Jun 19 2023

NETMANAGEIT

Intelligence Report

ChamelGang and ChamelDoH: A DNS-over-HTTPS implant

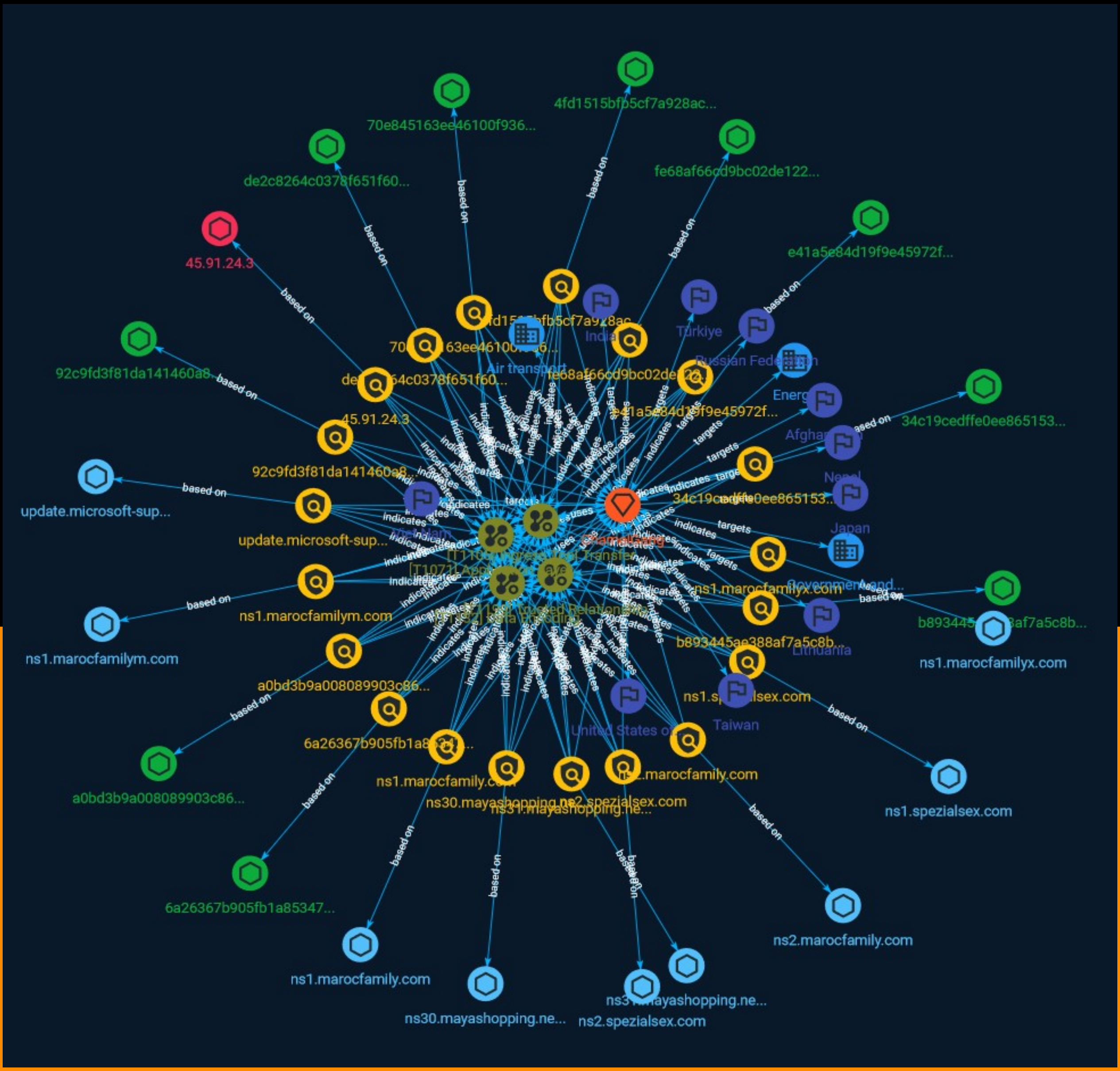

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A report on the capabilities and detection of tools used by ChamelGang, a sophisticated threat actor with a nexus to China, has been published by the Stairwell Threat Research team in the United States.

