Jul 06 2023

NETMANAGEIT

Intelligence Report

Unleashing the Viper : A Technical Analysis of WhiteSnake Stealer

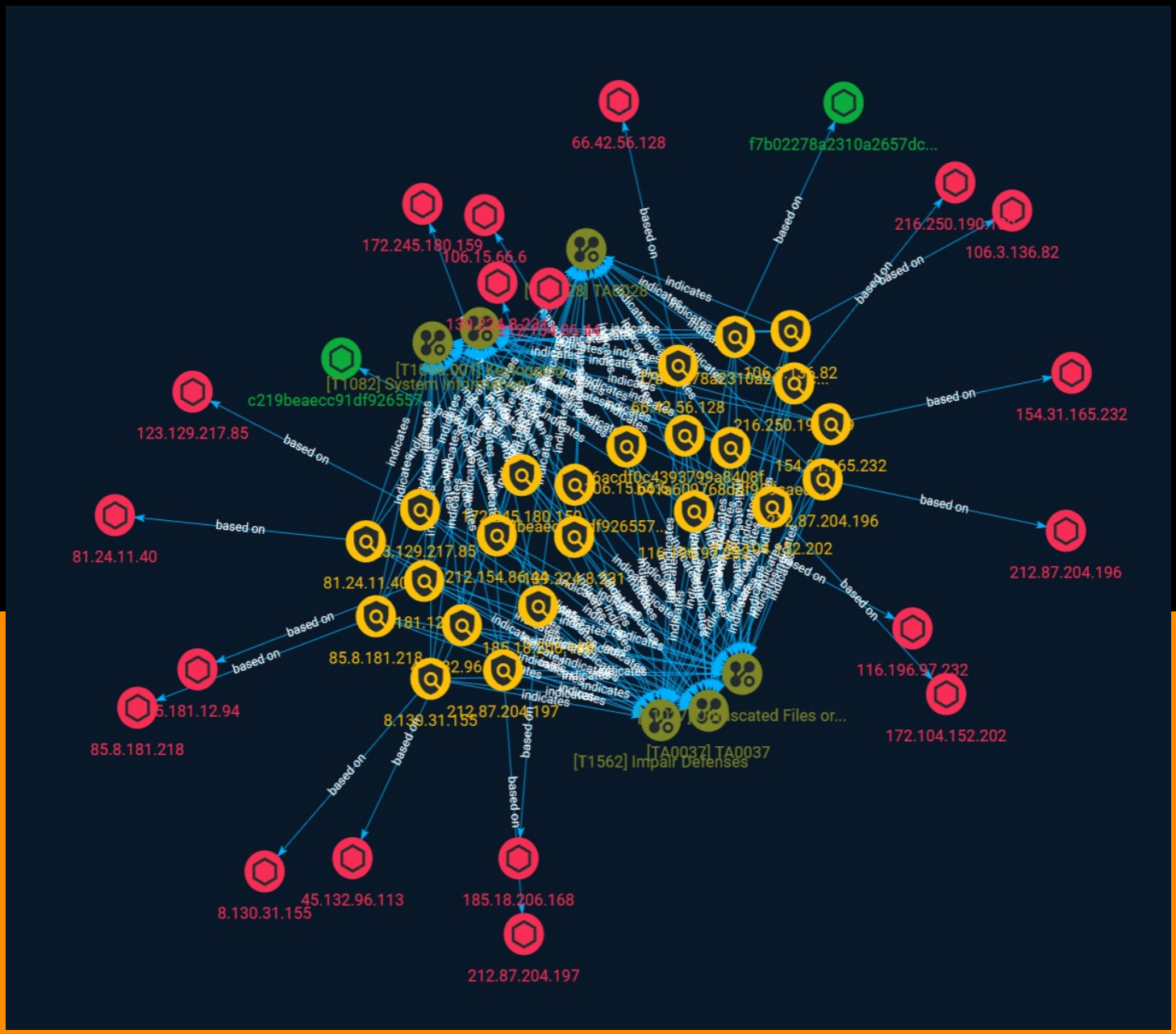

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The stealer collects data from various browsers such as Firefox, Chrome, Chromium, Edge, Brave, Vivaldi, CocCoc, and CentBrowser. Besides browsing data, it also collects data from Thunderbird, OBS-Studio, FileZilla, Snowflake-SSH, Steam, Signal, Telegram, Discord, Pidgin, Authy, WinAuth, Outlook, Foxmail, The Bat!, CoreFTP, WinSCP, AzireVPN, WindscribeVPN.

