Jun 21 2023

NETMANAGEIT

Intelligence Report

Graphican: Flea Uses New Backdoor in Attacks Targeting Foreign Ministries

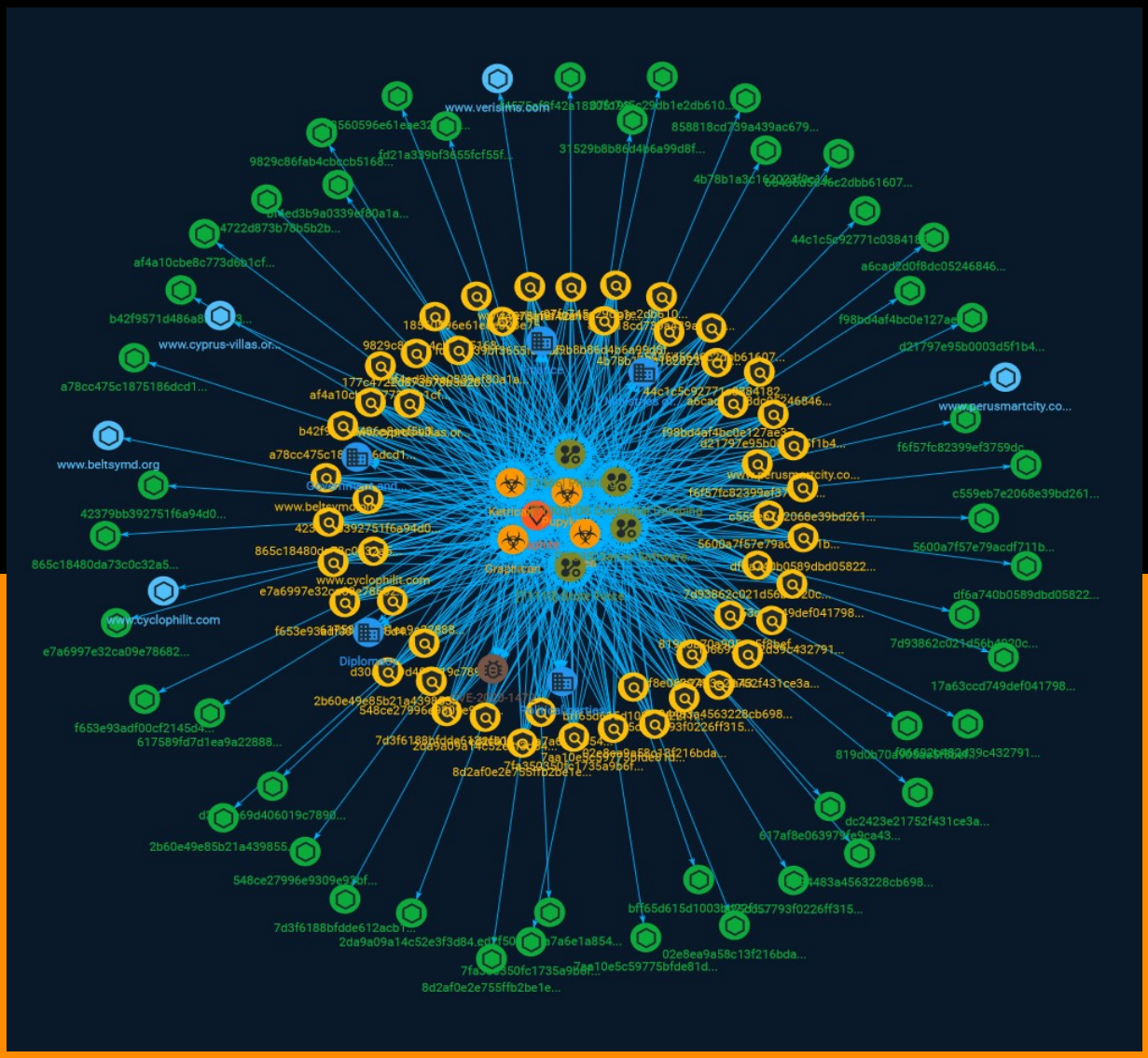

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Attack-Pattern 5
- Sector 8
- Indicator 10
- Intrusion-Set 31
- Malware 32

Observables

- StixFile 33
- Hostname 36

External References

- External References 37

Overview

Description

A new backdoor used by the Flea malware group in a recent attack campaign targeted foreign ministries in the Americas.

