Oct 03 2023

NETMANAGEIT

Intelligence Report

Attacks on Southeast Asian Government Have Links to Alloy Taurus

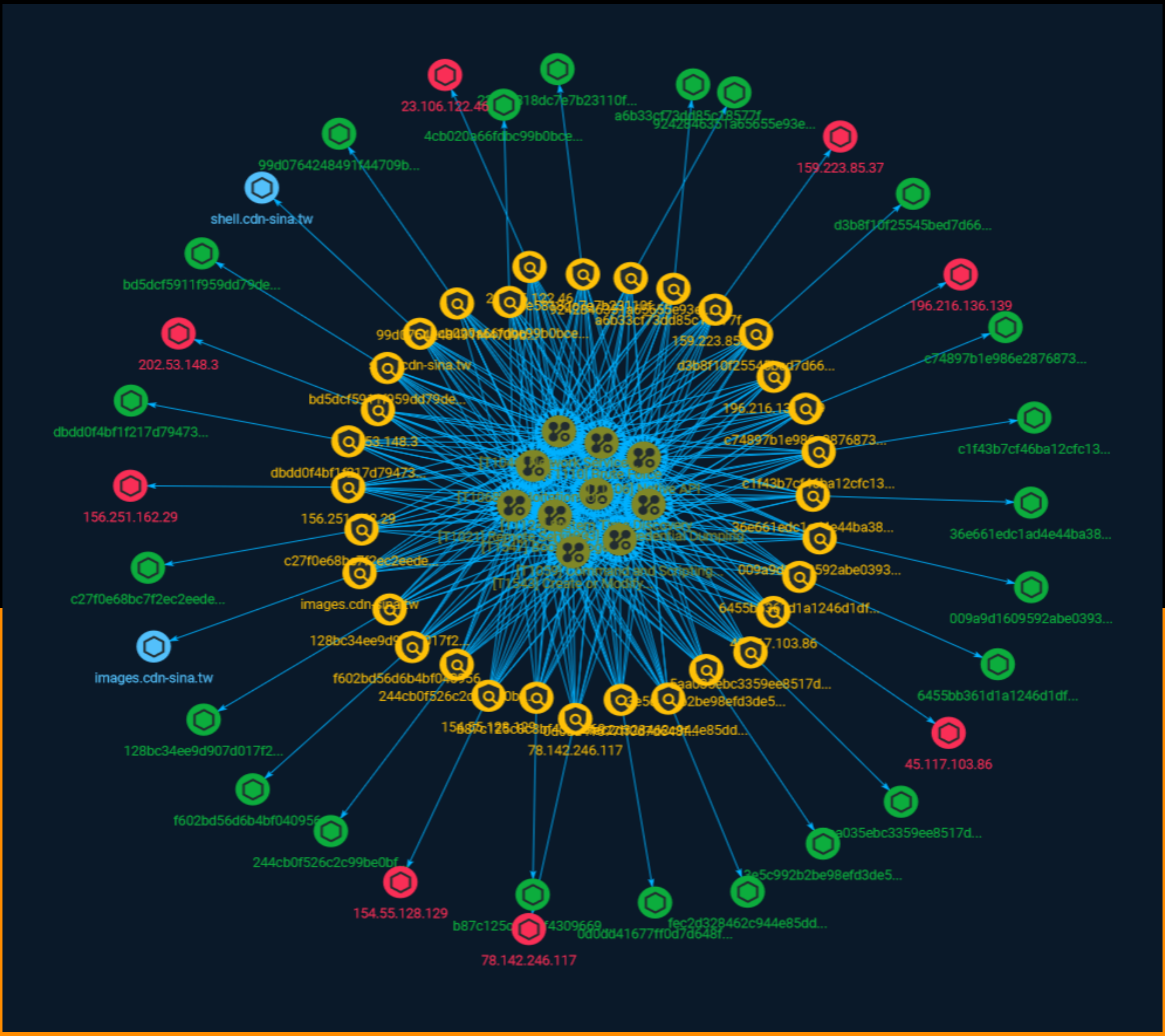

Table of contents

Overview

Entities

Observables

External References

Overview

Description

We observed a series of intrusions directed at a Southeast Asian government target, a cluster of activity that we attribute with a moderate level of confidence to Alloy Taurus, a group believed to be operating on behalf of Chinese state interests. The multiwave intrusions, which started in early 2022 and persisted throughout 2023, capitalized on vulnerabilities in Exchange Servers to deploy a large number of web shells.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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

Boot or Logon Autostart Execution

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.

