Rare Backdoors Suspected to be Tied to Gelsemium APT Found in Targeted Attack in Southeast Asian Government

Lior Rochberger, Tom Fakterman, Robert Falcone ⋮⋮ 9/22/2023

By Lior Rochberger, Tom Fakterman and Robert Falcone

September 22, 2023 at 6:05 AM

Category: Government

This post is also available in: 日本語 (Japanese)

Executive Summary

A cluster of threat actor activity that Unit 42 observed attacking a Southeast Asian government target could provide insight into a rarely seen, stealthy APT group known as Gelsemium.

We found this activity as part of an investigation into compromised environments within a Southeast Asian government. We identified the cluster as CL-STA-0046.

This unique cluster had activity spanning over six months between 2022-2023. It featured a combination of rare tools and techniques that the threat actor leveraged to gain a clandestine foothold and collect intelligence from sensitive IIS servers belonging to a government entity in Southeast Asia.

In addition to an array of web shells, the main backdoors used by the threat actor were OwlProxy and SessionManager. This combination, which was publicly documented once before in 2020, is rare and was previously used to target several entities in Laos.

Based on our analysis and available threat intelligence, we attribute CL-STA-0046 to the Gelsemium APT group, with a moderate level of confidence. The observations we describe here could provide a view into a threat group about which only a handful of public reports have been published to date.

According to research published by ESET, the Gelsemium APT group has been operational since at least 2014. It is recognized for its tendency to target a diverse range of entities, including governments, universities, electronics manufacturers and religious organizations, predominantly in East Asia and the Middle East.

Despite Gelsemium's long-standing presence in the threat landscape, limited information has been available about their tactics, techniques, and procedures (TTPs). Our analysis and description of this cluster of activities provides deep technical insights into the tools and strategies that this APT group might employ.

Additionally, we provide a documented timeline of the operations we observed, presenting a repository of indicators for defenders.

Palo Alto Networks customers receive protections against the threats discussed in this article through Advanced WildFire, Advanced URL Filtering, DNS Security, Cortex XDR and Cortex XSIAM, as detailed in the conclusion.

Organizations can engage the Unit 42 Incident Response team for specific assistance with this threat and others.

