Aug 26 2023

NETMANAGEIT

Intelligence Report

Flax Typhoon using legitimate software to quietly access Taiwanese organizations

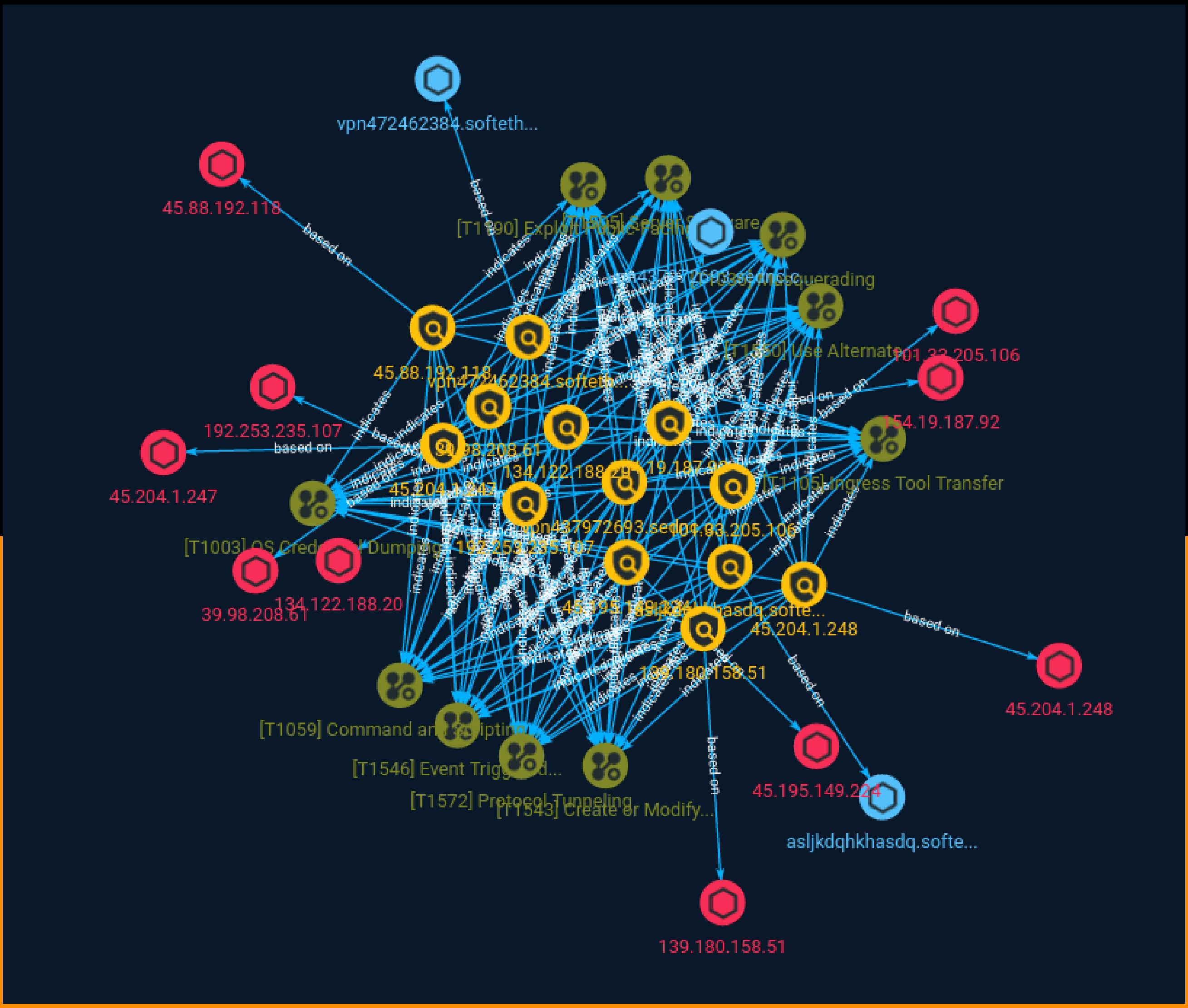

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Indicator 5
- Attack-Pattern 11
- Country 18

Observables

- Hostname 19
- IPv4-Addr 20

External References

- External References 21

Overview

Description

Microsoft has observed a distinctive pattern of malicious activity almost exclusively affecting organizations in Taiwan using techniques that could be easily reused in other operations outside the region and would benefit from broader industry visibility. Microsoft attributes this campaign to Flax Typhoon (overlaps with ETHEREAL PANDA), a nation-state actor based out of China.

