Jun 19 2023

NETMANAGEIT

Intelligence Report

Mystic Stealer – Evolving “stealth” Malware

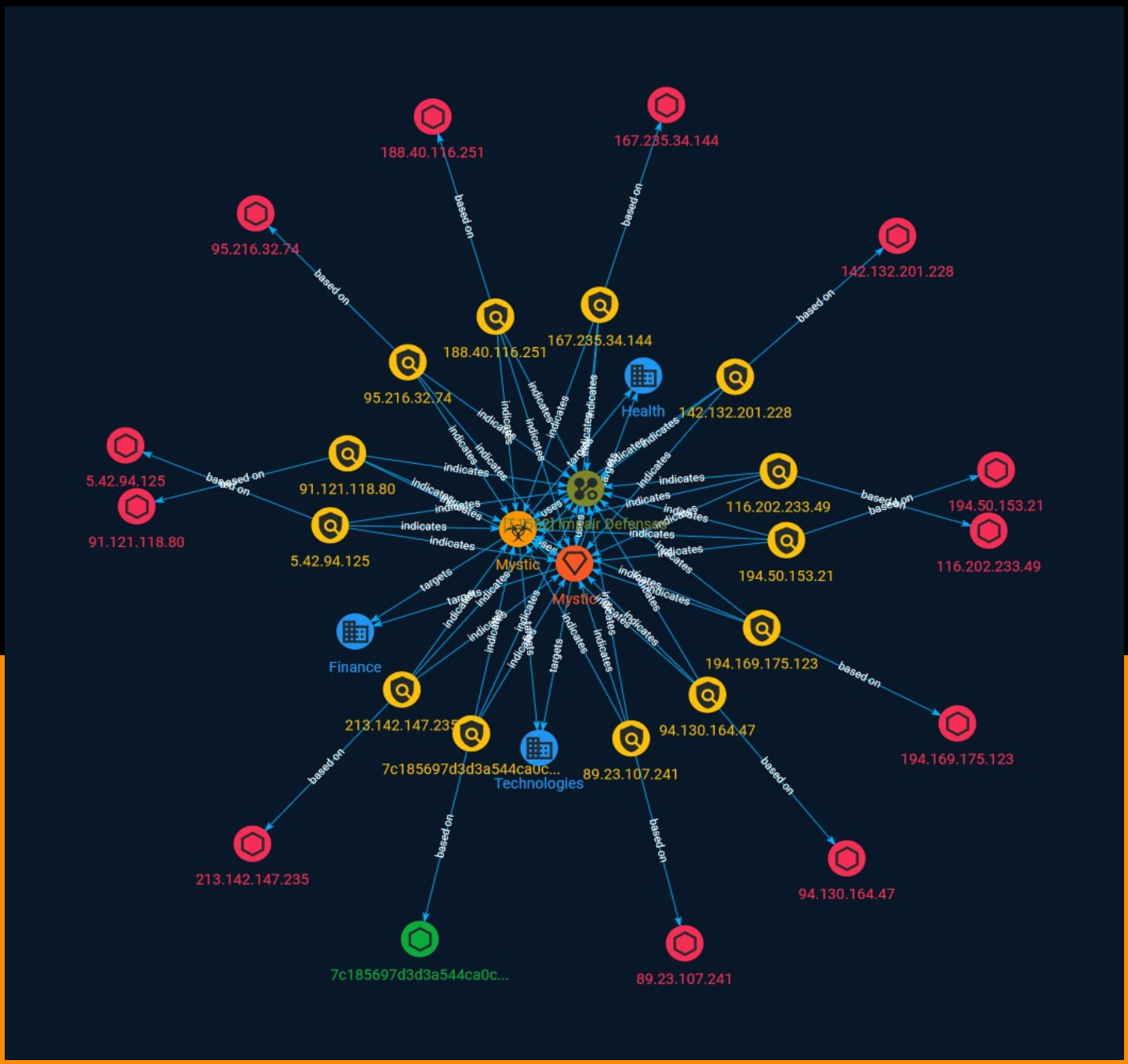

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A report highlights the growing popularity of an information stealer, as well as its ability to evade detection by anti-virus products.

