Sep 25 2023

NETMANAGEIT

Intelligence Report

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

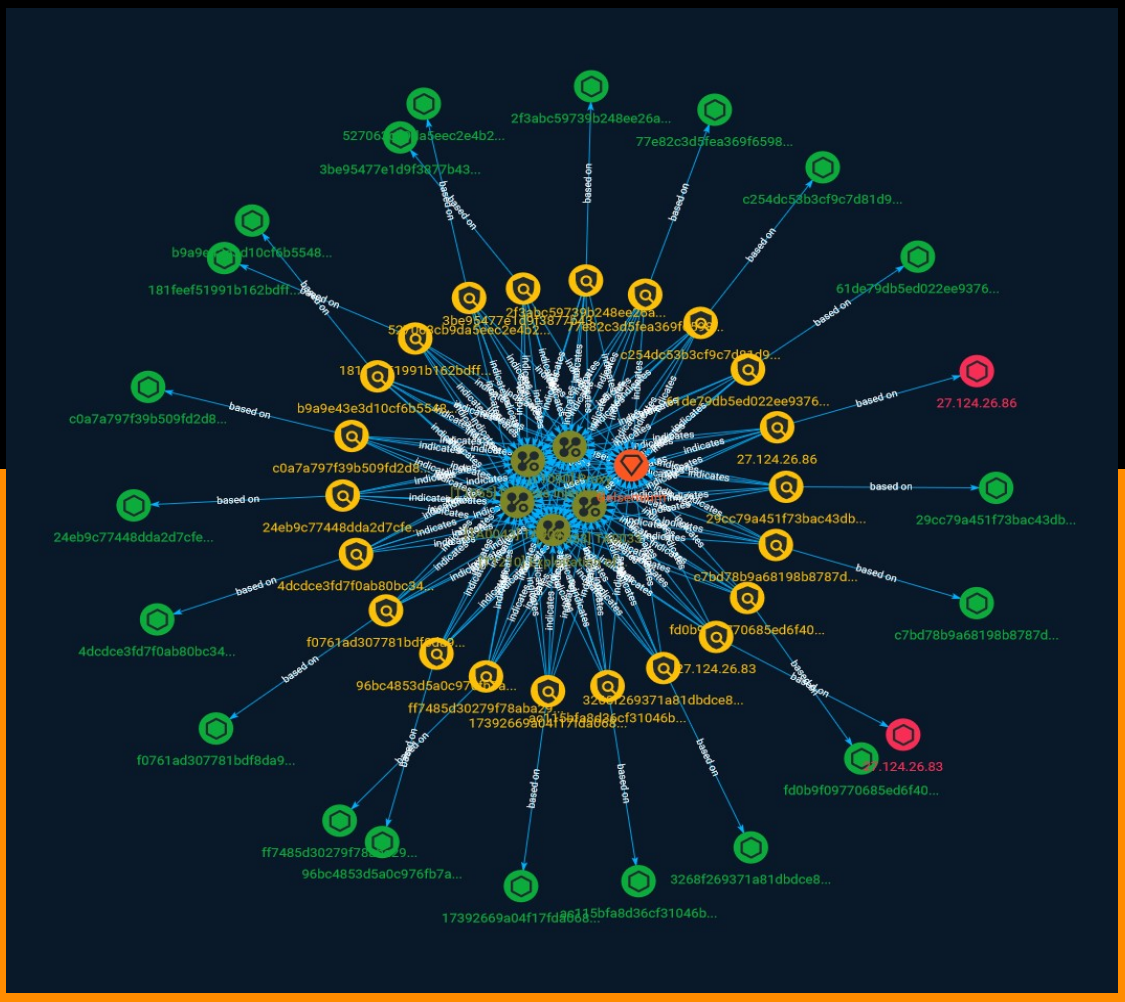

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Attack-Pattern 5
- Indicator 8
- Intrusion-Set 18

Observables

- StixFile 19
- IPv4-Addr 21

External References

- External References 22

Overview

Description

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.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
Process Injection
ID
T1055
Description
Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.
Name
Exploitation of Remote Services
ID
T1210

