the malicious script to ensure that users don't notice anything is amiss.

Tools such as LNK parser reveal the entire content of the "arguments" field:

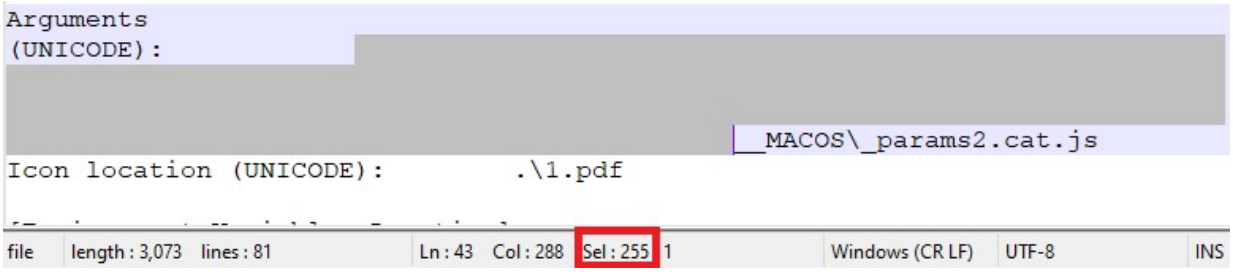

Figure 4. 255 space characters were used before the actual argument value.

Second stage: Obfuscated JavaScript file

The second stage is obfuscated with Dean Edward's JavaScript Packer, a tool designed to obfuscate JavaScript code to hinder analysis and detections.

Third stage: Deobfuscated JavaScript file and dropper

The third stage drops a text file containing hexadecimal data to the *%APPDATA%\Roaming* directory.

```
new ActiveXObject("WScript.Shell");file.WriteLine(
"4d534346000000005a950b00000000002c0000000000000000
```

Figure 6. The text string with “4d534346 = MSCF” marker is written to a temporary file.

This text file contains a magic signature, *4d534346*, which is the Microsoft Cabinet File (MSCF) signature of a cabinet archive. The JavaScript then uses a living-off-the-land technique and calls a few LOLBins to decode a hexadecimal string to the binary file (*certutil.exe*) and unpack the cabinet archive (*expand.exe*).

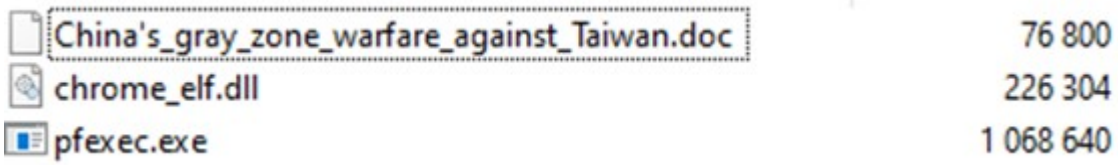

Figure 7. Content of cabinet archive

The extracted cabinet archive contains a decoy file, a signed legitimate executable file, and a malicious DLL library.

In the cases we observed, we found the decoy files to be either Microsoft Word documents, Microsoft PowerPoint documents, or PDF documents. Although these were written by professionals involved in political relations between China and Taiwan, we could not find any of these documents

compromise of their systems.

The signed legitimate executable file, *360se.exe* from Qihoo 360, was renamed to *pfexec.exe* by Earth Lusca in a case of DLL hijacking. Once executed, it launches the DLL contained in the same folder (*chrome_elf.dll*).

Fourth stage: Cobalt Strike stageless client (malicious obfuscated DLL library)

The last stage of the infection chain is a stageless Cobalt Strike payload. The noteworthy parameters extracted from the embedded configuration are listed here:

```
C2Server                          -
upserver.updateservice.store,/common.html
HttpPostUri                       - /r-arrow
Watermark                         - 100000000
```

Similar attacks

During the monitoring of this campaign, we received more archives using similar structures and employing comparable tricks but having different file names, decoy names, and command-and-control (C&C) servers, among others.

One such noteworthy file, another 7z archive file named "*ppt-cih1w4.7z*", contained a folder named "*Sino-Africa_relations*" as seen in Figure 8:

Figure 8. Content of the 7-Zip archive

The folder also contained an LNK file and a __MACOS folder with payload, this time timestamped Dec. 22, 2023.

Similar to the previously analyzed archive, several stages lead to this last stage (namely Cobalt Strike), only with different configurations. The C&C server name abuses the name of the cybersecurity company Cybereason. The malleable profile is also different this time and uses different URLs, although the watermark remains the same.

```
C2Server                          -
www.cybereason.xyz,/mobile-android
HttpPostUri                       - /RELEASE_NOTES
Watermark                         - 100000000
```

Attack started shortly before 2024

As mentioned in the introduction, the campaign exposed in this report was likely active between December 2023 and January 2024, with the lure document created just two days before the Taiwanese national elections.

The C&C domain used by Earth Lusca (*updateservice[.]store*) was registered anonymously on Dec. 12, 2023 and a subdomain was used for C&C communications (*upserver.updateservice[.]store*).

Meanwhile, the other C&C domain used in this attack campaign (*Cybereason[.]xyz*) was registered anonymously on Oct. 27, 2023.

We also found evidence that Earth Lusca targeted a Taiwan-based private academic think tank dedicated to the study of international political and economic situations.

