Jan 12 2024

NETMANAGEIT

Intelligence Report

Pivoting through a Sea of indicators to spot Turtles

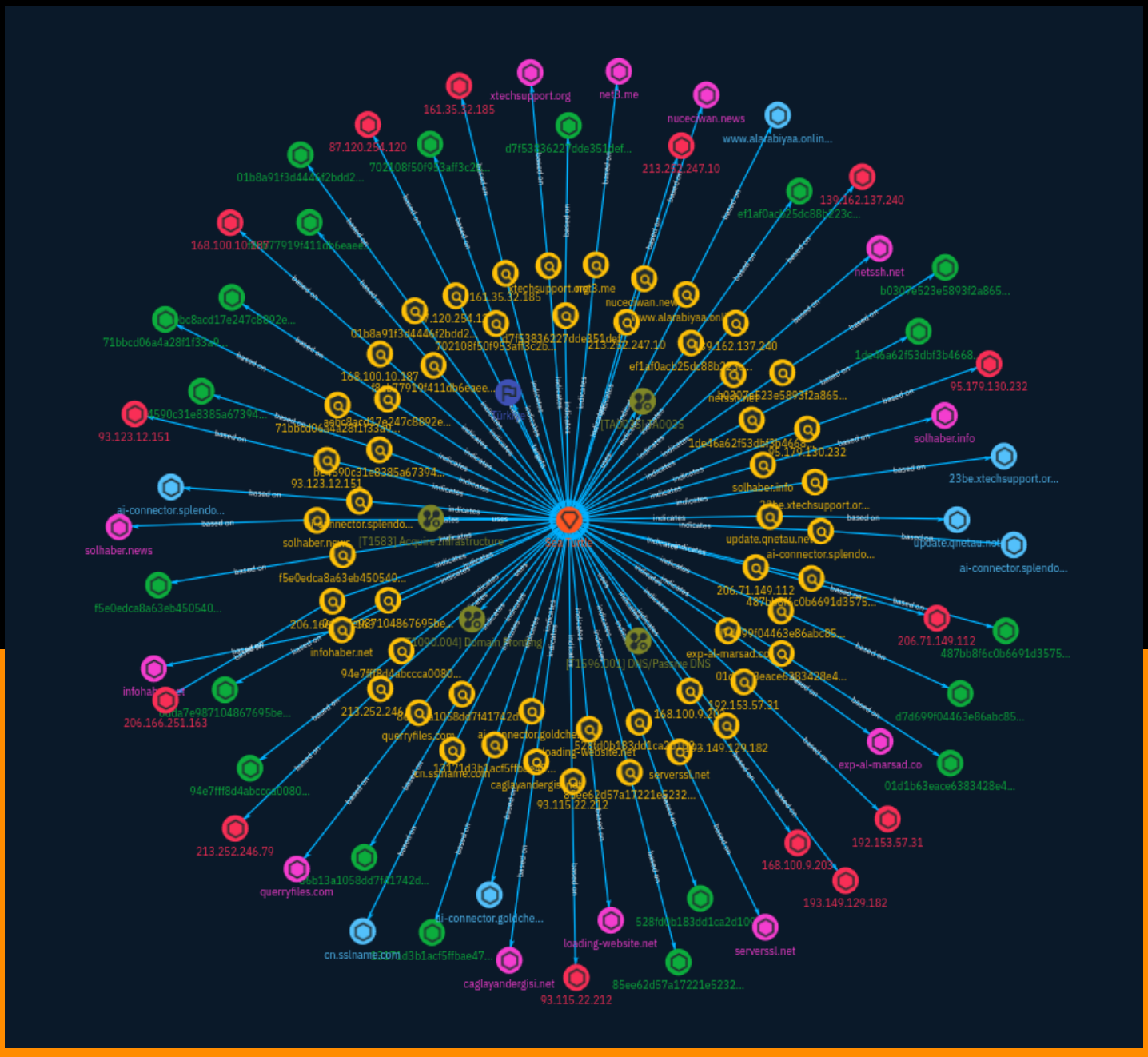

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Sea Turtle is a threat group that tends to swim under the radar, but recently the Ministry of Justice in Greece, PWC, and others before them, published reports containing infrastructure currently in use. It was once believed that when an IP or domain was outed publicly, that an actor, especially a well-resourced one, would burn it down. In this blog we'll pull on threads to show that isn't always the case.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Domain Fronting
ID
T1090.004
Description
Adversaries may take advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. (Citation: Fifield Blocking Resistent Communication through domain fronting 2015) Domain fronting involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. If both domains are served from the same CDN, then the CDN may route to the address specified in the HTTP header after unwrapping the TLS header. A variation of the the technique, "domainless" fronting, utilizes a SNI field that is left blank; this may allow the fronting to work even when the CDN attempts to validate that the SNI and HTTP Host fields match (if the blank SNI fields are ignored). For example, if domain-x and domain-y are customers of the same CDN, it is possible to place domain-x in the TLS header and domain-y in the HTTP header. Traffic will appear to be going to domain-x, however the CDN may route it to domain-y.
Name
Acquire Infrastructure
ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090), including from residential proxy services.(Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing) (Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Name

TA0035

ID

TA0035

Name

DNS/Passive DNS

ID

T1596.001

Description

Adversaries may search DNS data for information about victims that can be used during targeting. DNS information may include a variety of details, including registered name servers as well as records that outline addressing for a target's subdomains, mail servers,