Description

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources. There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169) Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to

avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name
TA0033
ID
TA0033
Name
TA0043
ID
TA0043

Indicator

Name
c0a7a797f39b509fd2d895b5731e79b57b350b85b20be5a51c0a1bda19321bd0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c0a7a797f39b509fd2d895b5731e79b57b350b85b20be5a51c0a1bda19321bd0']
Name
27.124.26.86
Description
CC=IN ASN=AS64050 BGPNET Global ASN
Pattern Type
stix
Pattern

[ipv4-addr:value = '27.124.26.86']

Name

ff7485d30279f78aba29326d9150b8c302294351e716ece77f4a3b890008e5fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ff7485d30279f78aba29326d9150b8c302294351e716ece77f4a3b890008e5fe']

Name

3be95477e1d9f3877b4355cff3fbcdd3589bb7f6349fd4ba6451e1e9d32b7fa6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3be95477e1d9f3877b4355cff3fbcdd3589bb7f6349fd4ba6451e1e9d32b7fa6']

Name

fd0b9f09770685ed6f40ecabcd31bc467fa22801164b52fdc638334009b7c06f

Description

TEL:Exploit:Win32/ShellPdb.B

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fd0b9f09770685ed6f40ecabcd31bc467fa22801164b52fdc638334009b7c06f']
Name
4dcdce3fd7f0ab80bc34b924ecaa640165ee49aa1a22179b3f580b2f74705dd9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4dcdce3fd7f0ab80bc34b924ecaa640165ee49aa1a22179b3f580b2f74705dd9']
Name
c254dc53b3cf9c7d81d92f4e060a5c44a4f51a228049fd1e2d90fafa9c0a44ee
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c254dc53b3cf9c7d81d92f4e060a5c44a4f51a228049fd1e2d90fafa9c0a44ee']

Name

ac115bfa8d36cf31046b8ccce30e9ebcede899395d56400955f95e242d5c9c75

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ac115bfa8d36cf31046b8ccce30e9ebcede899395d56400955f95e242d5c9c75']

Name

181feef51991b162bdff5d49bb7fd368d9ec2b535475b88bc197d70d73eef886

Description

Backdoor:ASP/Ace.T

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '181feef51991b162bdff5d49bb7fd368d9ec2b535475b88bc197d70d73eef886']

Name

29cc79a451f73bac43dbe9455d2184770beae69f4e6bc2d824abd2cfbedf53f1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29cc79a451f73bac43dbe9455d2184770beae69f4e6bc2d824abd2cfbedf53f1']

Name

96bc4853d5a0c976fb7a02d747cd268fb2dfc8c2361d68bb4ffcc16adec5ea19

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '96bc4853d5a0c976fb7a02d747cd268fb2dfc8c2361d68bb4ffcc16adec5ea19']

Name

2f3abc59739b248ee26a575700eef93b18bd2029eb9f8123598ffdd81fa54d8b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f3abc59739b248ee26a575700eef93b18bd2029eb9f8123598ffdd81fa54d8b']

Name

27.124.26.83

Description

CC=IN ASN=AS64050 BGPNET Global ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '27.124.26.83']

Name

24eb9c77448dda2d7cfecc60c804a378e89cbd450fbf7f4db875eb131cd4510a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '24eb9c77448dda2d7cfecc60c804a378e89cbd450fbf7f4db875eb131cd4510a']

Name

61de79db5ed022ee9376e86a2094a51cf3b31fa6bce126cbcdacad33469c752f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '61de79db5ed022ee9376e86a2094a51cf3b31fa6bce126cbcdacad33469c752f']

Name

17392669a04f17fda068d18ae5850d135f3912d08b4e2eee81fce915849887b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '17392669a04f17fda068d18ae5850d135f3912d08b4e2eee81fce915849887b3']

Name

527063cb9da5eec2e4b290019eaac5edd47ff3807fec74efa0f1b7ddf5a1b271

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '527063cb9da5eec2e4b290019eaac5edd47ff3807fec74efa0f1b7ddf5a1b271']

