Apr 10 2024

NETMANAGEIT

Intelligence Report

Malware-Initiated Vulnerability Scanning Is on the Rise

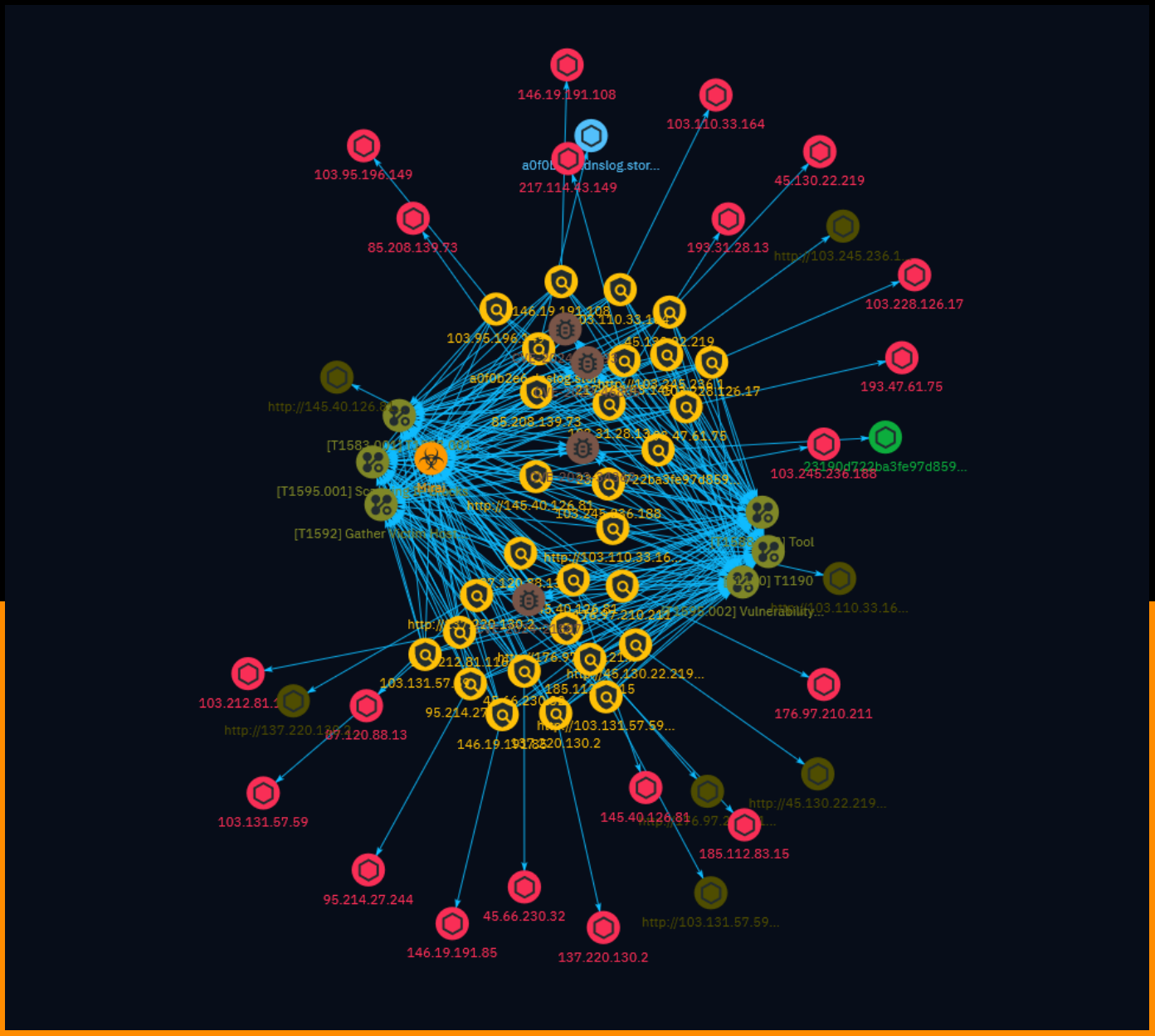

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Vulnerability 23
- Malware 25
- Attack-Pattern 26