Confidence

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

15 / 100

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
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

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto

their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

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)

Sector

Name
Diplomacy
Description
Public or private entities which are actors of or involved in international relations activities.
Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Political parties
Description
A recognized or non recognized political group or party taking part into the political life of a country, weither by being part of the majority or opposed to the ruling power

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
Ministries of foreign affairs
Description
Governmental entities in charge of the diplomatic action of the State.

Indicator

Name
7d93862c021d56b4920cab5e6cb30a2d5fb21478e7158f104e520cc739a1678d
Description
SLF:Python/PypyKatz.A
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7d93862c021d56b4920cab5e6cb30a2d5fb21478e7158f104e520cc739a1678d']
Name
617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd']

Name

4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5']

Name

e25cc57793f0226ff31568be1fce1e279d35746016fc086a6f67734d26e305a0

Description

HackToolWin32Lsascan

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e25cc57793f0226ff31568be1fce1e279d35746016fc086a6f67734d26e305a0']

Name

af4a10cbe8c773d6b1cfb34be2455eb023fb1b0d6f0225396920808fefb11523

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af4a10cbe8c773d6b1cfb34be2455eb023fb1b0d6f0225396920808fefb11523']

Name

f6f57fc82399ef3759dcbc16b7a25343dea0b539332dacdf0ed289cc82e900db

Description

HackTool:Win64/Mikatz!dha

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6f57fc82399ef3759dcbc16b7a25343dea0b539332dacdf0ed289cc82e900db']

Name

ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56

Description

HackTool:Win32/LaZagne

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56']
Name
fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476']
Name
17a63ccd749def0417981c42b0765f7d56e6be3092a1f282b81619ca819f82ef
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '17a63ccd749def0417981c42b0765f7d56e6be3092a1f282b81619ca819f82ef']

Name
www.cyclophilit.com
Pattern Type
stix
Pattern
[hostname:value = 'www.cyclophilit.com']
Name
858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253']
Name
7aa10e5c59775bfde81d27e63dfca26a1ec38065ddc87fe971c30d2b2b72d978
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '7aa10e5c59775bfde81d27e63dfca26a1ec38065ddc87fe971c30d2b2b72d978']

Name

www.cyprus-villas.org

Pattern Type

stix

Pattern

[hostname:value = 'www.cyprus-villas.org']

Name

5600a7f57e79acdf711b106ee1c360fc898ed914e6d1af3c267067c158a41db6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5600a7f57e79acdf711b106ee1c360fc898ed914e6d1af3c267067c158a41db6']

Name

d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30']

Name

f4575af8f42a1830519895a294c98009ffbb44b20baa170a6b5e4a71fd9ba663

Description

JSP:WebShell-B\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f4575af8f42a1830519895a294c98009ffbb44b20baa170a6b5e4a71fd9ba663']

Name

617af8e063979fe9ca43479f199cb17c7abeab7bfe904a2baf65708df8461f6d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '617af8e063979fe9ca43479f199cb17c7abeab7bfe904a2baf65708df8461f6d']

Name

42379bb392751f6a94d08168835b67986c820490a6867c28a324a807c49eda3b

Description

Win.Trojan.Mimikatz-6463690-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '42379bb392751f6a94d08168835b67986c820490a6867c28a324a807c49eda3b']

Name

a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86

Description

Virtool.PWDump

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86']

Name

8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b']

Name

9829c86fab4cbccb5168f98dcb076672dc6d069ddb693496b463ad704f31722e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9829c86fab4cbccb5168f98dcb076672dc6d069ddb693496b463ad704f31722e']

Name

df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f

Description

HackTool:Win32/Mimikatz.E

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f']

Name

f653e93adf00cf2145d4bfa00153ae86905fe2c2d3c1f63e8f579e43b7069d51

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f653e93adf00cf2145d4bfa00153ae86905fe2c2d3c1f63e8f579e43b7069d51']

Name

31529b8b86d4b6a99d8f3b5f4b1f1b67f3c713c11b83b71d8df7d963275c5203

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '31529b8b86d4b6a99d8f3b5f4b1f1b67f3c713c11b83b71d8df7d963275c5203']