and other hosts. Adversaries may search DNS data to gather actionable information. Threat actors can query nameservers for a target organization directly, or search through centralized repositories of logged DNS query responses (known as passive DNS).(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Adversaries may also seek and target DNS misconfigurations/leaks that reveal information about internal networks. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

Indicator

Name

01d1b63eace6383428e42c48f3d1e13e643e8a8f70d4af5d4ee6f47a0522e300

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01d1b63eace6383428e42c48f3d1e13e643e8a8f70d4af5d4ee6f47a0522e300']

Name

168.100.10.187

Description

ISP: BL Networks **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEPI/5eUEBhseO4L04Xb44XF gWklEsNlukEmSS2KESFyqf0jkY+l8C78coWCSp0N4RqahP0FvnIHLwQVz9o4q+s= Fingerprint: 45:8b:38:f9:25:45:33:22:fa:5c:6f:9c:e9:29:db:f7 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256

kex-strict-s-v00@openssh.com Server Host Key Algorithms: 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 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 = '168.100.10.187']

Name

161.35.32.185

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_9.0p1 Ubuntu-1ubuntu7.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLo3fynUa0DDQd2jOiHCvL0Z /+09ed7/9bpmlclrB8dsnCUoBfzkP/VFPB21FzTBKBDB9wwx5Qtfw+ZvVeq7YhA= Fingerprint: f7:6d:b1:0c:c1:7d:18:7d:be:f1:be:67:fe:a0:c7:d7 Kex Algorithms: sntrup761x25519-sha512@openssh.com 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 Server Host Key Algorithms: 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 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:** ``` ``` ---------- **443:** ``` SSL Error: TLSV1_UNRECOGNIZED_NAME ``` ----------

8000: ``` HTTP/1.1 404 Not Found date: Tue, 09 Jan 2024 12:09:33 GMT server: uvicorn content-length: 22 content-type: application/json ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '161.35.32.185']

Name

cn.sslname.com

Pattern Type

stix

Pattern

[hostname:value = 'cn.sslname.com']

Name

b0307e523e5893f2a865b0abea91cb4fb2e9d86fc71e33adaf63c8878fac2748

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b0307e523e5893f2a865b0abea91cb4fb2e9d86fc71e33adaf63c8878fac2748']