Confidence

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

15 / 100

Attack-Pattern

Name
Impair Defenses
ID
T1562
Description
Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name

5.42.94.125

Description

ISP: AEZA GROUP Ltd **OS:** Ubuntu ---------- Hostnames: - juicy-milk.aeza.network ---------- Domains: - aeza.network ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFf0vXRtnyF2WJX/TeBQVlG3yHYNDJk3sLSuxq0BxJGeZR/G/tHHsxNlbgb+Ltuc4oatXFLEVfw2VsmVSkVND90= Fingerprint: 27:09:7a:68:a7:09:80:77:e2:1f:fc:72:57:88:6a:73 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Sat, 03 Jun 2023 18:36:36 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=GJ1E93IXtUgts7Ft2OSGUqqiWk0HFECjxuuuQg6ZKkhbXFi0k4u2tb35Ck1CBjSJ; expires=Sat, 01 Jun 2024 18:36:36 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.42.94.125']

Name

116.202.233.49

Description

ISP: Hetzner Online GmbH **OS:** Ubuntu ---------- Hostnames: - static.49.233.202.116.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMRIUOX9dOy6Sqr1LOyjkpML 08dEHOxfHw96WcWbi4haPzNvaKjey5lPPQUgHF7qAfHvJUTVs7eLq7V1F7NXshU= Fingerprint: b5:c5:2c:2d:97:04:dc 50:7c:b1:6b:8d:73:1e:3a:04 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Serve nginx/1.18.0 (Ubuntu) Date: Thu, 08 Jun 2023 17:02:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=7gjri7tTQHf9wRQiRCIMmGAWykHHN1gW61KDZYybDBQ11M4MBYVxYT2uruHg6ch2; expires=Thu, 06 Ju 2024 17:02:00 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '116.202.233.49']

Name

89.23.107.241

Description

ISP: GLOBAL INTERNET SOLUTIONS LLC **OS:** None ---------- Hostnames: - zloyarbitrannnnn.ip-ptr.tech - Server.ip-ptr.tech ---------- Domains: - ip-ptr.tech ---------- Services: **21:** ``` 220 ProFTPD Server (Debian) [::ffff:89.23.107.241] 530 Login incorrect. 214-The following commands are recognized (* =>'s unimplemented): 214-CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV 214-EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD 214-XRMD MKD XMKD PWD XPWD SIZE SYST HELP 214-NOOP FEAT OPTS HOST CLNT AUTH CCC* CONF* 214-ENC* MIC* PBSZ PROT TYPE STRU MODE RETR 214-STOR STOU APPE REST ABOR USER PASS ACCT* 214-REIN* LIST NLST STAT SITE MLSD MLST 214 Direct comments to root@zloyarbitrannnnn.ip-ptr.tech 211-Features: 211-AUTH TLS 211-CCC 211-CLNT 211-EPR 211-EPSV 211-HOST 211-LANG en-US.UTF-8*;en-US;ru-RU.UTF-8;ru-RU 211-MDTM 211-MFF modify;UNIX.group;UNIX.mode; 211-MFMT 211-MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.groupname*;UNIX.mode*;UNIX.owner*;UNIX.ownername 211-PBSZ 211-PROT 211-REST STREAM 211-SITE COPY 211-SITE MKDIR 211-SITE RMDIR 211-SITE SYMLINK 211-SITE UTIME 211-SIZE 211-SSCN 211-TVFS 211-UTF8 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGB2hpGxrAJh+CBuT3tNm5DS vGZ5PxUbMT02murO9EJGjyqIbZ6wGmt0WszWJHDXI65acT7BLWZqIdS2NZu4EMQ= Fingerprint: e9:c0:c4:84:c4:19:e4:ac:fc:d2:bc:52:75:96:4c:18 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.o 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Serve nginx/1.18.0 (Ubuntu) Date: Mon, 29 May 2023 02:39:29 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=I3K0jTQVNRMMHur4cDrdVAiUlq124g1beRLi2H5X52tOodboPBtqPiOHTLlGYXJo; expires=Mon, 27 May 2024 02:39:29 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ---------- **587:** ``` 220 zloyarbitrannnnn.ip-ptr.tech ESMTP Exim 4.92 Sun, 18 Jun 2023 23:02:04 +0200 250-zloyarbitrannnnn.ip-ptr.tech Hello 224.212.251.55 [224.212.251.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAI LOGIN CRAM-MD5 250-CHUNKING 250-STARTTLS 250 HELP ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.23.107.241']

Name

95.216.32.74

Description

ISP: Hetzner Online GmbH **OS:** Ubuntu ---------- Hostnames: - static.74.32.216.95.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFdux03G/OQ4+CA9HuvSeZFs Fj1NkqQ/9sDeDWIpid1APIGe46XTvhHPwcbx1aRfdG7niU4rJeyN/PnqGCayGH8= Fingerprint: 66:c5:62:b4:81:db:0c:c7:3f:9d:0f:e5:b1:46:07:e3 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 08 Jun 2023 15:14:34 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=bo0d6RTKt3CF4vxv5B5bbfkMfyW1eUjizXpk3YHnbdidaAhg5JB05xTtI4AbwFtz expires=Thu, 06 Jun 2024 15:14:34 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.216.32.74']