Related Unit 42 Topics **Government**, APTs

Table of Contents

Timeline of Activity

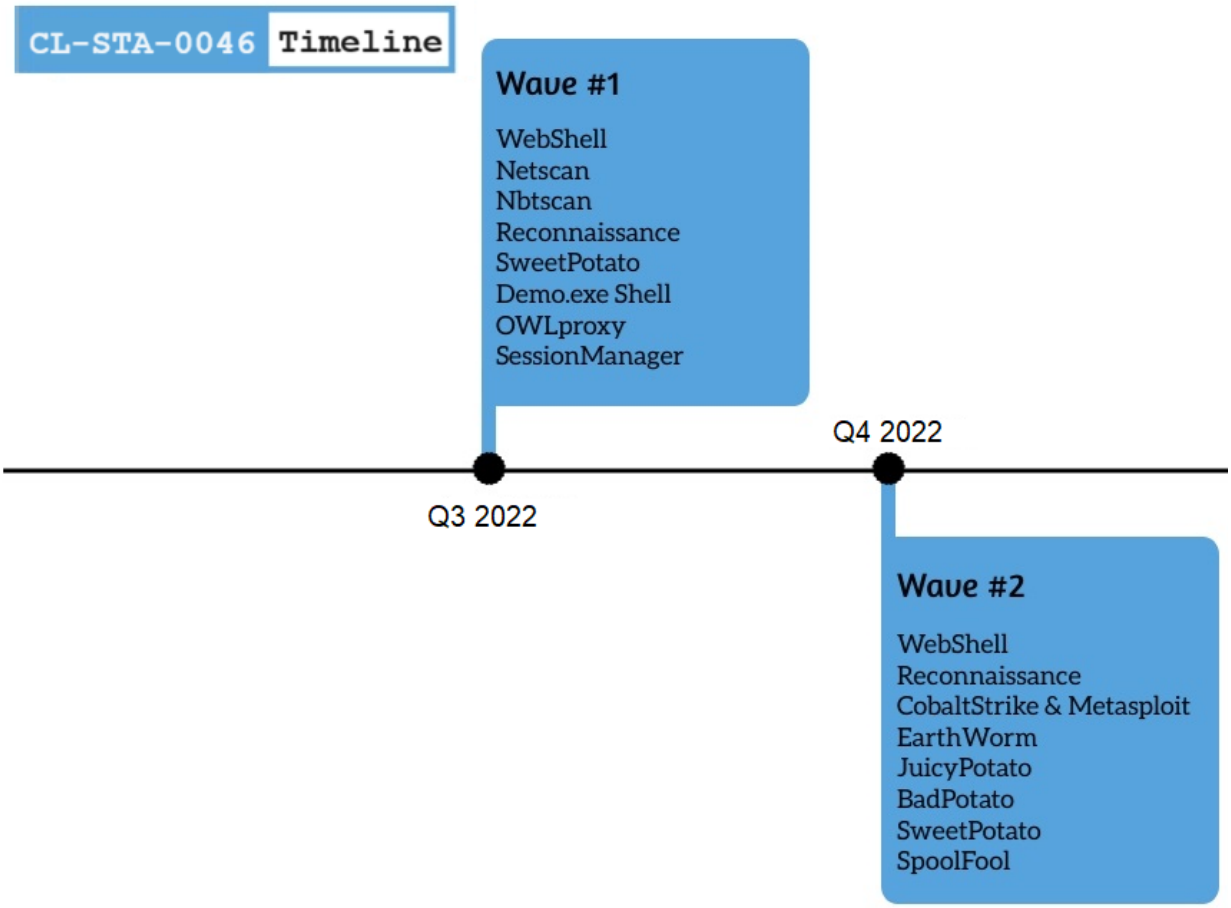

Figure 1. Timeline of CL-STA-0046.

CL-STA-0046 Details

Infection Vector

The threat actor behind CL-STA-0046 gained access to the environment after installing several web shells on a compromised web server. Among the types of web shells observed are the following:

- reGeorg
- China Chopper
- AspxSpy web shell

One of the AspxSpy web shells that we saw the threat actor behind CL-STA-0046 use was reportedly used by Iron Taurus (aka APT 27) for operation Iron Tiger in 2015 (according to Trend Micro). However, this particular web shell is publicly available and could be used by any threat actor (and was therefore not included in our attribution consideration).

The attackers conducted additional activities using the web shells. They moved laterally via SMB and downloaded additional tools. Initially, the attackers performed basic reconnaissance commands such as ipconfig and whoami. Later, they used netscan and nbtscan to gather further information about the victim.

In some instances, we observed that the attackers started to deliver tools to the compromised server. The attackers used a “shell-like” tool named demo.exe to run additional commands, and they used the Potato Suite (JuicyPotato – j.exe, BadPotato and SweetPotato – ev.exe) to try to perform privilege escalation.

Installing Additional Tools and Malware

To gain a foothold in the environment, the attackers behind CL-STA-0046 downloaded several different tools. Some of these tools attackers rarely use, and when other researchers have observed attackers using them in the past, it was sophisticated APT groups.

We will describe the following tools we observed in further sections:

- OwlProxy
- SessionManager
- Cobalt Strike
- SpoolFool
- EarthWorm

The attackers checked connectivity to the internet, as shown in Figure 2, by pinging www.qq[.]com. This site is a well-known Chinese web portal.