Name

Brute Force

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

System Time Discovery

ID

T1124

Description

An adversary may gather the system time and/or time zone from a local or remote system. The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network. (Citation: MSDN System Time)(Citation: Technet Windows Time Service) System time information may be gathered in a number of ways, such as with [Net](https://attack.mitre.org/software/S0039) on Windows by performing `net time \\hostname` to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using `w32tm /tz`.(Citation: Technet Windows Time Service) On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show clock detail` can be used to see the current time configuration.(Citation: show_clock_detail_cisco_cmd) This information could be useful for performing other techniques, such as executing a file with a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053)(Citation: RSA EU12 They're Inside), or to discover locality information based on time zone to assist in victim targeting (i.e. [System Location Discovery](https://attack.mitre.org/techniques/T1614)). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.(Citation: AnyRun TimeBomb)

Name

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. 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. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

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

Network Service Discovery

ID

T1046

Description

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021) Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well. Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host's registered services on the network. For example, adversaries can use a mDNS query (such as `dns-sd -B _ssh._tcp .`) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

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)

Name

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Indicator

Name

0d0dd41677ff0d7d648f8563db3a4b4844d86d70562d844bad1983333ae5633d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0d0dd41677ff0d7d648f8563db3a4b4844d86d70562d844bad1983333ae5633d']

Name

shell.cdn-sina.tw

Pattern Type

stix

Pattern

[hostname:value = 'shell.cdn-sina.tw']

Name

36e661edc1ad4e44ba38d8f7a6bd00c2b4bc32e9fae8b955b1b4c6355aa6abed

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '36e661edc1ad4e44ba38d8f7a6bd00c2b4bc32e9fae8b955b1b4c6355aa6abed']

Name

128bc34ee9d907d017f2e6f8fbbba24c3e51ed5a2fdba417ba893b496c8c18a7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '128bc34ee9d907d017f2e6f8fbbba24c3e51ed5a2fdba417ba893b496c8c18a7']

Name

225e5818dc7e7b23110f64fbb718c1792ad93ba7eb893bfbee96cdb13180fbf7

Description

ConventionEngine_Term_Users

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '225e5818dc7e7b23110f64fbb718c1792ad93ba7eb893bfbee96cdb13180fbf7']

Name

3e5c992b2be98efd3de5b13969900f207665116063a889b1c763371d4104f7f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e5c992b2be98efd3de5b13969900f207665116063a889b1c763371d4104f7f9']

Name

156.251.162.29

Description

CC=HK ASN=AS40065 CNSERVERS

Pattern Type

stix

Pattern

[ipv4-addr:value = '156.251.162.29']

Name

196.216.136.139

Description

ISP: Metrofibre Networx **OS:** Windows ------------------------- Hostnames: - autodiscover.saspecialforces.co.za - mail.saspecialforces.co.za - saspecialforces.co.za ------------------------- Domains: - saspecialforces.co.za ------------------------- Services: **25:** ``` 220 SFHQ.sfhq.saspecialforces.com Microsoft ESMTP MAIL Service ready at Thu, 14 Sep 2023 20:59:48 +0200 250-SFHQ.sfhq.saspecialforces.com Hello [224.107.7.218] 250-SIZE 37748736 250-PIPELINING 250-DSN 250-ENHANCEDSTATUSCODES 250-STARTTLS 250-X-ANONYMOUSTLS 250-AUTH NTLM 250-X-EXPS GSSAPI NTLM 250-8BITMIME 250-BINARYMIME 250-CHUNKING 250-SMTPUTF8 250 XRDST SMTP NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: SFHQ0 NetBIOS Domain Name: SFHQ0 NetBIOS Computer Name: SFHQ DNS Domain Name: sfhq.saspecialforces.com DNS Tree Name: sfhq.saspecialforces.com FQDN: SFHQ.sfhq.saspecialforces.com ``` ------------------ **80:** ``` HTTP/1.1 403 Forbidden Server: Microsoft-IIS/10.0 Date: Sat, 30 Sep 2023 07:06:06 GMT Content-Length: 0 ``` ------------------ **443:** ``` HTTP/1.1 200 OK Cache-Control: no-cache, no-store Pragma: no-cache Content-Type: text/html; charset=utf-8 Expires: -1 Server: Microsoft-IIS/10.0 request-id: fb84492f-73ee-432f-968e-0a994e0b310b X-Frame-Options: SAMEORIGIN X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Date: Sat, 23 Sep 2023 15:11:58 GMT Content-Length: 58715 Microsoft Exchange: Name: Exchange Server 2019 RTM Mar21SU Build Number: 15.2.221.18 Build Date: March 2, 2021 ``` HEARTBLEED: 2023/09/23 15:12:35 196.216.136.139:443 - ERROR: write tcp 196.216.136.139:443: broken pipe ------------------ **587:** ``` 220 SFHQ.sfhq.saspecialforces.com Microsoft ESMTP MAIL Service ready at Wed, 27 Sep 2023 12:21:03 +0200 250-SFHQ.sfhq.saspecialforces.com Hello [224.57.205.251] 250-SIZE 37748736 250-PIPELINING 250-DSN 250-ENHANCEDSTATUSCODES 250-STARTTLS 250-AUTH GSSAPI NTLM 250-8BITMIME 250-BINARYMIME 250-CHUNKING 250 SMTPUTF8 SMTP NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: SFHQ0 NetBIOS Domain Name: SFHQ0 NetBIOS Computer Name: SFHQ DNS Domain Name: sfhq.saspecialforces.com DNS Tree Name: sfhq.saspecialforces.com FQDN: SFHQ.sfhq.saspecialforces.com ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '196.216.136.139']

