Jul 03 2023

NETMANAGEIT

Intelligence Report

Neo_Net | The Kingpin of Spanish eCrime

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In partnership with vx-underground, SentinelOne recently ran its first Malware Research Challenge, in which we asked researchers across the cybersecurity community to submit previously unpublished work to showcase their talents and bring their insights to a wider audience.

Confidence

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

15 / 100

Indicator

Name

28b973c1b890a0aa8250f13768fd841fd65e25361c0a58be893a2109c8cc99fb

Description

SHA256 of 6a907b8e5580a5067d9fb47ef21826f164f68f3f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '28b973c1b890a0aa8250f13768fd841fd65e25361c0a58be893a2109c8cc99fb']

Name

c234eb45e0e0d6a502462a6208f17b0e6b7971ce3b39330b5a347a626eabcd80

Description

SHA256 of db8eeab4ab2e2e74a34c47ad297039485ff75f22

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c234eb45e0e0d6a502462a6208f17b0e6b7971ce3b39330b5a347a626eabcd80']

Name

bbva.esentregas.ga

Pattern Type

stix

Pattern

[hostname:value = 'bbva.esentregas.ga']

Name

c82590821068b9f894d2dc2c5337442d4424909f571b7bb6796f89dda9b1dde8

Description

SHA256 of 34d0faea99d94d3923d0b9e36ef9e0c48158e7a0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c82590821068b9f894d2dc2c5337442d4424909f571b7bb6796f89dda9b1dde8']

Name
1b390636ec80fe950f72f2f36735d7ae196dc3f62df391bb3026dc8062ef088a
Description
SHA256 of dbf0cec18caabeb11387f7e6d14df54c808e441d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1b390636ec80fe950f72f2f36735d7ae196dc3f62df391bb3026dc8062ef088a']
Name
santander.esentregas.ga
Pattern Type
stix
Pattern
[hostname:value = 'santander.esentregas.ga']
Name
6f150854a7654a7e49d2bb105a25836c4ab8e877fd37887ed27fd9fa33e86a3f
Description

SHA256 of 445468cd5c298f0393f19b92b802cfa0f76c32d4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f150854a7654a7e49d2bb105a25836c4ab8e877fd37887ed27fd9fa33e86a3f']

Name

0e29076b9471d0a9d437a901f91c02150560ac2ce166eb9fbe8be63905d09f1c

Description

SHA256 of 62236a501e11d5fbfe411d841caf5f2253c150b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e29076b9471d0a9d437a901f91c02150560ac2ce166eb9fbe8be63905d09f1c']

Name

119afa1196edf4e79e1b4eeb410e907c2cc4ec0572866b82f35c97f3d450e2c5

Description

SHA256 of 5d1c7ff3d16ec770cf23a4d82a91358b9142d21a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '119afa1196edf4e79e1b4eeb410e907c2cc4ec0572866b82f35c97f3d450e2c5']

Name

correos.esentregas.ga

Pattern Type

stix

Pattern

[hostname:value = 'correos.esentregas.ga']

Name

e929e13ce2652bd5228186ab57ca621f001b6615e911251fa782d5a6c7b6210c

Description

SHA256 of a5208de82def52b4019a6d3a8da9e14a13bc2c43

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e929e13ce2652bd5228186ab57ca621f001b6615e911251fa782d5a6c7b6210c']

Name

30c804492ca939db5041444399db46d341927d5d2dea936d1543aa6aa36788ce

Description

SHA256 of ab14161e243d478dac7a83086ed4839f8ad7ded8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '30c804492ca939db5041444399db46d341927d5d2dea936d1543aa6aa36788ce']

Name

67e96978fb69f3d83159bef19689a9773e30ef0eaf84a1c78413f98545cf093e

Description

SHA256 of 145bd67f94698cc5611484f46505b3dc825bd6cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '67e96978fb69f3d83159bef19689a9773e30ef0eaf84a1c78413f98545cf093e']

Name

08dd2f12c5ea56224da1cae319e8e4e4d347f8a8304e33387850fa4070a0b7cd

Description

SHA256 of 69d38eed5dc89a7b54036cc7dcf7b96fd000eb92

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '08dd2f12c5ea56224da1cae319e8e4e4d347f8a8304e33387850fa4070a0b7cd']