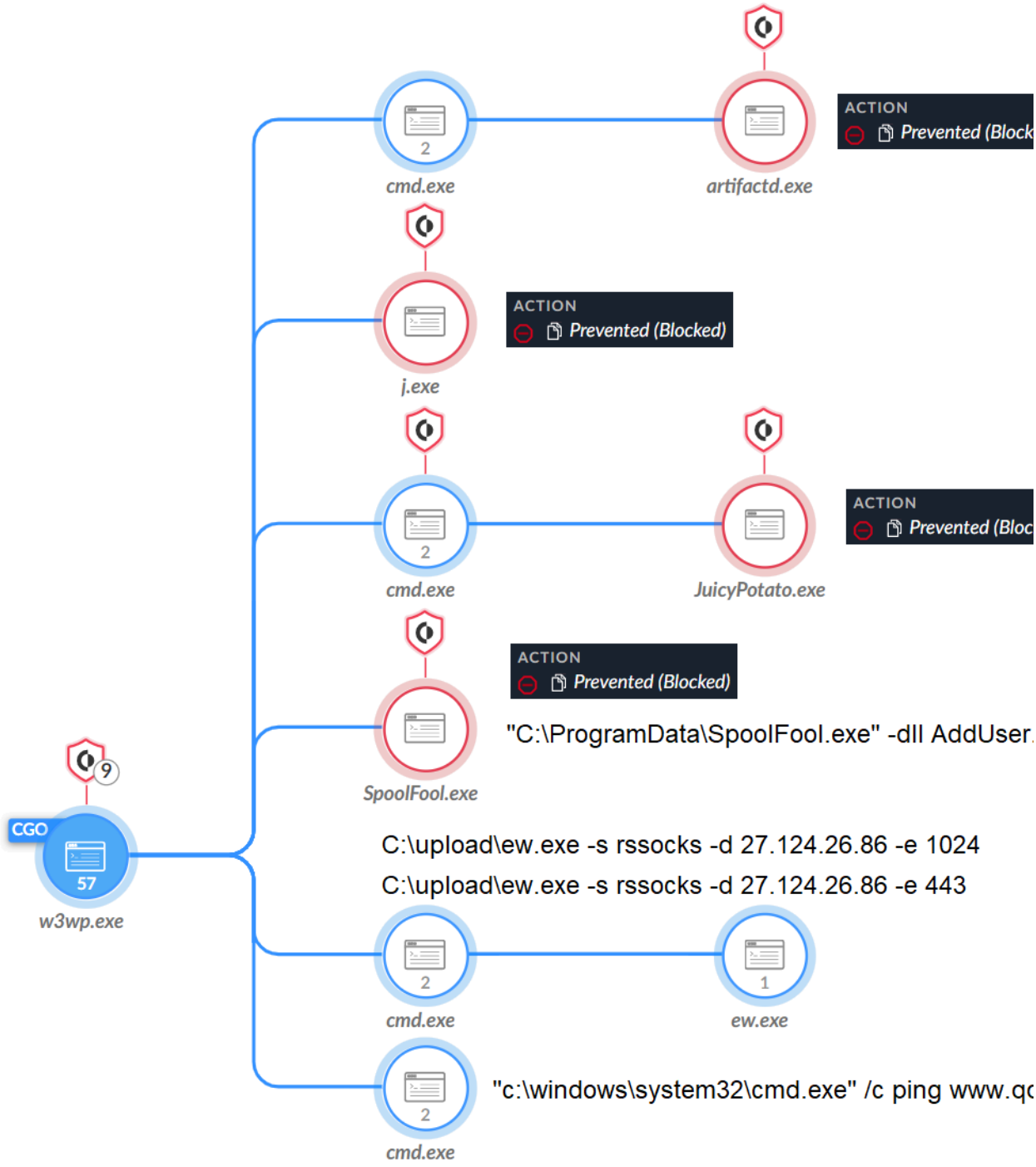

Figure 2. Process tree of Cobalt Strike, the Potato Suite, SpoolFool and EarthWorm.

SessionManager

During our investigation, there were several unsuccessful attempts to install a variant of the SessionManger IIS backdoor on a compromised web server. Cortex XDR blocked these attempts automatically.

SessionManager is a unique custom backdoor that allows its operators to run commands, as well as uploading files to and downloading them from the web server. This threat also allows attackers to use the web server as a proxy to communicate with additional systems on the network.

According to a Kaspersky blog published in June 2022, the Gelsemium APT group used SessionManager in compromises dating back to at least March 2021. Attackers specifically used it in government, nongovernment, military and industrial organizations.

The SessionManager sample we observed in CL-STA-0046 was designed to inspect all inbound HTTP requests and look for requests containing a specifically crafted Cookie field within the HTTP request.

