Aug 18 2023

NETMANAGEIT

Intelligence Report

DLL Hijacking in the Asian Gambling Sector

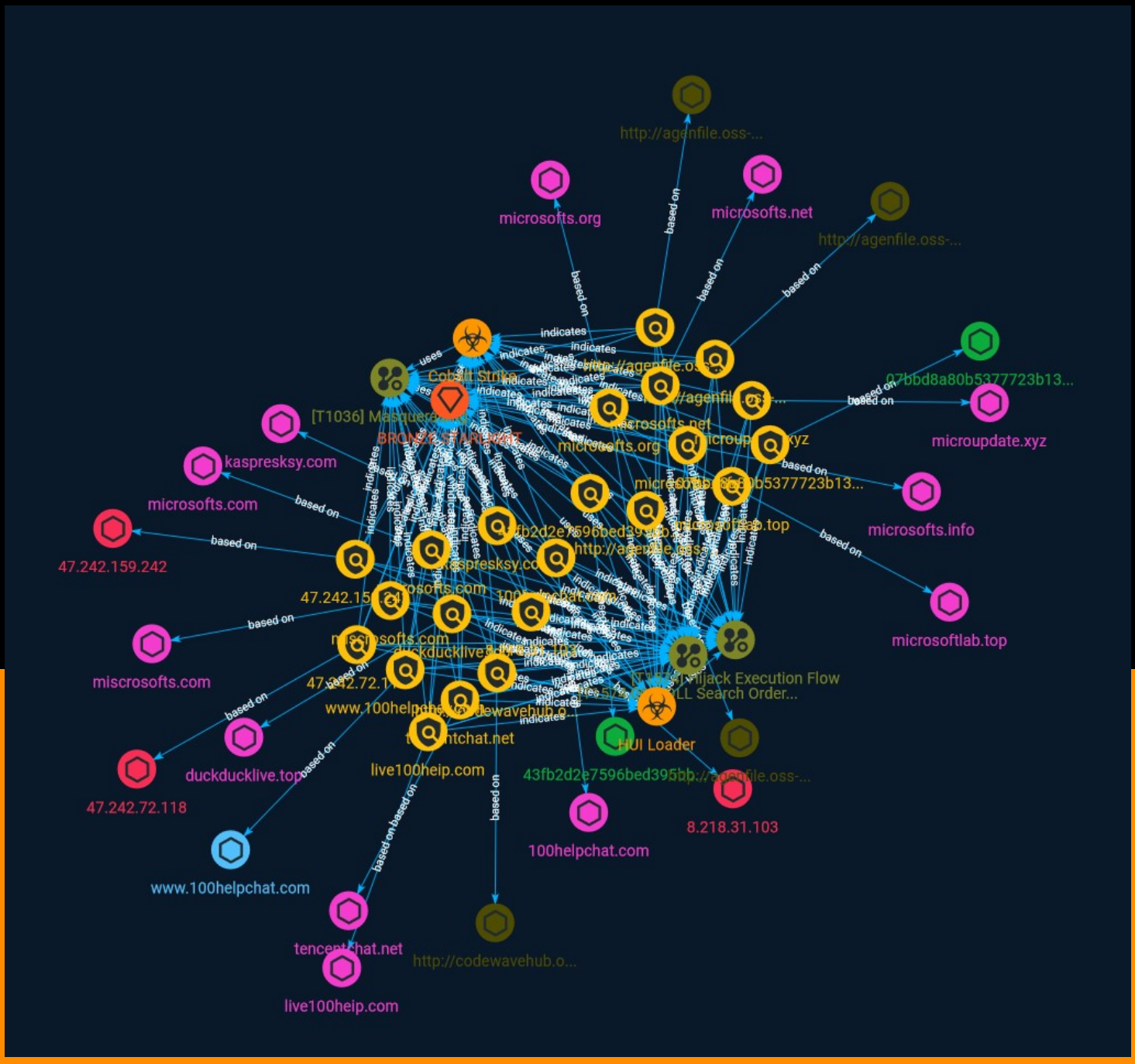

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Chinese hackers are targeting the gambling sector within Southeast Asia, according to SentinelLabs and ESET, who have identified suspected-Chinese malware and infrastructure linked to a series of attacks reported in March 2023.

