Mar 26 2024

NETMANAGEIT

Intelligence Report

The Updated APT Playbook: Tales from the Kimsuky threat actor group

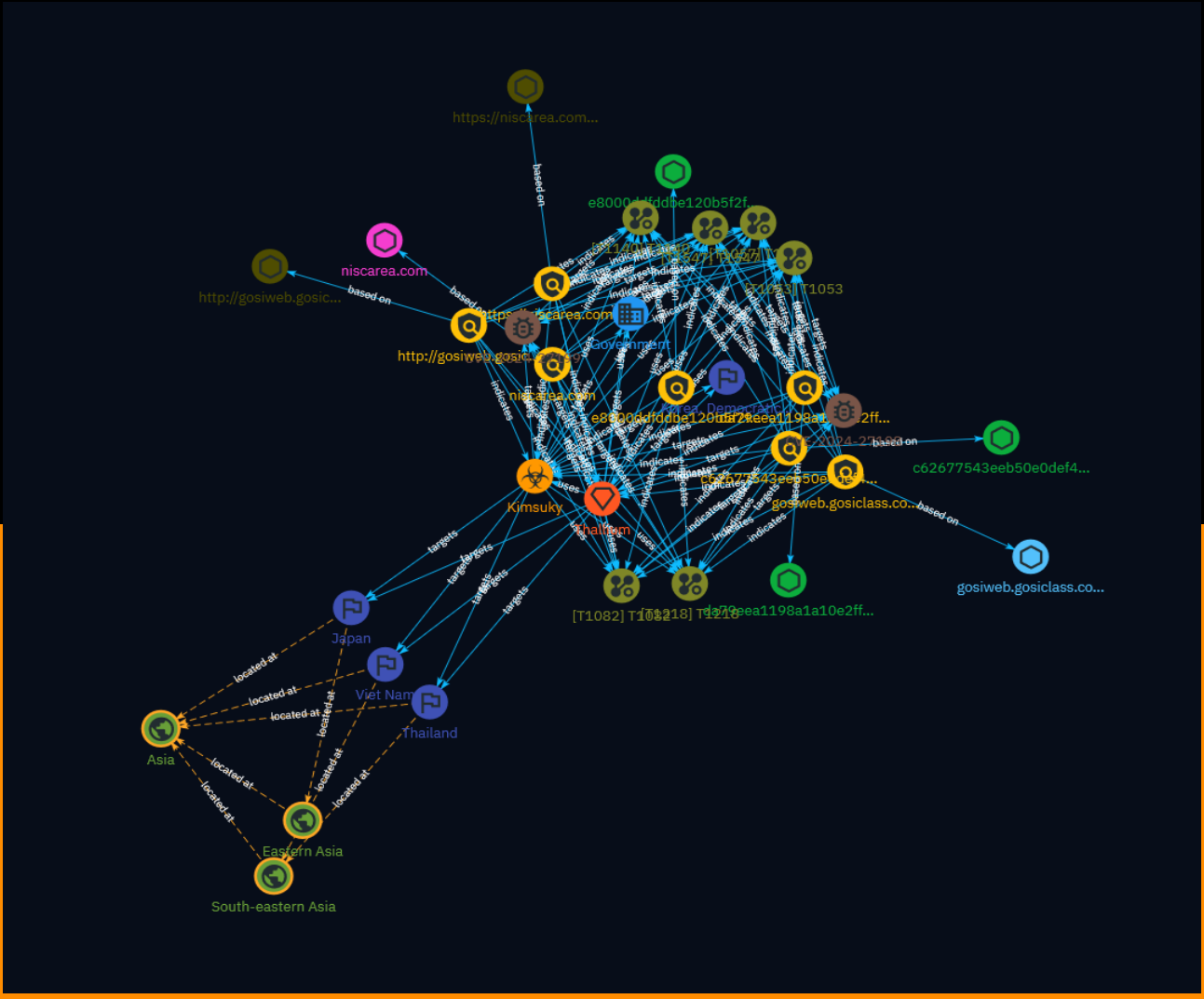

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Kimsuky threat actor group, also known as Black Banshee or Thallium, originates from North Korea and has been active since at least 2012, Kimsuky focuses primarily on intelligence gathering. Researchers believe Kimsuky is using CHM files which are delivered in several ways, as part of an ISO|VHD|ZIP or RAR file. The reason they would use this approach is that such containers have the ability to pass the first line of defense and then the CHM file will be executed.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
gosiweb.gosiclass.com
Pattern Type
stix
Pattern
[hostname:value = 'gosiweb.gosiclass.com']
Name
niscarea.com
Pattern Type
stix
Pattern
[domain-name:value = 'niscarea.com']
Name
https://niscarea.com/in.php?cn=[base64]&fn=[DateTime]

Pattern Type

stix

Pattern

[url:value = 'https://niscarea.com/in.php?cn=[base64]&fn=[DateTime]']

Name

e8000ddfddbe120b5f2fb3677abbad901615d1abd01a0de204fade5d2dd5ad0d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e8000ddfddbe120b5f2fb3677abbad901615d1abd01a0de204fade5d2dd5ad0d']

Name

http://gosiweb.gosiclass.com/m/gnu/convert/html/com/list.php?query=6

Pattern Type

stix

Pattern

[url:value = 'http://gosiweb.gosiclass.com/m/gnu/convert/html/com/list.php?query=6']

Name

da79eea1198a1a10e2ffd50fd949521632d8f252fb1aadb57a45218482b9fd89

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da79eea1198a1a10e2ffd50fd949521632d8f252fb1aadb57a45218482b9fd89']

Name

c62677543eeb50e0def44fc75009a7748cdbedd0a3ccf62f50d7f219f6a5aa05

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c62677543eeb50e0def44fc75009a7748cdbedd0a3ccf62f50d7f219f6a5aa05']

Vulnerability

Name
CVE-2024-27199
Name
CVE-2024-27198
Description
JetBrains TeamCity contains an authentication bypass vulnerability that allows an attacker to perform admin actions.

Malware

Name
Kimsuky

Country

Name
Korea, Democratic People's Republic of
Name
Viet Nam
Name
Thailand
Name
Japan

Intrusion-Set

Name

Thallium

Description

[Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky) [Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

Attack-Pattern

Name

T1057

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

Name

T1218

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Name

T1140

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/

encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

T1053

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

T1082

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

T1547

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending

features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Region

Name
South-eastern Asia
Name
Eastern Asia
Name
Asia

Sector

Name
Government
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Hostname

Value
gosiweb.gosiclass.com

Domain-Name

Value
niscarea.com

Url

Value
https://niscarea.com/in.php?cn=[base64]&fn=[DateTime]
http://gosiweb.gosiclass.com/m/gnu/convert/html/com/list.php?query=6

StixFile

Value
e8000ddfddbe120b5f2fb3677abbad901615d1abd01a0de204fade5d2dd5ad0d
c62677543eeb50e0def44fc75009a7748cdbedd0a3ccf62f50d7f219f6a5aa05
da79eea1198a1a10e2ffd50fd949521632d8f252fb1aadb57a45218482b9fd89

External References

- https://www.rapid7.com/blog/post/2024/03/20/the-updated-apt-playbook-tales-from-the-kimsuky-threat-actor-group/
- https://otx.alienvault.com/pulse/6601a1ded54ba4a842d23988