The Cookie field would contain the actor's desired command. SessionManager supports the following commands:

- Uploading files to the server
- Downloading files from the server
- Running commands and applications
- Proxying connections to additional systems

The proxy functionality offered by SessionManager suggests the actors wanted to use the server as an ingress point to communicate with other systems on the network.

OwlProxy Malware

Another unique and custom tool that attackers used was OwlProxy. OwlProxy is an HTTP proxy with backdoor functionality that was first discovered in April 2020 in an attack targeting the Taiwanese government. The attack, which was part of a campaign targeting governmental entities in East Asia and the Middle East, was attributed to Gelsemium.

The threat actor deployed an executable that saved an embedded DLL to c:\windows\system32\wmipd.dll and created a service named WMI Provider to run the DLL.

The wmipd.dll DLL is a variant of OwlProxy that differs slightly from those discussed in the April 2020 attacks in Taiwan. This variant of OwlProxy creates an HTTP service that will handle inbound HTTP requests to URLs based on the following UrlPrefix formats:

- HTTPS://+:443/topics/
- HTTPS://+:443/topics/pp/

The DLL checks incoming requests that match these URLs for s?pa= and s?pp= to run commands or to set up a proxy, respectively. Like the SessionManager tool, the proxy functionality within OwlProxy furthers the theme of the actors planning to use the server as a gateway to other systems on the network.

As part of CL-STA-0046 activities, the attackers tried to execute the OwProxy malware (named client.exe) but Cortex XDR prevented the execution. After being thwarted, the attackers tried using a replacement for the tool that is not necessarily malicious on its own, called EarthWorm.

Cobalt Strike

The attackers attempted to execute Artifactd.exe, as shown in Figure 2 above, which is a Cobalt Strike beacon configured to communicate with the command and control (C2) 27.124.26[.]83.

EarthWorm

EarthWorm is a publicly available SOCKS tunneler that, although initially created for research purposes, gained popularity among Chinese-speaking actors. For example, Kaspersky reported that APT 27 used EarthWorm in a campaign targeting Asian government entities.

The use of EarthWorm by the threat actor behind CL-STA-0046 occurred after the attackers failed to execute OwlProxy, and we assess that they delivered EarthWorm as a replacement.

As shown in Figure 2 above, the attackers used EarthWorm (ew.exe) to create a tunnel to their C2 traffic that was hosted on 27.124.26[.]86. This tunnel allowed the attackers to connect the local area network (LAN) of the infected network to their external C2. Figure 3 shows a screenshot of the EarthWorm website.

Figure 3. Screenshot from the EarthWorm website.

Using EarthWorm, the attackers sent and received data to and from their C2 server.

SpoolFool

In addition to using the Potato Suite mentioned above, the attackers also used another local privilege escalation (LPE) proof of concept (PoC) published on GitHub called SpoolFool, as shown in Figure 2 above. This tool exploits CVE-2022-21999 (Windows Print Spooler Elevation of Privilege Vulnerability).

The attackers used this tool to attempt to create a local administrator user (username admin with the default password Passw0rd!) using the following command.

```
"C:\ProgramData\SpoolFool.exe" -dll AddUser.dll
```

Attribution

Unit 42 assesses with moderate confidence that the activity observed in CL-STA-0046 is associated with the Gelsemium APT group.

This assessment is based on the unique combination of malware that attackers used in CL-STA-0046, namely the SessionManager IIS backdoor and OwlProxy. At the time of writing this report, the only publicly available report about attackers using SessionManager and OwlProxy in conjunction is a report about the Gelsemium APT group.

In addition, there is a victimology overlap between CL-STA-0046 and Gelsemium. Researchers from ESET have reported that this threat group has targeted the government sector in Southeast Asia in the past.

Gelsemium has been in operation since 2014. Publicly available research reports that this group targets governments, and that they have been operating in Southeast Asia in the past. Although the researchers who first discovered Gelsemium did not attribute it to any specific state, the security firm Telsy and the Thai CERT consider this group to be operating from China. At the time of writing this report, Unit 42 cannot confirm these attribution claims.