Name

b87c125c8c3bf43096690bf74df960e2c0120654635c4ea715039fbe9115ecef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b87c125c8c3bf43096690bf74df960e2c0120654635c4ea715039fbe9115ecef']

Name

99d0764248491f44709bd000104f6f99e53c9de8d55649b45112320d7bc4deed

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99d0764248491f44709bd000104f6f99e53c9de8d55649b45112320d7bc4deed']

Name

009a9d1609592abe039324da2a8a69c4a305ca999920bf6bbef839273516783a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '009a9d1609592abe039324da2a8a69c4a305ca999920bf6bbef839273516783a']

Name

images.cdn-sina.tw

Pattern Type

stix

Pattern

[hostname:value = 'images.cdn-sina.tw']

Name

a6b33cf73dd85c18577f58a75802ea0820f11aba88fac23ee3794fac1f4bacfa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a6b33cf73dd85c18577f58a75802ea0820f11aba88fac23ee3794fac1f4bacfa']

Name

fec2d328462c944e85dd112e61c97d3e67a39f3c83c59e07410d228c7222d153

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fec2d328462c944e85dd112e61c97d3e67a39f3c83c59e07410d228c7222d153']

Name

202.53.148.3

Description

CC=HK ASN=AS55639 Asia Web Service Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '202.53.148.3']

Name

c74897b1e986e2876873abb3b5069bf1b103667f7f0e6b4581fbda3fd647a74a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c74897b1e986e2876873abb3b5069bf1b103667f7f0e6b4581fbda3fd647a74a']

Name

244cb0f526c2c99be0bf822463cd338630afa12ab32cc9b6cfd6e85fa315a478

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '244cb0f526c2c99be0bf822463cd338630afa12ab32cc9b6cfd6e85fa315a478']

Name

23.106.122.46

Description

CC=SG ASN=AS59253 Leaseweb Asia Pacific pte. ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.106.122.46']

Name

45.117.103.86

Description

CC=JP ASN=AS4785 xTom

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.117.103.86']

Name

c27f0e68bc7f2ec2eede8a8e08fa341d41d5d2d0fb2b74260679a5504115947e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c27f0e68bc7f2ec2eede8a8e08fa341d41d5d2d0fb2b74260679a5504115947e']

Name

159.223.85.37

Description

CC=SG ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.223.85.37']

Name

78.142.246.117

Description

CC=TH ASN=AS23884 Proen Corp Public Company Limited.