Name

192.153.57.31

Description

ISP: BL Networks **OS:** None ---------- Hostnames: - solhaber.news ---------- Domains: - solhaber.news ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIz0xOodFW2BPhu5eWKLrNtO xOUfPY8EiEF+QFSkcZ/9G++UEsUhyWWrNKx3YNvKHj/bdvEJjrrpB9SmsMpsrfE= Fingerprint: d2:70:02:60:de:1a:85:4a:fb:c3:e8:d6:b3:14:06:f0 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: 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 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 ``` ---------- **443:** ``` HTTP/1.1 404 NOT FOUND Server: nginx Date: Fri, 05 Jan 2024 03:12:46 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.153.57.31']

Name

168.100.9.203

Description
IcedID botnet C2 server (confidence level: 75%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '168.100.9.203']
Name
ai-connector.splendos.org
Pattern Type
stix
Pattern
[hostname:value = 'ai-connector.splendos.org']
Name
86b13a1058dd7f41742dfb192252ac9449724c5c0a675c031602bd9f36dd49b5
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '86b13a1058dd7f41742dfb192252ac9449724c5c0a675c031602bd9f36dd49b5']

Name

f5e0edca8a63eb45054039104f509ef0e66fc2e67637614a0f386803506cbac1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f5e0edca8a63eb45054039104f509ef0e66fc2e67637614a0f386803506cbac1']

Name

exp-al-marsad.co

Pattern Type

stix

Pattern

[domain-name:value = 'exp-al-marsad.co']

Name

be4590c31e8385a67394f7d49147a0b97cff07da6ff771614d3d3ed9ad2cd49f

Description

research_pe_signed_outside_timestamp

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'be4590c31e8385a67394f7d49147a0b97cff07da6ff771614d3d3ed9ad2cd49f']

Name

nuceciwan.news

Pattern Type

stix

Pattern

[domain-name:value = 'nuceciwan.news']

Name

93.115.22.212

Description

CC=NL ASN=AS202448 MVPS LTD

Pattern Type

stix

Pattern

[ipv4-addr:value = '93.115.22.212']

Name

caglayandergisi.net

Pattern Type

stix

Pattern

[domain-name:value = 'caglayandergisi.net']

Name

213.252.247.10

Description

ISP: Informacines sistemos ir technologijos, UAB **OS:** Ubuntu ---------- Hostnames: - 24223-41004.bacloud.info - 21282-40076.bacloud.info ---------- Domains: - bacloud.info ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDt3X3ZWYpUKSpIyfJYc6rbROHqDpdY5rQxkayCCj7/amdU sBpoH9F6p9+8gfS+ohwlcxcyEyH5adyXS06eamR+WKmGgOYB8q3LjcTfwWLstWHq5FbY22mcvnyb FjzO3CbWqmUtOiJOa6Em5f0DN9U7+xd+Ma5+wQ3/DXneAjHMHaQ2QR1gHe79Mrc5wDeTN3fEKvzV VAdmrRdyRqL+ji8LvJnbS73rBCi5gnpfUZA15JAjnHF8vAnGlOU6orp5qBt7Rer/e64iP38GyGK5 RU2oOMBKnj+XP+h880JGuDHAY56T5O+IqeKnNeOWt/NRx1wrYb/inTvRIWB/MdE1uXFf Fingerprint: d8:db:d2:38:53:f1:06:7e:a2:52:58:3e:00:20:e6:17 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 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa 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 ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Mon, 18 Dec 2023 00:22:21 GMT Content-Type: text/html; charset=utf-8 Content-Length: 628 Last-Modified: Fri, 01 Dec 2023 18:57:15 GMT Connection: keep-alive ETag: "656a2c8b-274" Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Accept-Ranges: bytes ``` HEARTBLEED: 2023/12/18 00:22:30 213.252.247.10:443 - SAFE ---------- **9100:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Connection: close 400 Bad Request Prometheus Node Exporter: node_exporter_build_info: branch: HEAD goarch: amd64 goos: linux goversion: go1.21.4 revision: 7333465abf9efba81876303bb57e6fadb946041b tags: netgo osusergo static_build version: 1.7.0 node_os_info: id: ubuntu id_like: debian name: Ubuntu pretty_name: Ubuntu 20.04 LTS version: 20.04 LTS (Focal Fossa) version_codename: focal version_id: 20.04 node_uname_info: domainname: (none) machine: x86_64 nodename: aussietrust-node2 release: 5.4.0-28-generic sysname: Linux version: #32-Ubuntu SMP Wed Apr 22 17:40:10 UTC 2020 node_dmi_info: bios_date: 04/01/2014 bios_vendor: SeaBIOS bios_version: 1.11.0-2.el7 chassis_vendor: Red Hat chassis_version: RHEL 7.6.0 PC (i440FX + PIIX, 1996) product_family: Red Hat Enterprise Linux product_name: KVM product_version: RHEL 7.6.0 PC (i440FX + PIIX, 1996) system_vendor: Red Hat node_network_info: lo: address: 00:00:00:00:00:00 adminstate: up broadcast: 00:00:00:00:00:00 device: lo operstate: unknown ovs-system: address: 4a:f3:49:a1:16:70 adminstate: down broadcast: ff:ff:ff:ff:ff:ff device: ovs-system operstate: down mysql-se-06a0dc: address: c2:25:0d:a8:0c:f1 adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: mysql-se-06a0dc duplex: full operstate: up antrea-gw0: address: 5e:24:e4:0c:07:05 adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: antrea-gw0 operstate: unknown genev_sys_6081: address: 32:2b:3b:ff:ed:7e adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: genev_sys_6081 operstate: unknown antrea-egress0: address: 3a:d1:c3:3b:77:80 adminstate: down broadcast: ff:ff:ff:ff:ff:ff device: antrea-egress0 operstate: down eth0: address: 00:16:3c:e5:42:05 adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: eth0 duplex: unknown operstate: up ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.252.247.10']