Observables

- Hostname 31
- Url 32
- IPv4-Addr 33

- StixFile 35

External References

- External References 36

Overview

Description

This insightful analysis examines the growing trend of malware-driven vulnerability scanning, where threat actors leverage infected devices to conduct scans and exploit vulnerabilities. It delves into various case studies, including the evolution of the Mirai botnet and the exploitation of Ivanti vulnerabilities. The report provides valuable insights into the tactics, techniques, and indicators associated with these malicious activities, emphasizing the importance of robust defense mechanisms against such scanning attacks.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

a0f0b2e6.dnslog.store

Pattern Type

stix

Pattern

[hostname:value = 'a0f0b2e6.dnslog.store']

Name

http://176.97.210.211/mips

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 176.97.210.211 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://176.97.210.211/mips']

Name

http://145.40.126.81/mips

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 145.40.126.81 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://145.40.126.81/mips']

Name

http://103.110.33.164/mips;$

Pattern Type

stix

Pattern

[url:value = 'http://103.110.33.164/mips;$']

Name

87.120.88.13

Description

- **Zip Code:** N/A - **ISP:** Stark Industries Solutions - **ASN:** 44477 - **Organization:** Stark Industries Solutions - **Is Crawler:** False - **Timezone:** Asia/Bangkok - **Mobile:** False - **Host:** 87.120.88.13 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** TH - **Region:** Phuket - **City:** Phuket - **Latitude:** 7.89 - **Longitude:** 98.4

Pattern Type

stix

Pattern

[ipv4-addr:value = '87.120.88.13']

Name

217.114.43.149

Description

ISP: Cloud Hosting Solutions, Limited. **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBENl0AIFGYXghVgbgIfUbqos27f4qe3WCkWEHWWOEudRg3lHniBp6kGKsY7942XtctpwGr4hgOxzyfA11UPVYfw= Fingerprint: bd:cb:db:61:53:52:07:68:41:a0:61:01:52:d5:c3:fd 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 28 Mar 2024 15:57:39 GMT Content-Type: text/html Content-Length: 98 Last-Modified: Mon, 19 Jun 2023 22:10:50 GMT Connection: keep-alive ETag: "6490d26a-62" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.114.43.149']

Name

185.112.83.15

Description

ISP: Aeza Group Ltd. **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAirYwZEuOVuWG4l+gl0m6jR yPbuH70/+wmIsyvLmxRjjW5n3gj3tluXQODUHMERbBeWeRxvIjgwJafY3BeFbs8= Fingerprint: c0:dc:f0:92:fc:91:84:f7:65:ba:73:13:be:0c:67:6a 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 = '185.112.83.15']

Name

103.95.196.149

Description

ISP: VIET DIGITAL TECHNOLOGY LIABILITY COMPANY **OS:** - ---------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 ; Administrator SES ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Wed, 03 Apr 2024 20:59:30 GMT Connection: close Content-Length: 315 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.95.196.149']

Name

23190d722ba3fe97d859bd9b086ff33a14ae9aecfc8a2c3427623f93de3d3b14

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23190d722ba3fe97d859bd9b086ff33a14ae9aecfc8a2c3427623f93de3d3b14']

Name

103.245.236.188

Description

- **Zip Code:** N/A - **ISP:** Lp Technology Electronic Commerce Company - **ASN:** 150867 - **Organization:** Lp Technology Electronic Commerce Company - **Is Crawler:** False - **Timezone:** Asia/Ho_Chi_Minh - **Mobile:** False - **Host:** 103.245.236.188 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** VN - **Region:** Ho Chi Minh - **City:** Quan Binh Thanh - **Latitude:** 10.81 - **Longitude:** 106.71

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.245.236.188']

Name

103.228.126.17

Description

- **Zip Code:** N/A - **ISP:** Vpsmmo Technology Company - **ASN:** 149078 - **Organization:** Vpsmmo Technology Company - **Is Crawler:** False - **Timezone:** Australia/Sydney - **Mobile:** False - **Host:** 103.228.126.17 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** AU - **Region:** New South Wales - **City:** Sydney - **Latitude:** -33.87149811 - **Longitude:** 151.2006073

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.228.126.17']

Name

95.214.27.244

Description

- **Zip Code:** N/A - **ISP:** Datacamp - **ASN:** 212238 - **Organization:** Datacamp - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** 95.214.27.244 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** North Holland - **City:** Amsterdam - **Latitude:** 52.36399841 - **Longitude:** 4.8913002