Name

194.50.153.21

Description

ISP: WAICORE TRANSIT **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC5GWLuy2V7NRF+ZHWTDFmRsBijCRFCk3d3CmHqi3dBSke9 9ifXzjSMW9G4TmI0ALMG9m4rxiyg3MZ0531Gzl7ehWJAHteyt9dtqoSBPMxRN9qc/TXix3T+A8zg w0aAJ0RMddHJAXorb2Mqw47heZyqGfldY/3p0QzsnOL1oUdiQTFNdsyU2nad6pA4CNj48WuNKeBq LbuIWuvy8tT48RcQM73kxQdJu+goYGZG+FaV77H29KBQ+8a/+yQlaGTDYzSElp3JgFpxd6oweELZ F3OHDKvbWz9NCkxK8Jl8NRz5rlyynZsTy3obc84syQLzzuFRK2ku1dLCzfFXNdBtr50ibY7ETmhz ungBVlGkO9RkfIRklQBIoJgzGRACFT3eZT+MgYJdsD8OGfOFraSIigNTpfqLp2YRPq7dYuh/+UnX T5Dy/u/yzxHq/ 1dTU7NldLqs2BYT0rJTJuaDHxvp/c7gcnwsHFr1HB5VSGNvc8JBr++k4LRcVUVQ mOVLPoDq8GM= Fingerprint: 89:97:5a:4a:fa:44:d2:5b:b5:c9:17:28:13:d1:f8:ad Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.o 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 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 Date Tue, 13 Jun 2023 13:53:05 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=0VvUoAiyxEpFCvIPiCeC3n0euiGwn5l1Y7ytEmT1FskjrDUdPZG9MDx8lpoIjv64; expires=Tue, 11 Jun 2024 13:53:05 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.50.153.21']

Name

213.142.147.235

Description

ISP: Scalaxy B.V. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 05 Jun 2023 14:39:06 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=67B7S1m4F6mvTWWHJHfFU7PWPXkFWzIuBiA50kqu4sFnmgeB84q118f2ov85o9wG; expires=Mon, 03 Jun 2024 14:39:06 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x01\x08\x00\x01\x00\x00\x00 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.142.147.235']

Name

167.235.34.144

Description

ISP: Hetzner Online GmbH **OS:** Ubuntu ---------- Hostnames: - static.144.34.235.167.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCx8vlqPs0+JLp30Bqj0TMqw T/RuF6xhZL5BMfFMgYMEkuW6C0qxlsBE5j3bfNM2M/Aty8c1E7lxpopOQm0uNqs= Fingerprint: 74:28:93:35:5c:da:d2:52:b4:d9:91:ac:23:34:b1:67 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 29 May 2023 21:16:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=E3BAactOzj3mnRym8igEMlIp8kOKKj1tFJsq44eUn0qpQ2uIAwaFMyW9390T4x8z; expires=Mon, 27 May 2024 21:16:12 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '167.235.34.144']

Name

94.130.164.47

Description

ISP: Hetzner Online GmbH **OS:** Debian ---------- Hostnames: - static.47.164.130.94.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDWvQum0suem1Xl/eskSiY1gHMCfMY8vYHl67rP41Yk8mNX P8khSxVwWK7IAVczQzVr5p72xEfG/6cbNU/1Hbw45srdygUAGEALtJoJdbg6k4GF8SM29NDI59KC b0Rv6VdNdLNQNLogJLSqvN3Oni83zLgbVqyxeQKA4pS1fXzwKnUojTyrgaRZzwWYOYGkENrRFL4e sDhi8CXjduMSwO5Gwh4I+gNroHFp53ZYvdYsrfv54+60GcflzWqvo+jM//2B+ekUPE6NYo6JIBnz ic7Vrt+3vtKlGnRtFWnMFkVmLx5qy7JTDU9keVHPzCEFakE9tftf/bxLkksarPZyLKDKaEkWQ1PP 2HeijMYJej/ 5obknFaJlIzOfAQfdrcwQkXkukXsqkM1ckj33E8bkVw+2i3j8MP2ugUY5KfEfnALX AYtW7MYzGAjpUP+W2DcDsJQ2Xg9hYqcAM/7IOSyTlPO8e3Oi3VfpZZE60y2mxDtVdcPvfq1e0xtN nc0psjPTRPM= Fingerprint: 1c:e8:16:b8:29:f7:d6:60:89:41:97:fc:9b:10:d0:2a 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 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 Date: Wed, 07 Jun 2023 14:32:46 GMT Content-Type: text/html; charset=utf-8 Content-Length: 353 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=DLRTP3HWoxepVg5Cy9cAebVLXe99S55i0DAyBPXofXa0Pco91ZNF8ruvqLD1LUib; expires=Wed, 05 Jun 2024 14:32:46 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.130.164.47']

