NETMANAGEIT

Intelligence Report

Botnet Fenix: New botnet going after tax payers in Mexico and Chile

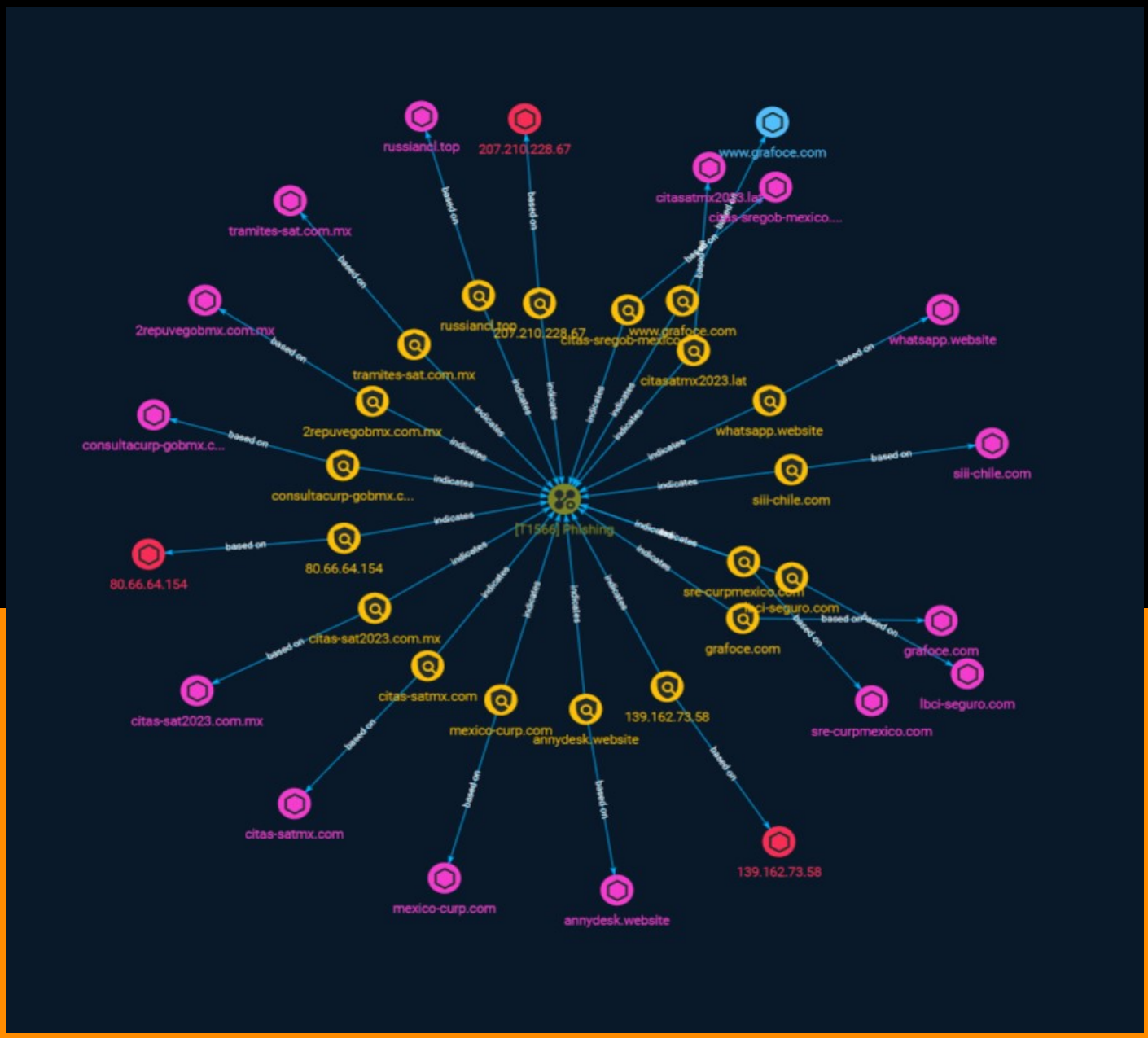

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers recently uncovered a local group that created a new botnet self-proclaimed as “Fenix,” which specifically targets users accessing government services, particularly tax-paying individuals in Mexico and Chile.