While we could not find other campaign targets at the time of writing, we suspect Earth Lusca might be planning to attack more politically related entities.

The I-Soon lead

A recent leak on GitHub exposed sizeable data on a Chinese company called I-Soon that has seemingly been active since 2016. The company describes itself on its website as an "APT Defense and Research Laboratory" and provides descriptions of its services: offensive and defensive security, antifraud solutions, blockchain forensics solutions, security products, and more. The group also notes several law enforcement and government entities with which it collaborates. As an interesting aside, I-Soon had been the recipient of a few rounds of fundings since 2017. One of its investors was the antivirus company Qihoo from China — which, as stated earlier, had an executable file abused for DLL hijacking.

We found a few indicators in the I-Soon leak that made us believe that some of the Earth Lusca activities are similar to the contents of the leak:

1. **There is some victim overlap between Earth Lusca and I-Soon: Some of the names on the victim lists of the I-Soon leak were also victims of Earth Lusca's attacks.**
2. **The malware and tools arsenal used by I-Soon and Earth Lusca has a few strong overlaps. Malware such as ShadowPad, Winnti and a few other tools have been used extensively by Earth Lusca and are used by i-Soon as well.**

Conclusion

Earth Lusca remains an active threat actor that counts cyberespionage among its primary motivations. Organizations must remain vigilant against APT groups employing sophisticated TTPs. In particular, government organizations face potential harm that could affect not only national and economic security but also international relations if malicious actors were to succeed in stealing classified information. Meanwhile, businesses that fall prey to cyberespionage attacks might face a decline in customer trust and operational disruptions that in turn lead to financial repercussions.

Given Earth Lusca's penchant for using email, resorting to social engineering as one of its main avenues of infection, and capitalizing on relevant social and political issues as seen in this campaign, we advise individuals and organizations to adhere to security best practices, such as avoiding clicking on suspicious email and website links and updating software in a timely manner to minimize the chances of falling victim to an Earth Lusca attack

MITRE ATT&CK techniques

Below listed techniques are subset of MITRE ATT&CK list..

Tactic	Technique	ID	Description
Initial Access	Phishing: Spear-phishing Link	T1566.002	Used to send spear-phishing emails with a malicious attachment in an attempt to gain

Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	cmd to execute various commands and payloads.
Execution	Command and Scripting Interpreter: JavaScript	T1059.007	Used to execute various commands and payloads.
Execution	User Execution: Malicious Link	T1204.001	An adversary may rely upon a user clicking a malicious link in order to gain execution.
Execution	User Execution: Malicious File	T1204.002	An adversary may rely upon a user opening a malicious file in order to gain execution.
Defense Evasion	Deobfuscate/Decode Files or Information	T1140	Used Obfuscated Files or Information to hide artifacts of an intrusion from analysis
Defense Evasion	Hide Artifacts: Hidden Files and Directories	T1564.001	Set files and directories to be hidden to evade detection mechanisms.
Defense Evasion	Hijack Execution Flow: DLL Search Order Hijacking	T1574.001	Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs.
Defense Evasion	Indirect Command Execution	T1202	Used to abuse utilities that allow for command execution to bypass security restrictions that limit the use of

Defense Evasion	Masquerading: Double File Extension	T1036.007	double extension in the filename as a means of masquerading the true file type.
Defense Evasion	Obfuscated Files or Information: Software Packing	T1027.002	Adversaries may perform software packing or virtual machine software protection to conceal their code.
Defense Evasion	Obfuscated Files or Information: Embedded Payloads	T1027.009	Adversaries may embed payloads within other files to conceal malicious content from defenses.
Defense Evasion	Obfuscated Files or Information: LNK Icon Smuggling	T1027.012	Adversaries may smuggle commands to download malicious payloads past content filters by hiding them within otherwise seemingly benign windows shortcut files.
Discovery	File and Directory Discovery	T1083	Adversaries may enumerate files and directories.
Command and Control	Data Encoding	T1132	Adversaries may encode data to make the content of command and control traffic more difficult to detect.
Command and Control	Data Obfuscation	T1001	Adversaries may obfuscate command and control traffic to

Command and Control	Encrypted Channel	T1573	employ a known encryption algorithm to conceal command and control traffic.
Exfiltration	Exfiltration Over C2 Channel	T1041	Adversaries may steal data by exfiltrating it over an existing command and control channel.

The final payload, Cobalt Stike, might use additional techniques listed on the MITRE website.

Indicators of Compromise (IOCs)

The indicators of compromise for this entry can be found here.

We'd like to thank Trend's Ian Kenefick and Cyris Tseng for additional intelligence.

Tags

APT & Targeted Attacks | Malware | Endpoints | Research | Articles, News, Reports

Cedric Pernet
Sr. Threat Researcher

Jaromir Horejsi
Threat Researcher

CONTACT US

SUBSCRIBE

Related Articles

ICO Scams Leverage 2024 Olympics to Lure Victims, Use AI for Fake Sites

Attackers in Profile: menuPass and ALPHV/BlackCat

Omdia Report: Trend Disclosed 60% of Vulnerabilities

See all articles ›

Resources

Support

About Trend

Country Headquarters

Trend Micro - United States (US)

225 East John Carpenter Freeway
Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900

Select a country / region

United States