Name

bff65d615d1003bd22f17493efd65eb9ffbfe9a63668deebe09879982e5c6aa8

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'bff65d615d1003bd22f17493efd65eb9ffbfe9a63668deebe09879982e5c6aa8']
Name
b42f9571d486a8aef5b36d72c1c8fff83f29cac2f9c61aece3ad70537d49b222
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b42f9571d486a8aef5b36d72c1c8fff83f29cac2f9c61aece3ad70537d49b222']
Name
f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286']

Name

7d3f6188bfdde612acb17487da1b0b1aaaeb422adc9e13fd7eb61044bac7ae08

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7d3f6188bfdde612acb17487da1b0b1aaaeb422adc9e13fd7eb61044bac7ae08']

Name

18560596e61eae328e75f4696a3d620b95db929bc461e0b29955df06bc114051

Description

HackTool:Win64/Mikatz!dha

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '18560596e61eae328e75f4696a3d620b95db929bc461e0b29955df06bc114051']

Name

819d0b70a905ae5f8bef6c47423964359c2a90a168414f5350328f568e1c7301

Description

InstallShield2000

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '819d0b70a905ae5f8bef6c47423964359c2a90a168414f5350328f568e1c7301']

Name

865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48']

Name

44c1c5c92771c0384182f72e9866d5fed4fda896d90c931fe8de363ed81106cf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44c1c5c92771c0384182f72e9866d5fed4fda896d90c931fe8de363ed81106cf']

Name

7fa350350fc1735a9b6f162923df8d960daffb73d6f5470df3c3317ae237a4e6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7fa350350fc1735a9b6f162923df8d960daffb73d6f5470df3c3317ae237a4e6']

Name

bf4ed3b9a0339ef80a1af557d0f4e031fb4106a04b0f72c85f7f0ff0176ebb64

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf4ed3b9a0339ef80a1af557d0f4e031fb4106a04b0f72c85f7f0ff0176ebb64']

Name

c559eb7e2068e39bd26167dd4dca3eea48e51ad0b2c7631f2ed6ffcba01fb819

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c559eb7e2068e39bd26167dd4dca3eea48e51ad0b2c7631f2ed6ffcba01fb819']

Name

548ce27996e9309e93bf0bd29c7871977530761b2c20fc7dc3e2c16c025eb7bc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '548ce27996e9309e93bf0bd29c7871977530761b2c20fc7dc3e2c16c025eb7bc']

Name

07fc745c29db1e2db61089d8d46299078794d7127120d04c07e0a1ea6933a6df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07fc745c29db1e2db61089d8d46299078794d7127120d04c07e0a1ea6933a6df']

Name

9a94483a4563228cb698173c1991c7cf90726c2c126a3ce74c66ba226040f760

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a94483a4563228cb698173c1991c7cf90726c2c126a3ce74c66ba226040f760']

Name

www.beltsymd.org

Pattern Type

stix

Pattern

[hostname:value = 'www.beltsymd.org']

Name

d21797e95b0003d5f1b41a155cced54a45cd22eec3f997e867c11f6173ee7337

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd21797e95b0003d5f1b41a155cced54a45cd22eec3f997e867c11f6173ee7337']

Name

2da9a09a14c52e3f3d8468af24607602cca13bc579af958be9e918d736418660

Description

Backdoor:JS/Makdichi.A!MTB

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2da9a09a14c52e3f3d8468af24607602cca13bc579af958be9e918d736418660']

Name

177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf']

Name

f06692b482d39c432791acabb236f7d21895df6f76e0b83992552ab5f1b43c8d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f06692b482d39c432791acabb236f7d21895df6f76e0b83992552ab5f1b43c8d']

Name

e7a6997e32ca09e78682fc9152455edaa1f9ea674ec51aecd7707b1bbda37c2f

Description

!PEExpkUnpackedFile

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7a6997e32ca09e78682fc9152455edaa1f9ea674ec51aecd7707b1bbda37c2f']

Name

65436d5646c2dbb61607ed466132302f8c87dab82251f9e3f20443d5370b7806

Description

Win.Trojan.ChopperJsp-1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '65436d5646c2dbb61607ed466132302f8c87dab82251f9e3f20443d5370b7806']

Name

02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5']

Name

a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8

Description

Win32:Evo-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8']

Name
www.perusmartcity.com
Pattern Type
stix
Pattern
[hostname:value = 'www.perusmartcity.com']
Name
2b60e49e85b21a439855b5cb43cf799c1fb3cc0860076d52e41d48d88487e6d8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2b60e49e85b21a439855b5cb43cf799c1fb3cc0860076d52e41d48d88487e6d8']
Name
www.verisims.com
Pattern Type
stix
Pattern