Confidence

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

15 / 100

Indicator

Name
www.grafoce.com
Pattern Type
stix
Pattern
[hostname:value = 'www.grafoce.com']
Name
sre-curpmexico.com
Pattern Type
stix
Pattern
[domain-name:value = 'sre-curpmexico.com']
Name
tramites-sat.com.mx

Pattern Type
stix
Pattern
[domain-name:value = 'tramites-sat.com.mx']
Name
grafoce.com
Pattern Type
stix
Pattern
[domain-name:value = 'grafoce.com']
Name
citas-satmx.com
Pattern Type
stix
Pattern
[domain-name:value = 'citas-satmx.com']
Name
lbci-seguro.com

Pattern Type
stix
Pattern
[domain-name:value = 'lbci-seguro.com']
Name
citas-sat2023.com.mx
Pattern Type
stix
Pattern
[domain-name:value = 'citas-sat2023.com.mx']
Name
citas-sregob-mexico.com
Pattern Type
stix
Pattern
[domain-name:value = 'citas-sregob-mexico.com']
Name
siii-chile.com

Pattern Type
stix
Pattern
[domain-name:value = 'siii-chile.com']
Name
207.210.228.67
Description
CC=US ASN=AS17378 AS17378
Pattern Type
stix
Pattern
[ipv4-addr:value = '207.210.228.67']
Name
russiancl.top
Pattern Type
stix
Pattern
[domain-name:value = 'russiancl.top']

Name

annydesk.website

Pattern Type

stix

Pattern

[domain-name:value = 'annydesk.website']

Name

80.66.64.154

Description

ISP: HUIZE LTD **OS:** Debian ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDAt0NzG7Vajv/z6/uFwUH8SQPsH3fLU7fL3RqYd4NFPcPZ 0IZUVGbYbh0/dk/PbiiA9HMLmCTDuUgRPt94l2vNQZBaqt9SttPtAUWQkuHsqsnVIgJD43JWterK 5XRHXS/1Gh4OUKN/9udSfjRnhzbxP5FDBa/aEfJQvmhrDoPD0Q/UjstXSp7lsBcLEyJJZ5t32tih andS+Apim7tRiMJDQeSTU3rg6GbyrYHHo8SwqtJtc87lVkvREjYlmp5GOpxDRnBFbgV6VwpNXSNP dwjFGG/8biWz3aTuUMhUynQuSL+5PN8VPWlJSTXLysBpQhIH+BnXGoJK+T26dQ8e6ldv Fingerprint: 96:ea:77:a1:a9:01:e3:8a:ac:8b:9d:57:72:d3:d7:65 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.0 503 Service

Unavailable Cache-Control: no-cache Connection: close Content-Type: text/html ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.64.154']

Name

citasatmx2023.lat

Pattern Type

stix

Pattern

[domain-name:value = 'citasatmx2023.lat']

Name

mexico-curp.com

Pattern Type

stix

Pattern

[domain-name:value = 'mexico-curp.com']

Name

consultacurp-gobmx.com.mx

Pattern Type

stix

Pattern

[domain-name:value = 'consultacurp-gobmx.com.mx']

Name

139.162.73.58

Description

ISP: Akamai Connected Cloud **OS:** None ------------------------- Hostnames: - 139-162-73-58.ip.linodeusercontent.com ------------------------- Domains: - linodeusercontent.com ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDRQrutGlAicn2tf+gkymMKE13Px9747Q/kVd8bAmr8JGRv bX52c/b6TTbPviXYWm1QBryVh3oU+iNP0q++JT+OFgGp1z6EUqICV9whX8ICoFJc+EkQ4ALVyVav UoOhiEowr6/v6oKoFMdrecmmOvsUCqtrcfneKBp1sBt3K615QxwRexYH1hDzvL13Z3HUZ5bjh1uB icX0yu86Co4nn65zH4+q9+JzvvRhtpqD6UQpVYf0KrkZaRlZHZy3rJlmN/EIVEM4PGR2dVG+as7M +Z2r++mSTKU7ga+PQwc+9FHvRbfRfMVzwXeG2GvrlRJFyOlwuasOrO84zEx5gWqQbTef Fingerprint: ce:9d:b3:2b:eb:d9:b9:9d:d3:53:32:06:85:42:ac:09 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com

umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.162.73.58']

Name

2repuvegobmx.com.mx

Pattern Type

stix

Pattern

[domain-name:value = '2repuvegobmx.com.mx']

Name

whatsapp.website

Pattern Type

stix

Pattern

[domain-name:value = 'whatsapp.website']

Country

Name
Chile

Name
Mexico

Attack-Pattern

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)

Domain-Name

Value
grafoce.com
citas-sat2023.com.mx
citas-sregob-mexico.com
sre-curpmexico.com
citasatmx2023.lat
whatsapp.website
citas-satmx.com
russiancl.top
lbci-seguro.com
consultacurp-gobmx.com.mx
2repuvegobmx.com.mx
mexico-curp.com
tramites-sat.com.mx

siii-chile.com

annydesk.website

Hostname

Value
www.grafoce.com

IPv4-Addr

Value
139.162.73.58
80.66.64.154
207.210.228.67

External References

- https://otx.alienvault.com/pulse/64c1336884593c36acc3e40e