Pattern Type

stix

Pattern

[ipv4-addr:value = '78.142.246.117']

Name

bd5dcf5911f959dd79de046d151e8a4aed3b854a322135acc37e3edb3643d0e2

Description

!Petite_v14

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd5dcf5911f959dd79de046d151e8a4aed3b854a322135acc37e3edb3643d0e2']

Name

c1f43b7cf46ba12cfc1357b17e4f5af408740af7ae70572c9cf988ac50260ce1

Description

HackTool:JS/ReGeorg

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c1f43b7cf46ba12cfc1357b17e4f5af408740af7ae70572c9cf988ac50260ce1']

Name

f602bd56d6b4bf040956b86ed030643523a8b6611a21b5aafeaa82478820c395

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f602bd56d6b4bf040956b86ed030643523a8b6611a21b5aafeaa82478820c395']

Name

9242846351a65655e93ed2aeaf36b535ff5b79ddf76c33d54089d9005a66265b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9242846351a65655e93ed2aeaf36b535ff5b79ddf76c33d54089d9005a66265b']

Name

5aa035ebc3359ee8517d99569c8881fcb7f48ab7e9a2f101f7e7ec23e636c79b

Description

KnownMaliciousObfuscationPattern

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5aa035ebc3359ee8517d99569c8881fcb7f48ab7e9a2f101f7e7ec23e636c79b']

Name

dbdd0f4bf1f217d794738b7d4f83483a5b3579be8791a7e2f2a62ec3e839be3c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'dbdd0f4bf1f217d794738b7d4f83483a5b3579be8791a7e2f2a62ec3e839be3c']

Name

d3b8f10f25545bed7d661b6a80be53356c00947800c7e53f050cb15b1f9b953b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd3b8f10f25545bed7d661b6a80be53356c00947800c7e53f050cb15b1f9b953b']

Name

154.55.128.129

Description

CC=US ASN=AS139646 HONG KONG Megalayer Technology Co.,Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.55.128.129']

Name

4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66']

Name

6455bb361d1a1246d1df39b0785fc0f370eb54dd7d5b64d70457e4f9881f6c3c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6455bb361d1a1246d1df39b0785fc0f370eb54dd7d5b64d70457e4f9881f6c3c']

StixFile

Value
d3b8f10f25545bed7d661b6a80be53356c00947800c7e53f050cb15b1f9b953b
f602bd56d6b4bf040956b86ed030643523a8b6611a21b5aafeaa82478820c395
0d0dd41677ff0d7d648f8563db3a4b4844d86d70562d844bad1983333ae5633d
5aa035ebc3359ee8517d99569c8881fcb7f48ab7e9a2f101f7e7ec23e636c79b
fec2d328462c944e85dd112e61c97d3e67a39f3c83c59e07410d228c7222d153
c74897b1e986e2876873abb3b5069bf1b103667f7f0e6b4581fbda3fd647a74a
9242846351a65655e93ed2aeaf36b535ff5b79ddf76c33d54089d9005a66265b
36e661edc1ad4e44ba38d8f7a6bd00c2b4bc32e9fae8b955b1b4c6355aa6abed
c1f43b7cf46ba12cfc1357b17e4f5af408740af7ae70572c9cf988ac50260ce1
6455bb361d1a1246d1df39b0785fc0f370eb54dd7d5b64d70457e4f9881f6c3c
3e5c992b2be98efd3de5b13969900f207665116063a889b1c763371d4104f7f9
b87c125c8c3bf43096690bf74df960e2c0120654635c4ea715039fbe9115ecef
99d0764248491f44709bd000104f6f99e53c9de8d55649b45112320d7bc4deed

a6b33cf73dd85c18577f58a75802ea0820f11aba88fac23ee3794fac1f4bacfa
c27f0e68bc7f2ec2eede8a8e08fa341d41d5d2d0fb2b74260679a5504115947e
bd5dcf5911f959dd79de046d151e8a4aed3b854a322135acc37e3edb3643d0e2
dbdd0f4bf1f217d794738b7d4f83483a5b3579be8791a7e2f2a62ec3e839be3c
225e5818dc7e7b23110f64fbb718c1792ad93ba7eb893bfbee96cdb13180fbf7
244cb0f526c2c99be0bf822463cd338630afa12ab32cc9b6cfd6e85fa315a478
009a9d1609592abe039324da2a8a69c4a305ca999920bf6bbef839273516783a
128bc34ee9d907d017f2e6f8fbbba24c3e51ed5a2fdba417ba893b496c8c18a7
4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66

Hostname

Value
images.cdn-sina.tw
shell.cdn-sina.tw

IPv4-Addr

Value
196.216.136.139
159.223.85.37
202.53.148.3
45.117.103.86
78.142.246.117
156.251.162.29
23.106.122.46
154.55.128.129

External References

- https://otx.alienvault.com/pulse/651aca1636127242b4dd6af9
- https://unit42.paloaltonetworks.com/alloy-taurus-targets-se-asian-government/