Confidence

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

15 / 100

Indicator

Name
duckducklive.top
Pattern Type
stix
Pattern
[domain-name:value = 'duckducklive.top']
Name
tencentchat.net
Pattern Type
stix
Pattern
[domain-name:value = 'tencentchat.net']
Name
kaspresksy.com

Pattern Type
stix
Pattern
[domain-name:value = 'kaspresksy.com']
Name
100helpchat.com
Pattern Type
stix
Pattern
[domain-name:value = '100helpchat.com']
Name
47.242.72.118
Description
CC=HK ASN=AS45102 Alibaba US Technology Co., Ltd.
Pattern Type
stix
Pattern
[ipv4-addr:value = '47.242.72.118']

Name

43fb2d2e7596bed395bba6e012d0ee13ed61856cd63db47bf94160881d3e3ac7

Description

SHA256 of 6e9592920cdce90a7c03155ef8b113911c20bb3a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '43fb2d2e7596bed395bba6e012d0ee13ed61856cd63db47bf94160881d3e3ac7']

Name

8.218.31.103

Description

CC=HK ASN=AS45102 Alibaba US Technology Co., Ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '8.218.31.103']

Name

microsofts.com

Pattern Type

stix

Pattern

[domain-name:value = 'microsofts.com']

Name

microsoftlab.top

Pattern Type

stix

Pattern

[domain-name:value = 'microsoftlab.top']

Name

live100heip.com

Pattern Type

stix

Pattern

[domain-name:value = 'live100heip.com']

Name

microsofts.info

Pattern Type

stix

Pattern

[domain-name:value = 'microsofts.info']

Name

http://codewavehub.oss-ap-southeast-1.aliyuncs.com/org/com/file/CodeVerse.zip

Pattern Type

stix

Pattern

[url:value = 'http://codewavehub.oss-ap-southeast-1.aliyuncs.com/org/com/file/CodeVerse.zip']

Name

microsofts.org

Pattern Type

stix

Pattern

[domain-name:value = 'microsofts.org']

Name
microupdate.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'microupdate.xyz']
Name
miscrosofts.com
Pattern Type
stix
Pattern
[domain-name:value = 'miscrosofts.com']
Name
http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp3/adobe_helper.zip
Pattern Type
stix
Pattern

[url:value = 'http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp3/adobe_helper.zip']

Name

http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp1/cefhelper.zip

Pattern Type

stix

Pattern

[url:value = 'http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp1/cefhelper.zip']

Name

47.242.159.242

Description

CC=HK ASN=AS45102 Alibaba US Technology Co., Ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '47.242.159.242']

Name

http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp2/agent_bak.zip

Pattern Type

stix

Pattern

[url:value = 'http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp2/agent_bak.zip']

Name

www.100helpchat.com

Pattern Type

stix

Pattern

[hostname:value = 'www.100helpchat.com']

Name

microsofts.net

Pattern Type

stix

Pattern

[domain-name:value = 'microsofts.net']

Name

07bbd8a80b5377723b13dbb40a01ca44cbc203369f5e5652a25b448e27ca108c

Description

SHA256 of 32b545353f4e968dc140c14bc436ce2a91aacd82

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07bbd8a80b5377723b13dbb40a01ca44cbc203369f5e5652a25b448e27ca108c']

Malware

Name
HUI Loader

Name
Cobalt Strike

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Intrusion-Set

Name
BRONZE STARLIGHT

Attack-Pattern

Name

DLL Search Order Hijacking

ID

T1574.001

Description

Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load into a program. (Citation: Microsoft Dynamic Link Library Search Order)(Citation: FireEye Hijacking July 2010) Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution. There are many ways an adversary can hijack DLL loads. Adversaries may plant trojan dynamic-link library files (DLLs) in a directory that will be searched before the location of a legitimate library that will be requested by a program, causing Windows to load their malicious library when it is called for by the victim program. Adversaries may also perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program.(Citation: FireEye fxsst June 2011) Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft Security Advisory 2269637) Adversaries may also directly modify the search order via DLL redirection, which after being enabled (in the Registry and creation of a redirection file) may cause a program to load a different DLL.(Citation: Microsoft Dynamic-Link Library Redirection)(Citation: Microsoft Manifests) (Citation: FireEye DLL Search Order Hijacking) If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used

for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program. Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of

execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Domain-Name

Value
live100heip.com
kaspresksy.com
microsofts.org
tencentchat.net
microsofts.com
microupdate.xyz
100helpchat.com
miscrosofts.com
microsofts.info
duckducklive.top
microsofts.net
microsoftlab.top

StixFile

Value
43fb2d2e7596bed395bba6e012d0ee13ed61856cd63db47bf94160881d3e3ac7
07bbd8a80b5377723b13dbb40a01ca44cbc203369f5e5652a25b448e27ca108c

Hostname

Value
www.100helpchat.com

IPv4-Addr

Value
8.218.31.103
47.242.72.118
47.242.159.242

Url

Value
http://codewavehub.oss-ap-southeast-1.aliyuncs.com/org/com/file/CodeVerse.zip
http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp2/agent_bak.zip
http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp3/adobe_helper.zip
http://agenfile.oss-ap-southeast-1.aliyuncs.com/agent_source/temp1/cefhelper.zip

External References

- https://otx.alienvault.com/pulse/64de13fc81707f73da535f87
- https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/