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.214.27.244']

Name

193.31.28.13

Description

ISP: Dominic Scholz trading as ITP-Solutions GmbH & Co. KG **OS:** -
---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCn3ZZPOOZFFO2FU115paW0n6Q2pTmr7dWy00hTFizQP/w3 h+7BLaH5jNtVgc7j0/xzXDinN3K93SYWEvclJdVbI/3Gy30rE2kxpB4fpNVl2eeIV13aQL1SG8VA VuvQo5Jf/UTfMByW5JHG0jGDxp2AAbx2sQNfjfVOnRgSqA0E28nnGyC/6Alrf2SAHsKLqKUD8SD/6Z6YMmIMEuEMacz5mBdzAgJ0mkbUmd60ggNG6AdLCvo8FUQnLEFgtl17pLdvy5i+Jy0vznkGVdUb Aqhf94DFWH8/+tATYkd0zVwOGMvIu7FIQyVTJyT+MO9q9kIIfsTjFXiRY4GQ/QTtihC5 Fingerprint: 9d:2c:e4:b5:e9:04:67:67:20:89:e9:c9:36:ee:a9:a1 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: 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 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/1.1 301 Moved Permanently Server: nginx Date: Tue, 09 Apr 2024 06:20:30 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Location: https://panel.phantopia.net/ ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Cache-Control: no-cache, private Date: Tue, 09 Apr 2024 06:20:31 GMT Set-Cookie: XSRF-TOKEN=eyJpdiI6IlFKUnRhZWxQQVd5Z25DV25ycHRJWVE9PSIsInZhbHVlIjoieUlBTW9JbXI2bEpJYWV4SklhKzVmMGxGOXlqaEQyVE5ZTUp4L2NmeUZVMGpPblVMVTdTSERhN0Q4eEhWZlRCTU5kaFFtUzVEcVhGUXdiMndEM3dKdjN0UzNpRXRrMjNIbFRpTC9uSitBalpUNWNLdnRCeUdFVGd0Rzd3N1dENVoiLCJtYWMiOiIxYjIzOGVjYmRlNDM5YjY1OGUwZGVmNmQ0MDc1MmM5NmM3Y2Y5OTZmOWEyNzdlYTliZjI4NDQwNDNjM2UwN2QwIiwidGFnIjoiIn0%3D; expires=Tue, 09-Apr-2024 18:20:31 GMT; Max-Age=43200; path=/; secure; samesite=lax Set-Cookie: pterodactyl_session=eyJpdiI6IjJ1ZlQ5YVgyT01BVXZadFpCTEFXaUE9PSIsInZhbHVlIjoiWU5OOGJ2QnZncmdYRHZYUm10SG42bkZUNEUxM2NFSWVNeW9CT3FnR2lPdnlvSFVKdG9rdjc2YldiK3A3RUtYbVIvMkpjOFVvZnlHdUUxRlVuaDJCbUZlYitCdVQwV0xlVTdxRWdiTTFyLytXNkNmR1ViTEp1VGNXRFhuUDhsTEkiLCJtYWMiOiJmZjNlMTlmN2E4MWNmNGFiNTAyOTQ1MzgyZmY1MzhhNTdiZTViZjc3YTc0MjBiNjFiMmMxN2MxNGEwOTViMTg3IiwidGFnIjoiIn0%3D; expires=Tue, 09-Apr-2024 18:20:31 GMT; Max-Age=43200; path=/; secure; httponly; samesite=lax X-Content-Type-

Options: nosniff X-XSS-Protection: 1; mode=block X-Robots-Tag: none Content-Security-Policy: frame-ancestors 'self' X-Frame-Options: DENY Referrer-Policy: same-origin ``` HEARTBLEED: 2024/04/09 06:20:35 193.31.28.13:443 - SAFE ------------------ **6080:** ``` ``` ------------------ **25565:** ``` Minecraft Server: Version: Velocity 1.7.2-1.20.1 (Protocol 763) Description: - Online Players: 0 Maximum Players: 50 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.31.28.13']

Name

145.40.126.81

Description

ISP: Packet Host, Inc. **OS:** - ------------------------- Services: **5070:** ``` \x00\x00\x06\x04\x00\x00\x00\x00\x00\x00\x05\x00\x00@\x00 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '145.40.126.81']