Confidence

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

15 / 100

Attack-Pattern

Name

Data Encoding

ID

T1132

Description

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

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

Trusted Relationship

ID

T1199

Description

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network. Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](https://attack.mitre.org/techniques/T1078) used by the other party for access to internal network systems may be compromised and used.(Citation: CISA IT Service Providers) In Office 365 environments, organizations may grant Microsoft partners or resellers delegated administrator permissions. By compromising a partner or reseller account, an adversary may be able to leverage existing delegated administrator relationships or send new delegated administrator offers to clients in order to gain administrative control over the victim tenant.(Citation: Office 365 Delegated Administration)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/ network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Sector

Name

Energy

Description

Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.

Name

Government and administrations

Description

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

Name

Air transport

Description

All entities transporting people or goods by plane, managing or exploiting airports and structures, traffic authorities and plane manufacturers. Includes all civilian space activities.

Indicator

Name

70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007']

Name

ns1.spezialsex.com

Pattern Type

stix

Pattern

[hostname:value = 'ns1.spezialsex.com']

Name

ns1.marocfamilym.com

Pattern Type

stix

Pattern

[hostname:value = 'ns1.marocfamilym.com']

Name

e41a5e84d19f9e45972f497270133167669052ad6f11e7a16e832cf1de59da7d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e41a5e84d19f9e45972f497270133167669052ad6f11e7a16e832cf1de59da7d']

Name

ns1.marocfamily.com

Pattern Type

stix

Pattern

[hostname:value = 'ns1.marocfamily.com']

Name
92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b']
Name
b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a']
Name
6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe']

Name

4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0']

Name

ns2.spezialsex.com

Pattern Type

stix

Pattern

[hostname:value = 'ns2.spezialsex.com']

Name

update.microsoft-support.net

Pattern Type

stix

Pattern

[hostname:value = 'update.microsoft-support.net']

Name

34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7']

Name

ns30.mayashopping.net

Pattern Type

stix

Pattern

[hostname:value = 'ns30.mayashopping.net']

Name

de2c8264c0378f651f607ef5d0b93aca5760d370d5fed562e784ce5404bbc1a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de2c8264c0378f651f607ef5d0b93aca5760d370d5fed562e784ce5404bbc1a9']

Name

ns2.marocfamily.com

Pattern Type

stix

Pattern

[hostname:value = 'ns2.marocfamily.com']

Name

a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c']

Name

fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72']

Name

ns31.mayashopping.net

Pattern Type

stix

Pattern

[hostname:value = 'ns31.mayashopping.net']

Name

45.91.24.3

Description

CC=AT ASN=AS57878 Prager Connect GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.91.24.3']

Name

ns1.marocfamilyx.com

Pattern Type

stix

Pattern

[hostname:value = 'ns1.marocfamilyx.com']

Intrusion-Set

Name
ChamelGang

Country

Name
Taiwan
Name
India
Name
Japan
Name
Viet Nam
Name
Afghanistan
Name
Lithuania
Name
Türkiye

Name
Nepal

Name
United States of America

Name
Russian Federation

StixFile

Value
6a26367b905fb1a8534732746fa968e3282d065e13267d459770fe0ec9f101fe
a0bd3b9a008089903c8653d0fcbc16e502da08eb2e77211473d0dfdec2cce67c
fe68af66cd9bc02de1221765d793637d27856fcaa632fabb81e805d2a2862b72
4fd1515bfb5cf7a928acfacabe9d6b5272c036def898d1de3de7659f174475e0
e41a5e84d19f9e45972f497270133167669052ad6f11e7a16e832cf1de59da7d
b893445ae388af7a5c8b398edf98cfb7acd191fb7c2e12c7d3b2d82ee8611b1a
92c9fd3f81da141460a8e9c65b544425f2553fa828636daeab8f3f4f23191c5b
70e845163ee46100f93633e135a7ca4361a0d7bc21030bc200d45bb14756f007
de2c8264c0378f651f607ef5d0b93aca5760d370d5fed562e784ce5404bbc1a9
34c19cedffe0ee86515331f93b130ede89f1773c3d3a2d0e9c7f7db8f6d9a0a7

Hostname

Value
ns1.marocfamilyx.com
ns1.spezialsex.com
ns31.mayashopping.net
ns1.marocfamily.com
ns2.marocfamily.com
update.microsoft-support.net
ns2.spezialsex.com
ns30.mayashopping.net
ns1.marocfamilym.com

IPv4-Addr

Value
45.91.24.3

External References

- https://otx.alienvault.com/pulse/64907e470e46bba8d3b68d52
- https://stairwell.com/news/chamelgang-and-chameldoh-a-dns-over-https-implant/