Name

85ee62d57a17221e52325020b4d6f587f68fb321723be7ed794503b40bd989f7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '85ee62d57a17221e52325020b4d6f587f68fb321723be7ed794503b40bd989f7']

Name

71bbcd06a4a28f1f33a998928bfe6d78aa7a56fe068c61556f41e2586809a470

Description

UPX

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '71bbcd06a4a28f1f33a998928bfe6d78aa7a56fe068c61556f41e2586809a470']

Name

d7d699f04463e86abc85ec029953ea7d558fd385a5e73ce0cc0d9cd0dbebd41e

Description

GoLandBuildPE

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd7d699f04463e86abc85ec029953ea7d558fd385a5e73ce0cc0d9cd0dbebd41e']

Name

213.252.246.79

Description

CC=LT ASN=AS61272 Informacines sistemos ir technologijos, UAB

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.252.246.79']

Name

87.120.254.120

Description

ISP: Neterra Ltd. **OS:** None ---------- Hostnames: - caglayandergisi.net ---------- Domains: - caglayandergisi.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHvv7AZTPi/UNkCD/QvSpba4 e90OpoCnnL8I21R4Vq+tdS5YnldkpPgMWRoWI6b4DH1edfyzdKNdEHxWrRyxMPM= Fingerprint: 5d:e2:21:cd:54:aa:ca:ba:01:33:ca:e1:60:b6:b7:b4 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: 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 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 ``` ---------- **443:** ``` HTTP/1.1 426 Upgrade Required Date: Sat, 30 Dec 2023 16:35:58 GMT Content-Type: application/json Content-Length: 29 Connection: keep-alive Server: Apache ``` HEARTBLEED: 2023/12/30 16:36:11 87.120.254.120:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '87.120.254.120']

Name

23be.xtechsupport.org

Pattern Type

stix

Pattern

[hostname:value = '23be.xtechsupport.org']

Name

93.123.12.151

Description

Cobalt Strike botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '93.123.12.151']

Name

d7f53836227dde351def7c1a5e9dd03c3a49bdc4eec6342136795038aa6d415d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd7f53836227dde351def7c1a5e9dd03c3a49bdc4eec6342136795038aa6d415d']