Name

103.212.81.116

Description

ISP: Hansin It Services Pvt. Ltd. **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC4bGBqzQOTKAREoDJEvJQ+27vxR7uxIhP+lDvTfnhQAHgk 9lik2ntQVFaGIwOwDPJ04z+jlm7WaddgSwRv6RIo8t02TfxghulLF+xcUwsg3FdtpwmNjt3IuEb9 CEtdxt7xoCPlyie/D5v8dG+ORu5JBBbFdA7y8NgxLO4EgmE7FIgO6tFIIykiwP1cPKBxxhU+0WWK eJQ8Uf9iJy062q8YLVpluf0waDpv6+SplPRmIB5CtrR3g4tr2WaoK6ey9sioOtUlrfh1odfnzlwZ LMEkKfsRDvUuFfHUGC0rNinRuPznKEViMlmUciK7FVsddB6TuYJaXHen62Z7YjRCaqfr Fingerprint: c6:e2:c5:4c:3b:1a:f5:1e:04:3a:bc:79:dc:2e:a9:6b 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 ``` ---------- **3128:** ``` HTTP/1.1 400 Bad Request Server: squid/3.5.20 Mime-Version: 1.0 Date: Sun, 17 Mar 2024 14:44:18 GMT Content-Type: text/html;charset=utf-8 Content-Length: 3538 X-Squid-Error: ERR_INVALID_URL 0 Vary: Accept-Language Content-Language: en X-Cache: MISS from pankaj.racksleaf.com X-Cache-Lookup: NONE from pankaj.racksleaf.com:3128 Via: 1.1 pankaj.racksleaf.com (squid/3.5.20) Connection: close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.212.81.116']

Name

http://45.130.22.219/ivanti.js

Pattern Type

stix

Pattern

[url:value = 'http://45.130.22.219/ivanti.js']

Name

http://137.220.130.2/doc

Pattern Type

stix

Pattern

[url:value = 'http://137.220.130.2/doc']

Name

45.130.22.219

Description

ISP: Owl Limited **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKzQ+9ADktGEpzVKLB3b16xM yewZkva7ZRya62CHUmsTYeVvr3oRF5V49JHxB4gGdAJvHDLFNuEPDCd4hw202rw= Fingerprint: 89:36:ea:e7:d8:ab:ba:2a:9d:a1:50:f0:d9:c3:b5:43 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 ``` ---------- **80:** ``` HTTP/1.1 200 Set-Cookie: JSESSIONID=C6CC80429AB46A1A994EA89239F3AA26; Path=/; HttpOnly Content-Type: text/html;charset=ISO-8859-1 Content-Length: 16 Date: Thu, 01 Feb 2024 03:57:16 GMT ``` ---------- **443:** ``` HTTP/1.1 200 Set-Cookie: JSESSIONID=A84AB67650AFD23C335F0B147EB0B669; Path=/; Secure; HttpOnly Content-Type: text/html;charset=ISO-8859-1 Content-Length: 16 Date: Sun, 04 Feb 2024 09:48:54 GMT ``` HEARTBLEED: 2024/02/04 09:48:58 45.130.22.219:443 - SAFE ---------- **465:** ``` ``` ---------- **995:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.130.22.219']

Name

137.220.130.2

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.220.130.2']

Name

http://103.245.236.188/skyljne.mips

Description

Threat: malware_download - Reporter: tolisec - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://103.245.236.188/skyljne.mips']

Name

176.97.210.211

Description

Agressive IP known malicious on AbuseIPDB - countryCode: RO - abuseConfidenceScore: 100 - lastReportedAt: 2024-02-12T23:03:07+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.97.210.211']

Name

103.131.57.59

Description

Mirai botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.131.57.59']

Name

103.110.33.164

Description

Mirai botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.110.33.164']

Name

45.66.230.32

Description

Mirai botnet C2 server (confidence level: 75%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.66.230.32']

Name

85.208.139.73

Description

Mirai botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.208.139.73']

Name

193.47.61.75

Description

Mirai botnet C2 server (confidence level: 75%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.47.61.75']

Name

146.19.191.85

Description

400 BAD REQUEST

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.19.191.85']

Name

146.19.191.108

Description

400 BAD REQUEST

Pattern Type

stix

Pattern

[ipv4-addr:value = '146.19.191.108']

Name

http://103.131.57.59/mips

Description

Threat: malware_download - Reporter: tolisec - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://103.131.57.59/mips']

Vulnerability

Name

CVE-2024-21893

Description

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure), Ivanti Policy Secure, and Ivanti Neurons contain a server-side request forgery (SSRF) vulnerability in the SAML component that allows an attacker to access certain restricted resources without authentication.