Conclusion

CL-STA-0046 is one of three clusters that we observed targeting the government sector in a country in Southeast Asia. Unit 42 associates the activity observed by the threat actor behind CL-STA-0046 to the Gelsemium APT group with a moderate level of confidence.

As part of the activity we observed, the threat actor received access through the use of several web shells, following the attempted installation of multiple types of proxy malware and an IIS backdoor. As some of the threat actor's attempts to install malware were unsuccessful, they kept delivering new tools, showing their ability to adapt to the mitigation process.

The findings of this investigation highlight the urgent need for enhanced security measures, vigilant monitoring and proactive threat intelligence sharing among government entities and affected industries in Southeast Asia. By adopting a multilayered defense approach and staying informed about emerging threats, organizations can better protect themselves against the persistent and evolving tactics employed by threat actors such as Gelsemium.

Protections and Mitigations

For Palo Alto Networks customers, our products and services provide the following coverage associated with the threats described above:

- WildFire cloud-based threat analysis service accurately identifies the known samples as malicious.
- Advanced URL Filtering and DNS Security identify domains associated with this group as malicious.
- Cortex XDR and XSIAM
    - Prevents the execution of known malicious malware
    - Prevents the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module
    - Protects against credential gathering tools and techniques using the new Credential Gathering Protection available from Cortex XDR 3.4
    - Protects from threat actors dropping and executing commands from web shells using Anti-Webshell Protection, newly released in Cortex XDR 3.4
    - Protects against exploitation of different vulnerabilities including ProxyShell and ProxyLogon using the Anti-Exploitation modules as well as Behavioral Threat Protection
    - Cortex XDR Pro detects postexploit activity, including credential-based attacks, with behavioral analytics

If you think you may have been impacted or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Web Shells

- 24eb9c77448dda2d7cfecc60c804a378e89cbd450fbf7f4db875eb131cd4510a
- 4dcdce3fd7f0ab80bc34b924ecaa640165ee49aa1a22179b3f580b2f74705dd9
- 96bc4853d5a0c976fb7a02d747cd268fb2dfc8c2361d68bb4ffcc16adec5ea19
- ac115bfa8d36cf31046b8ccce30e9ebcede899395d56400955f95e242d5c9c75
- 17392669a04f17fda068d18ae5850d135f3912d08b4e2eee81fce915849887b3
- 3be95477e1d9f3877b4355cff3fbcdd3589bb7f6349fd4ba6451e1e9d32b7fa6
- 181feef51991b162bdff5d49bb7fd368d9ec2b535475b88bc197d70d73eef886
- 61de79db5ed022ee9376e86a2094a51cf3b31fa6bce126cbcdacad33469c752f

The Potato Suite

- c7bd78b9a68198b8787d28ba5094827eb99a0798719bcb140f3afb695925566c
- fd0b9f09770685ed6f40ecabcd31bc467fa22801164b52fdc638334009b7c06f
- 77e82c3d5fea369f6598339dcd97b73f670ff0ad373bf7fc3a2d8586f58d9d32
- f0761ad307781bdf8da94765abd1a2041ac12a52c7fdde85f00b2b2cab6d6ce8
- 29cc79a451f73bac43dbe9455d2184770beae69f4e6bc2d824abd2cfbedf53f1
- 3268f269371a81dbdce8c4eedffd8817c1ec2eadec9ba4ab043cb779c2f8a5d2

Demo.exe

- 527063cb9da5eec2e4b290019eaac5edd47ff3807fec74efa0f1b7ddf5a1b271

OwlProxy

- 2f3abc59739b248ee26a575700eef93b18bd2029eb9f8123598ffdd81fa54d8b

SessionManager

- b9a9e43e3d10cf6b5548b8be78e01dc0a034955b149a20e212a79a2cf7bee956

Cobalt Strike

- ff7485d30279f78aba29326d9150b8c302294351e716ece77f4a3b890008e5fe

SpoolFool

- c0a7a797f39b509fd2d895b5731e79b57b350b85b20be5a51c0a1bda19321bd0

EarthWorm

- c254dc53b3cf9c7d81d92f4e060a5c44a4f51a228049fd1e2d90fafa9c0a44ee

Infrastructure

- 27.124.26[.]83
- 27.124.26[.]86