Name

91.121.118.80

Description

ISP: OVH SAS **OS:** Windows (Build 10.0.18362) ---------- Hostnames: - 1218.rbx.abcvg.ovh ---------- Domains: - abcvg.ovh ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDN4pWw9yKdi8p5/txpF5uq7dDLT9oq7oRY2esuj43eQpcNAeQCWf2ENykSenMVLuLzBz7qgjVQKjvA5AJKBWfU= Fingerprint: a2:d2:d7:37:46:b8:85:8f:84:dd:61:de:1c:20:5c:de 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 ``` ---------- **3389:** ``` Remote Desktop Protocol

\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protoc
NTLM Info: OS: Windows 10/Windows Server (version 1903) OS Build: 10.0.18362 Target Name:
DESKTOP-8JLKMOO NetBIOS Domain Name: DESKTOP-8JLKMOO NetBIOS Computer Name: DESKTOP-8JLKMO
DNS Domain Name: DESKTOP-8JLKMOO FQDN: DESKTOP-8JLKMOO ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.121.118.80']

Name

142.132.201.228

Description

ISP: Hetzner Online GmbH **OS:** Ubuntu ---------- Hostnames: - static.
228.201.132.142.clients.your-server.de ---------- Domains: - your-server.de
---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha
nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEnUierWp81HXjgJCApOvhG6
ff4D1/j2IpYp1GhAF1NqwaXjl8Y8hA3T9RiPv+j+gnCjBbw8ZIvcGx20dcOEunE= Fingerprint: 4e:fd:4f:ac:86:fc:07:30:d
77:0e:df:82:9d:22:d6 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0
(Ubuntu) Date: Sun, 28 May 2023 05:22:14 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539
Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy
same-origin Set-Cookie:
csrftoken=RBoot9ozvqshg8fCu4NZ3EF5iMVuBRsPhtnTP3Q4WP18NJO6dsguKplb03o6zYqt; expires=Sun, 26 May
2024 05:22:14 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '142.132.201.228']

Name

7c185697d3d3a544ca0cef987c27e46b20997c7ef69959c720a8d2e8a03cd5dc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c185697d3d3a544ca0cef987c27e46b20997c7ef69959c720a8d2e8a03cd5dc']

Name

188.40.116.251

Description

ISP: Hetzner Online GmbH **OS:** Ubuntu ---------- Hostnames: - static.251.116.40.188.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFCiHkocLkRfZbz+B5Dttrtt ABxO8xSPjWBvcAf00+X/IKRXbMOCceZL/cqzPWBrdVB+4tKLH10scSws9fS1Pc8= Fingerprint: b5:36:9c:21:90:8e:9a 83:98:78:1c:95:52:ed:ff:ea 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Sat, 17 Jun 2023 21:39:43 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=YE0T5fJLGX83RfbvFzUjyqTZGUJZT1478yUHhkvbU2PmgO0wRrJPnAMmOYiLxZ3c; expires=Sat, 15 Jun 2024 21:39:43 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '188.40.116.251']

Name

194.169.175.123

Description

ISP: Suisse Limited **OS:** Windows (build 6.3.9600) ---------- Hostnames: - net-194-169-175-123.cust.as211760.net ---------- Domains: - as211760.net ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 01 Jun 2023 21:02:04 GMT Content-Type: text/html; charset=utf-8 Content-Length: 3539 Connection: keep-alive X-Frame-Options: DENY Vary: Cookie X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=uoPkZ2S1tgy35qk3jVklZpxM3FtL7teJAAI5iETV9tZZRphuL5LHi7vEPV127zhV; expires=Thu, 30 May 2024 21:02:04 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-MEPBBP9GUV7 NetBIOS Domain Name: WIN-MEPBBP9GUV7 NetBIOS Computer Name: WIN-MEPBBP9GUV7 DNS Domain Name: WIN-MEPBBP9GUV7 FQDN: WIN-MEPBBP9GUV7 ``` ----------

Pattern Type

stix

Pattern
[ipv4-addr:value = '194.169.175.123']

Intrusion-Set

Name
Mystic

Malware

Name
Mystic

StixFile

Value
7c185697d3d3a544ca0cef987c27e46b20997c7ef69959c720a8d2e8a03cd5dc

IPv4-Addr

Value
142.132.201.228
89.23.107.241
95.216.32.74
194.50.153.21
91.121.118.80
5.42.94.125
94.130.164.47
116.202.233.49
194.169.175.123
213.142.147.235
188.40.116.251
167.235.34.144

External References

- https://otx.alienvault.com/pulse/649071937d0f8a435b37fafc
- https://www.cyfirma.com/outofband/mystic-stealer-evolving-stealth-malware/