Name

bbva.info-cliente.net

Pattern Type

stix

Pattern

[hostname:value = 'bbva.info-cliente.net']

Name

af6c68edd59caac782fa1db28e1eb197bf13233718c77067153c3f166dc41c96

Description

SHA256 of ef8c5d639390d9ba138ad9c2057524ff6e1398de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af6c68edd59caac782fa1db28e1eb197bf13233718c77067153c3f166dc41c96']

Name

d501c27494cd6a75af92eb69d725b4b4c5c33a9f0b54b1b2b26eac6455a998f9

Description

SHA256 of c38107addc00e2a2f5dcb6ea0cbce40400c23b49

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd501c27494cd6a75af92eb69d725b4b4c5c33a9f0b54b1b2b26eac6455a998f9']

Name

c725d8f61f83ca6586453bba3d2a198f5b67a7988bdbb0780a1a59bd13ea4b2b

Description

SHA256 of 7b4ab7b2ead7e004c0d93fe916af39c156e0bc61

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c725d8f61f83ca6586453bba3d2a198f5b67a7988bdbb0780a1a59bd13ea4b2b']

Intrusion-Set

Name
Neo_Net

Attack-Pattern

Name
Encrypted Channel
ID
T1521
Description
Adversaries may explicitly employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if necessary secret keys are encoded and/or generated within malware samples/configuration files.
Name
Web Service
ID
T1481
Description
Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover. This is due to the likelihood that

hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis, or enable operational resiliency (since this infrastructure may be dynamically changed).

Name

Application Layer Protocol

ID

T1437

Description

Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the mobile device, and often the results of those commands, will be embedded within the protocol traffic between the mobile device and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS.

Name

System Information Discovery

ID

T1426

Description

Adversaries may attempt to get detailed information about a device's operating system and hardware, including versions, patches, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1426) during automated discovery to shape follow-on behaviors, including whether or not to fully infects the target and/or attempts specific actions. On Android, much of this

information is programmatically accessible to applications through the `android.os.Build` class. (Citation: Android-Build) iOS is much more restrictive with what information is visible to applications. Typically, applications will only be able to query the device model and which version of iOS it is running.

Name

Obfuscated Files or Information

ID

T1406

Description

Adversaries may attempt to make a payload or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the device or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Portions of files can also be encoded to hide the plaintext strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled.(Citation: Microsoft MalLockerB)

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

StixFile

Value
08dd2f12c5ea56224da1cae319e8e4e4d347f8a8304e33387850fa4070a0b7cd
c234eb45e0e0d6a502462a6208f17b0e6b7971ce3b39330b5a347a626eabcd80
1b390636ec80fe950f72f2f36735d7ae196dc3f62df391bb3026dc8062ef088a
c82590821068b9f894d2dc2c5337442d4424909f571b7bb6796f89dda9b1dde8
e929e13ce2652bd5228186ab57ca621f001b6615e911251fa782d5a6c7b6210c
6f150854a7654a7e49d2bb105a25836c4ab8e877fd37887ed27fd9fa33e86a3f
67e96978fb69f3d83159bef19689a9773e30ef0eaf84a1c78413f98545cf093e
0e29076b9471d0a9d437a901f91c02150560ac2ce166eb9fbe8be63905d09f1c
d501c27494cd6a75af92eb69d725b4b4c5c33a9f0b54b1b2b26eac6455a998f9
119afa1196edf4e79e1b4eeb410e907c2cc4ec0572866b82f35c97f3d450e2c5
30c804492ca939db5041444399db46d341927d5d2dea936d1543aa6aa36788ce
c725d8f61f83ca6586453bba3d2a198f5b67a7988bdbb0780a1a59bd13ea4b2b
28b973c1b890a0aa8250f13768fd841fd65e25361c0a58be893a2109c8cc99fb

af6c68edd59caac782fa1db28e1eb197bf13233718c77067153c3f166dc41c96

Hostname

Value
bbva.info-cliente.net
bbva.esentregas.ga
santander.esentregas.ga
correos.esentregas.ga

External References

- https://otx.alienvault.com/pulse/64a2dd44dc904c36b1dcf74f
- https://www.sentinelone.com/blog/neo_net-the-kingpin-of-spanish-ecrime/