Name

aebc8acd17e247c8892e6a8226be4dbf2af3848bdcc1cc1536d1f8487bed55a4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aebc8acd17e247c8892e6a8226be4dbf2af3848bdcc1cc1536d1f8487bed55a4']

Name

702108f50f953aff3c2b345c2604e9fa614cb86d8299c209065b41878fd4f66b

Description

Win64:Trojan-gen

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '702108f50f953aff3c2b345c2604e9fa614cb86d8299c209065b41878fd4f66b']

Name

ai-connector.goldchekin.com

Pattern Type

stix

Pattern

[hostname:value = 'ai-connector.goldchekin.com']

Name

0dda7e987104867695be561a8008d3282252e05c611c247eae62c7b798be0e24

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0dda7e987104867695be561a8008d3282252e05c611c247eae62c7b798be0e24']

Name

update.qnetau.net

Pattern Type

stix

Pattern

[hostname:value = 'update.qnetau.net']

Name

13171d3b1acf5ffbae47777cae03d5d6cb96d2d9b76fe4491bf547b2e309fb52

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '13171d3b1acf5ffbae47777cae03d5d6cb96d2d9b76fe4491bf547b2e309fb52']

Name

netssh.net

Pattern Type

stix

Pattern

[domain-name:value = 'netssh.net']

Name

1de46a62f53dbf3b4668bfa7fe63c022c541d8651f776fa5fd8060f21036e63a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1de46a62f53dbf3b4668bfa7fe63c022c541d8651f776fa5fd8060f21036e63a']

Name

206.166.251.163

Description

ISP: BL Networks **OS:** None ---------- Hostnames: - www.alarabiyaa.online - alarabiyaa.online ---------- Domains: - alarabiyaa.online ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEl0SVzyokMOkjMw6GEUKZJE IY0TXKwBxwtd4Z2Rr/HPi/8/5YqgyfF0AfwtOHjbCU8QnAeGRPfLImU+pp58asA= Fingerprint: 5c:c4:e9:6f:31:34:ff:50:9c:40:68:c4:98:f6:45:4d Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: 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 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 ``` ---------- **443:** ``` HTTP/1.1 426 Upgrade Required Date: Sun, 17 Dec 2023 05:54:57 GMT Content-Type: application/json Content-Length: 29 Connection: keep-alive Server: Apache ``` HEARTBLEED: 2023/12/17 05:55:18 206.166.251.163:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '206.166.251.163']

Name

xtechsupport.org

Pattern Type

stix

Pattern

[domain-name:value = 'xtechsupport.org']

Name

serverssl.net

Pattern Type

stix

Pattern

[domain-name:value = 'serverssl.net']

Name

querryfiles.com

Pattern Type

stix

Pattern

[domain-name:value = 'querryfiles.com']

Name

95.179.130.232

Description

AsyncRAT botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.179.130.232']

Name

206.71.149.112

Description

ISP: BL Networks **OS:** None ---------- Hostnames: - www.pictture.online - pictture.online ---------- Domains: - pictture.online ---------- Services: **443:** ``` HTTP/1.1 426 Upgrade Required Date: Sat, 30 Dec 2023 12:50:36 GMT Content-Type: application/json Content-Length: 29 Connection: keep-alive Server: Apache ``` HEARTBLEED: 2023/12/30 12:50:55 206.71.149.112:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '206.71.149.112']

Name

01b8a91f3d4446f2bdd22c85b225dfd2f619951e8f33178c3185dbf7543845df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01b8a91f3d4446f2bdd22c85b225dfd2f619951e8f33178c3185dbf7543845df']

Name

528fd0b183dd1ca2d109af1714d1ee89d3244c37451203b7b14e951742e16741

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '528fd0b183dd1ca2d109af1714d1ee89d3244c37451203b7b14e951742e16741']

Name

94e7fff8d4abccca0080004a497153ce04f74f7507b52ca092462e22d84f0f8a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '94e7fff8d4abccca0080004a497153ce04f74f7507b52ca092462e22d84f0f8a']