Confidence

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

15 / 100

Indicator

Name
asljkdqhkhasdq.softether.net
Pattern Type
stix
Pattern
[hostname:value = 'asljkdqhkhasdq.softether.net']
Name
vpn437972693.sednc.cn
Pattern Type
stix
Pattern
[hostname:value = 'vpn437972693.sednc.cn']
Name
134.122.188.20

Description

CC=SG ASN=AS64050 BGPNET Global ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '134.122.188.20']

Name

45.204.1.248

Description

CC=HK ASN=AS136933 Gigabitbank Global

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.204.1.248']

Name

45.204.1.247

Description

CC=HK ASN=AS136933 Gigabitbank Global

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.204.1.247']

Name

154.19.187.92

Description

CC=JP ASN=AS149042 Silicon Cloud Global US

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.19.187.92']

Name

45.195.149.224

Description

CC=MU ASN=AS136933 Gigabitbank Global

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.195.149.224']

Name

39.98.208.61

Description

CC=CN ASN=AS37963 Hangzhou Alibaba Advertising Co.,Ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '39.98.208.61']

Name

101.33.205.106

Description

CC=CN ASN=AS45090 Shenzhen Tencent Computer Systems Company Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '101.33.205.106']

Name

192.253.235.107

Description

CC=US ASN=AS64050 BGPNET Global ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.253.235.107']

Name

vpn472462384.softether.net

Pattern Type

stix

Pattern

[hostname:value = 'vpn472462384.softether.net']

Name

139.180.158.51

Description

CC=SG ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.180.158.51']

Name

45.88.192.118

Description

CC=JP ASN=AS906 DMIT

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.88.192.118']

Attack-Pattern

Name

Use Alternate Authentication Material

ID

T1550

Description

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls. Authentication processes generally require a valid identity (e.g., username) along with one or more authentication factors (e.g., password, pin, physical smart card, token generator, etc.). Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process. (Citation: NIST Authentication)(Citation: NIST MFA) Caching alternate authentication material allows the system to verify an identity has successfully authenticated without asking the user to reenter authentication factor(s). Because the alternate authentication must be maintained by the system—either in memory or on disk—it may be at risk of being stolen through [Credential Access](https://attack.mitre.org/tactics/TA0006) techniques. By stealing alternate authentication material, adversaries are able to bypass system access controls and authenticate to systems without knowing the plaintext password or any additional authentication factors.

Name

Event Triggered Execution

ID
T1546
Description
Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events. (Citation: Backdooring an AWS account)(Citation: Varonis Power Automate Data Exfiltration)(Citation: Microsoft DART Case Report 001) Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked. (Citation: FireEye WMI 2015)(Citation: Malware Persistence on OS X)(Citation: amnesia malware) Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.
Name
Server Software Component
ID
T1505
Description
Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity_0day_sophos_FW)
Name

Create or Modify System Process
ID
T1543
Description
Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons) Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect. Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.(Citation: OSX Malware Detection)
Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools

mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

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

Protocol Tunneling

ID

T1572

Description

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet. There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel.(Citation: SSH Tunneling) [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19) Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Protocol Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2 communications and infrastructure.

Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Country

Name
Taiwan

Hostname

Value
vpn437972693.sednc.cn
asljkdqhkhasdq.softether.net
vpn472462384.softether.net

IPv4-Addr

Value
45.204.1.248
134.122.188.20
101.33.205.106
154.19.187.92
45.88.192.118
192.253.235.107
39.98.208.61
139.180.158.51
45.195.149.224
45.204.1.247

External References

- https://otx.alienvault.com/pulse/64e86c65ba511d1d4c4aa590
- https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/