[hostname:value = 'www.verisims.com']

Name

dc2423e21752f431ce3ad010ce41f56914e414f5a88fd3169e78d4cc08082f7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dc2423e21752f431ce3ad010ce41f56914e414f5a88fd3169e78d4cc08082f7b']

Intrusion-Set

Name
Graphite

Malware

Name
Graphican
Name
Pupykatz
Name
Flea
Name
Ketrican

StixFile

Value
865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48
4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5
07fc745c29db1e2db61089d8d46299078794d7127120d04c07e0a1ea6933a6df
b42f9571d486a8aef5b36d72c1c8fff83f29cac2f9c61aece3ad70537d49b222
17a63ccd749def0417981c42b0765f7d56e6be3092a1f282b81619ca819f82ef
02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5
819d0b70a905ae5f8bef6c47423964359c2a90a168414f5350328f568e1c7301
a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86
e25cc57793f0226ff31568be1fce1e279d35746016fc086a6f67734d26e305a0
df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f
44c1c5c92771c0384182f72e9866d5fed4fda896d90c931fe8de363ed81106cf
2da9a09a14c52e3f3d8468af24607602cca13bc579af958be9e918d736418660
7d3f6188bfdde612acb17487da1b0b1aaaeb422adc9e13fd7eb61044bac7ae08

31529b8b86d4b6a99d8f3b5f4b1f1b67f3c713c11b83b71d8df7d963275c5203

f653e93adf00cf2145d4bfa00153ae86905fe2c2d3c1f63e8f579e43b7069d51

bff65d615d1003bd22f17493efd65eb9ffbfe9a63668deebe09879982e5c6aa8

42379bb392751f6a94d08168835b67986c820490a6867c28a324a807c49eda3b

e7a6997e32ca09e78682fc9152455edaa1f9ea674ec51aecd7707b1bbda37c2f

617af8e063979fe9ca43479f199cb17c7abeab7bfe904a2baf65708df8461f6d

617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd

a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8

d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30

ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56

5600a7f57e79acdf711b106ee1c360fc898ed914e6d1af3c267067c158a41db6

c559eb7e2068e39bd26167dd4dca3eea48e51ad0b2c7631f2ed6ffcba01fb819

bf4ed3b9a0339ef80a1af557d0f4e031fb4106a04b0f72c85f7f0ff0176ebb64

f6f57fc82399ef3759dcbc16b7a25343dea0b539332dacdf0ed289cc82e900db

9829c86fab4cbccb5168f98dcb076672dc6d069ddb693496b463ad704f31722e

65436d5646c2dbb61607ed466132302f8c87dab82251f9e3f20443d5370b7806

f06692b482d39c432791acabb236f7d21895df6f76e0b83992552ab5f1b43c8d

f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286

d21797e95b0003d5f1b41a155cced54a45cd22eec3f997e867c11f6173ee7337

7fa350350fc1735a9b6f162923df8d960daffb73d6f5470df3c3317ae237a4e6

7d93862c021d56b4920cab5e6cb30a2d5fb21478e7158f104e520cc739a1678d

18560596e61eae328e75f4696a3d620b95db929bc461e0b29955df06bc114051

9a94483a4563228cb698173c1991c7cf90726c2c126a3ce74c66ba226040f760

dc2423e21752f431ce3ad010ce41f56914e414f5a88fd3169e78d4cc08082f7b

7aa10e5c59775bfde81d27e63dfca26a1ec38065ddc87fe971c30d2b2b72d978

8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b

177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf

858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253

f4575af8f42a1830519895a294c98009ffbb44b20baa170a6b5e4a71fd9ba663

2b60e49e85b21a439855b5cb43cf799c1fb3cc0860076d52e41d48d88487e6d8

fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476

548ce27996e9309e93bf0bd29c7871977530761b2c20fc7dc3e2c16c025eb7bc

af4a10cbe8c773d6b1cfb34be2455eb023fb1b0d6f0225396920808fefb11523

Hostname

Value
www.cyprus-villas.org
www.perusmartcity.com
www.verisims.com
www.beltsymd.org
www.cyclophilit.com

External References

- https://otx.alienvault.com/pulse/6492f2af01c58203dd0bcd3b
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15