Name

www.alarabiyaa.online

Pattern Type

stix

Pattern

[hostname:value = 'www.alarabiyaa.online']

Name

193.149.129.182

Description

ISP: BL Networks **OS:** None ------------------------- Hostnames: - solhaber.info ------------------------- Domains: - solhaber.info ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA8/dFCwo2kzeIQD0rZkzb62 hnOg3RrGt+D4gfLOLycSdjumoDxU8so+Li/h2GYeaM7PA/9VdQRzt32DieoF3FY= Fingerprint: 15:fe:2f:79:7b:78:45:01:58:52:9f:7f:19:19:4a:0d Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: 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 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 ``` ---------- **443:** ``` HTTP/1.1 426 Upgrade Required Date: Mon, 01 Jan 2024 20:13:42 GMT Content-Type: application/json Content-Length: 29 Connection: keep-alive Server: Apache ``` HEARTBLEED: 2024/01/01 20:13:58 193.149.129.182:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.149.129.182']

Name

f8cb77919f411db6eaeea8f0c8394239ad38222fe15abc024362771f611c360f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f8cb77919f411db6eaeea8f0c8394239ad38222fe15abc024362771f611c360f']

Name

ef1af0acb25dc88b223c7b6a6be48d35a64665bb372cf8b7674cacd5818f7ff3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ef1af0acb25dc88b223c7b6a6be48d35a64665bb372cf8b7674cacd5818f7ff3']

Name

solhaber.news

Pattern Type

stix

Pattern

[domain-name:value = 'solhaber.news']

Name

net3.me

Pattern Type

stix

Pattern

[domain-name:value = 'net3.me']

Name

loading-website.net

Pattern Type

stix

Pattern

[domain-name:value = 'loading-website.net']

Name

ai-connector.splendor.org

Pattern Type

stix

Pattern

[hostname:value = 'ai-connector.splendor.org']

Name

solhaber.info

Pattern Type

stix

Pattern

[domain-name:value = 'solhaber.info']

Name

infohaber.net

Pattern Type

stix

Pattern

[domain-name:value = 'infohaber.net']

Name

139.162.137.240

Description

ISP: Akamai Connected Cloud **OS:** None ---------- Hostnames: - a.greenblu.club - 139-162-137-240.ip.linodeusercontent.com ---------- Domains: - greenblu.club - linodeusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDwUEJLqDOFmiFtY7NmJd8JivWMm4Z+k2Qot2FE5CzW6aoy 0anVHEndzE1DETqfdUoP5OqIAL7et63PTsGBBKfGn+NQ3rGi4xSsJL/Nur5W4QMOHu/R1MbZEcBR 2bMVHfW9M9SNKHiW2LKIlNl73e73GeEgIh1kfj+/S8Gx2cdz9dLHkiAX08s2xInF+aqzJWwmtNX8 0rNy1MzLlYpqfurV7VvcVlgM+LhPQkkqiPHu8LuvMuKXN41319oK0+J2nDjDVnI/9fPioG4P6Nwa 7Y0MSgTHVtj3Vv1/93fQEtTvwibPkPqud0IeNuuXIFVCpNG8fenDOTyVHEhGjeKhJejFLMcY5vUg o8135Xqev0jfAWSX6EzmLK2hrT9/fXoV8Cc+YhvU6BD3UwyVmqce/qsTZWrefXmgXjiwkRFRNaxg bJfiEIkL8pOFPryLlbuvjr5HGSxlG4o0K6jlMc1X0166u9tlh/9pxIgrgx0YGZI0+TblaPAdxson eayPUYLFI/k= Fingerprint: e5:37:f5:31:22:26:e3:f0:56:f5:7d:58:3a:d3:0c:25 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Sat, 06 Jan 2024 17:42:01 GMT Content-Type: text/html; charset=utf-8 Content-Length: 147 Connection: keep-alive Cache-Control: no-cache, no-store, must-revalidate Expires: Sat, 06 Jan 2024 17:42:01 GMT Vary: Accept-Encoding ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Thu, 11 Jan 2024 03:28:53 GMT Content-Type: text/html; charset=utf-8 Content-Length: 147 Connection: keep-alive Cache-Control: no-cache, no-store, must-revalidate Expires: Thu, 11 Jan 2024 03:28:53 GMT Vary: Accept-Encoding ``` HEARTBLEED: 2024/01/11 03:28:57 139.162.137.240:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.162.137.240']