Name

c7bd78b9a68198b8787d28ba5094827eb99a0798719bcb140f3afb695925566c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7bd78b9a68198b8787d28ba5094827eb99a0798719bcb140f3afb695925566c']

Name

f0761ad307781bdf8da94765abd1a2041ac12a52c7fdde85f00b2b2cab6d6ce8

Description

Trojan:Win32/Skeeyah.A!rfn

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0761ad307781bdf8da94765abd1a2041ac12a52c7fdde85f00b2b2cab6d6ce8']

Name

77e82c3d5fea369f6598339dcd97b73f670ff0ad373bf7fc3a2d8586f58d9d32

Description

HackTool:Win32/Badcastle.A!dha

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77e82c3d5fea369f6598339dcd97b73f670ff0ad373bf7fc3a2d8586f58d9d32']

Name

3268f269371a81dbdce8c4eedffd8817c1ec2eadec9ba4ab043cb779c2f8a5d2

Description

VirTool:Win32/Tater.A!MTB

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3268f269371a81dbdce8c4eedffd8817c1ec2eadec9ba4ab043cb779c2f8a5d2']

Name

b9a9e43e3d10cf6b5548b8be78e01dc0a034955b149a20e212a79a2cf7bee956

Description

Win64:MalwareX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b9a9e43e3d10cf6b5548b8be78e01dc0a034955b149a20e212a79a2cf7bee956']

Intrusion-Set

Name
Gelsemium

Description
[Gelsemium](https://attack.mitre.org/groups/G0141) is a cyberespionage group that has been active since at least 2014, targeting governmental institutions, electronics manufacturers, universities, and religious organizations in East Asia and the Middle East. (Citation: ESET Gelsemium June 2021)

StixFile

Value
4dcdce3fd7f0ab80bc34b924ecaa640165ee49aa1a22179b3f580b2f74705dd9
fd0b9f09770685ed6f40ecabcd31bc467fa22801164b52fdc638334009b7c06f
29cc79a451f73bac43dbe9455d2184770beae69f4e6bc2d824abd2cfbedf53f1
3268f269371a81dbdce8c4eedffd8817c1ec2eadec9ba4ab043cb779c2f8a5d2
181feef51991b162bdff5d49bb7fd368d9ec2b535475b88bc197d70d73eef886
c7bd78b9a68198b8787d28ba5094827eb99a0798719bcb140f3afb695925566c
3be95477e1d9f3877b4355cff3fbcdd3589bb7f6349fd4ba6451e1e9d32b7fa6
24eb9c77448dda2d7cfecc60c804a378e89cbd450fbf7f4db875eb131cd4510a
ac115bfa8d36cf31046b8ccce30e9ebcede899395d56400955f95e242d5c9c75
77e82c3d5fea369f6598339dcd97b73f670ff0ad373bf7fc3a2d8586f58d9d32
2f3abc59739b248ee26a575700eef93b18bd2029eb9f8123598ffdd81fa54d8b
61de79db5ed022ee9376e86a2094a51cf3b31fa6bce126cbcdacad33469c752f
527063cb9da5eec2e4b290019eaac5edd47ff3807fec74efa0f1b7ddf5a1b271

c254dc53b3cf9c7d81d92f4e060a5c44a4f51a228049fd1e2d90fafa9c0a44ee

96bc4853d5a0c976fb7a02d747cd268fb2dfc8c2361d68bb4ffcc16adec5ea19

c0a7a797f39b509fd2d895b5731e79b57b350b85b20be5a51c0a1bda19321bd0

b9a9e43e3d10cf6b5548b8be78e01dc0a034955b149a20e212a79a2cf7bee956

17392669a04f17fda068d18ae5850d135f3912d08b4e2eee81fce915849887b3

ff7485d30279f78aba29326d9150b8c302294351e716ece77f4a3b890008e5fe

f0761ad307781bdf8da94765abd1a2041ac12a52c7fdde85f00b2b2cab6d6ce8

IPv4-Addr

Value
27.124.26.86
27.124.26.83

External References

- https://otx.alienvault.com/pulse/6511ba926fead70098c83c17
- https://unit42.paloaltonetworks.com/rare-possible-gelsemium-attack-targets-se-asia/