Name

CVE-2024-21887

Description

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure contain a command injection vulnerability in the web components of these products, which can allow an authenticated administrator to send crafted requests to execute code on affected appliances. This vulnerability can be leveraged in conjunction with CVE-2023-46805, an authenticated bypass issue.

Name

CVE-2023-46805

Description

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateways contain an authentication bypass vulnerability in the web component that allows an attacker to access restricted resources by bypassing control checks. This vulnerability can be leveraged in conjunction with CVE-2024-21887, a command injection vulnerability.

Name

CVE-2023-34362

Description

Progress MOVEit Transfer contains a SQL injection vulnerability that could allow an unauthenticated attacker to gain unauthorized access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or delete database elements.

Malware

Name
Mirai

Attack-Pattern

Name

Scanning IP Blocks

ID

T1595.001

Description

Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses. Adversaries may scan IP blocks in order to [Gather Victim Network Information](https://attack.mitre.org/techniques/T1590), such as which IP addresses are actively in use as well as more detailed information about hosts assigned these addresses. Scans may range from simple pings (ICMP requests and responses) to more nuanced scans that may reveal host software/versions via server banners or other network artifacts. (Citation: Botnet Scan) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Name

Tool

ID

T1588.002

Description

Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)). Tool acquisition can involve the procurement of commercial software licenses, including for red teaming tools such as [Cobalt Strike](https://attack.mitre.org/software/S0154). Commercial software may be obtained through purchase, stealing licenses (or licensed copies of the software), or cracking trial versions.(Citation: Recorded Future Beacon 2019) Adversaries may obtain tools to support their operations, including to support execution of post-compromise behaviors. In addition to freely downloading or purchasing software, adversaries may steal software and/or software licenses from third-party entities (including other adversaries).

Name

Vulnerability Scanning

ID

T1595.002

Description

Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use. These scans may also include more broad attempts to [Gather Victim Host Information](https://attack.mitre.org/techniques/T1592) that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.(Citation: OWASP Vuln Scanning) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources

(ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

Name

T1583.001

ID

T1583.001

Description

Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free. Adversaries may use acquired domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries may also use internationalized domain names (IDNs) and different character sets (e.g. Cyrillic, Greek, etc.) to execute "IDN homograph attacks," creating visually similar lookalike domains used to deliver malware to victim machines.(Citation: CISA IDN ST05-016)(Citation: tt_httrack_fake_domains)(Citation: tt_obliqueRAT)(Citation: httrack_unhcr)(Citation: lazgroup_idn_phishing) Adversaries may also acquire and repurpose expired domains, which may be potentially already allowlisted/trusted by defenders based on an existing reputation/history.(Citation: Categorisation_not_boundary)(Citation: Domain_Steal_CC)(Citation: Redirectors_Domain_Fronting)(Citation: bypass_webproxy_filtering) Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

Gather Victim Host Information

ID

T1592

Description

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Hostname

Value
a0f0b2e6.dnslog.store

Url

Value
http://176.97.210.211/mips
http://145.40.126.81/mips
http://103.110.33.164/mips;$
http://45.130.22.219/ivanti.js
http://137.220.130.2/doc
http://103.245.236.188/skyljne.mips
http://103.131.57.59/mips

IPv4-Addr

Value
87.120.88.13
217.114.43.149
185.112.83.15
103.95.196.149
103.245.236.188
103.228.126.17
95.214.27.244
193.31.28.13
145.40.126.81
103.212.81.116
45.130.22.219
137.220.130.2
176.97.210.211

103.131.57.59
103.110.33.164
45.66.230.32
85.208.139.73
193.47.61.75
146.19.191.85
146.19.191.108

StixFile

Value
23190d722ba3fe97d859bd9b086ff33a14ae9aecfc8a2c3427623f93de3d3b14

External References

- https://unit42.paloaltonetworks.com/malware-initiated-scanning-attacks/
- https://otx.alienvault.com/pulse/6615006425ead6665bb99e7d