Name
487bb8f6c0b6691d3575eee3faa8bfc73ddebe0d1052c02b636cc0a394ed384d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '487bb8f6c0b6691d3575eee3faa8bfc73ddebe0d1052c02b636cc0a394ed384d']

Intrusion-Set

Name
Sea Turtle

Country

Name
Türkiye

Domain-Name

Value
loading-website.net
net3.me
querryfiles.com
infohaber.net
netssh.net
solhaber.info
xtechsupport.org
caglayandergisi.net
exp-al-marsad.co
nuceciwan.news
serverssl.net
solhaber.news

StixFile

Value
01b8a91f3d4446f2bdd22c85b225dfd2f619951e8f33178c3185dbf7543845df
01d1b63eace6383428e42c48f3d1e13e643e8a8f70d4af5d4ee6f47a0522e300
487bb8f6c0b6691d3575eee3faa8bfc73ddebe0d1052c02b636cc0a394ed384d
d7f53836227dde351def7c1a5e9dd03c3a49bdc4eec6342136795038aa6d415d
0dda7e987104867695be561a8008d3282252e05c611c247eae62c7b798be0e24
d7d699f04463e86abc85ec029953ea7d558fd385a5e73ce0cc0d9cd0dbebd41e
ef1af0acb25dc88b223c7b6a6be48d35a64665bb372cf8b7674cacd5818f7ff3
94e7fff8d4abccca0080004a497153ce04f74f7507b52ca092462e22d84f0f8a
86b13a1058dd7f41742dfb192252ac9449724c5c0a675c031602bd9f36dd49b5
f8cb77919f411db6eaeea8f0c8394239ad38222fe15abc024362771f611c360f
13171d3b1acf5ffbae47777cae03d5d6cb96d2d9b76fe4491bf547b2e309fb52
be4590c31e8385a67394f7d49147a0b97cff07da6ff771614d3d3ed9ad2cd49f
85ee62d57a17221e52325020b4d6f587f68fb321723be7ed794503b40bd989f7

702108f50f953aff3c2b345c2604e9fa614cb86d8299c209065b41878fd4f66b
1de46a62f53dbf3b4668bfa7fe63c022c541d8651f776fa5fd8060f21036e63a
f5e0edca8a63eb45054039104f509ef0e66fc2e67637614a0f386803506cbac1
71bbcd06a4a28f1f33a998928bfe6d78aa7a56fe068c61556f41e2586809a470
b0307e523e5893f2a865b0abea91cb4fb2e9d86fc71e33adaf63c8878fac2748
528fd0b183dd1ca2d109af1714d1ee89d3244c37451203b7b14e951742e16741
aebc8acd17e247c8892e6a8226be4dbf2af3848bdcc1cc1536d1f8487bed55a4

Hostname

Value
ai-connector.splendor.org
update.qnetau.net
www.alarabiyaa.online
ai-connector.splendos.org
ai-connector.goldchekin.com
23be.xtechsupport.org
cn.sslname.com

IPv4-Addr

Value
168.100.9.203
206.166.251.163
168.100.10.187
192.153.57.31
87.120.254.120
139.162.137.240
213.252.246.79
213.252.247.10
193.149.129.182
93.123.12.151
206.71.149.112
93.115.22.212
161.35.32.185

95.179.130.232

External References

- https://otx.alienvault.com/pulse/65a0740fefe93d8593b812af
- https://blog.strikeready.com/blog/pivoting-through-a-sea-of-indicators-to-spot-turtles/