Confidence

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

15 / 100

Indicator

Name
f7b02278a2310a2657dcca702188af461ce8450dc0c5bced802773ca8eab6f50
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f7b02278a2310a2657dcca702188af461ce8450dc0c5bced802773ca8eab6f50']
Name
116.196.97.232
Description
ISP: Beijing Jingdong 360 Degree E-commerce Co., Ltd. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Server: nginx/1.16.1 Date: Wed, 05 Jul 2023 16:30:49 GMT Content-Type: text/html Content-Length: 555 Connection: keep-alive ``` ---------- **8080:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server 1.0 X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Mon, 03 Jul 2023 11:04:16 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '116.196.97.232']

Name

66.42.56.128

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 66.42.56.128.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC3Ixna4+gHZwgXh23dfLg32W0pmmA9iTKo8ZEZYT1IMn rn YSs6OgwqBrTga7h8pQ0L78Tf5JRQQhMHw7MK3aKzaAaxC46K53vsUnHjSkL/ priDfLN8yO5Z7qkk 9UdUS0vA7PqSHtGBvE9bRAXczA3ZFgO2i+GDmLSzlCJRPcebI+ltLHGZBW5Nxe2O2ZPYn0IodTNB u1TJtRD7EglIDCX0qdJ7sFLw43WHkld0gNqvCcmuM31boxrdzf3+3sx/pY9FO8rHvL5SvMtlm3f4 Gic0bBerQapdLB7QYnMXl+4QjYaqcJ3ZQ6oAaVPTYeUJWVBtdyv2DGKjpVSWa7WgnXAL Fingerprint: 80:11:62:7b:aa:5e:09:24:9b:79:52:ea:85:70:b3:f6 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Wed, 05 Jul 2023 22:33:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ---------- **2222:** ``` HTTP/1.1 200 OK Cache-Control: no-cache, no-store, must-revalidate Content-Type: text/html; charset=utf-8 X-Xss-Protection: 1; mode=block Date: Thu, 22 Jun 2023

19:48:15 GMT Transfer-Encoding: chunked ``` ---------- **8080:** ``` HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Mon, 03 Jul 2023 07:43:40 GMT Content-Type: text/html Content-Length: 12 Last-Modified: Fri, 18 Nov 2022 11:17:22 GMT Connection: keep-alive ETag: "637769c2-c" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '66.42.56.128']

Name

c219beaecc91df9265574eea6e9d866c224549b7f41cdda7e85015f4ae99b7c7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c219beaecc91df9265574eea6e9d866c224549b7f41cdda7e85015f4ae99b7c7']

Name

5.181.12.94

Description

ISP: CreeperHost LTD **OS:** None ---------- Hostnames: - 94.12.181.5.no-ptr.as201971.net ---------- Domains: - as201971.net ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server 1.0 X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Thu, 06 Jul 2023 07:02:58 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.181.12.94']

Name

172.104.152.202

Description

ISP: Akamai Connected Cloud **OS:** Ubuntu ---------- Hostnames: - li1668-202.members.linode.com ---------- Domains: - linode.com ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.12.1 (Ubuntu) Date: Wed, 05 Jul 2023 23:09:28 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Wed, 21 Nov 2018 22:52:11 GMT Connection: keep-alive ETag: "5bf5e19b-264" Accept-Ranges: bytes ``` ---------- **8080:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server 1.0 X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Sun, 02 Jul 2023 16:37:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.104.152.202']

Name

139.224.8.231

Description

ISP: Hangzhou Alibaba Advertising Co.,Ltd. **OS:** Ubuntu ---------- Hostnames: - bayern.detie.cn ---------- Domains: - detie.cn ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDesaFjgw84IzPoBuepyWRQTe3YF+bycBoUl7kBPM1uBIGH ZekO6mnKryZuNUYbtUDrRUFK8urN3pS2EB3B5pE4Ss3YthktB6BF9QwU4rDNbYIV8Hk+lurYSCCjxGYboseN/iY1d4BWXz/ZL8B1VGM5UexDYjA8vsmcoCGDEpUyDTw6bKj732Ez2TgJPVe2boiia5L9CtjZoeK5DMCoRpN1NjDvli7tPsS7wi4eReRudIPapvyOZc/mEaIcal3YZO5xcjHcwsDACTDbTEDglMtLe3x+ZYgWqKYi53vpKMY1tohk8P6BV/UxNqXGk8lVm9/LLIlOv2/whQrMY/j4slqT Fingerprint: 0d:a7:9c:5c:7f:6d:0a:08:f3:40:53:8a:15:e0:a1:08 Kex Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com chacha20-poly1305@openssh.com blowfish-cbc aes128-cbc 3des-cbc cast128-cbc arcfour aes192-cbc aes256-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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.10.3 (Ubuntu) Date: Sun, 02 Jul 2023 23:14:00 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Tue, 06 Mar 2018 15:25:44 GMT Connection: keep-alive ETag: "5a9eb2f8-264" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx/1.10.3 (Ubuntu) Date: Thu, 06 Jul 2023 01:48:50 GMT Content-Type: text/html; charset=utf-8 Content-Length: 5592 Connection: keep-alive Status: 404 Not Found X-Request-Id: 64a61d82_CS-000-01Omz43_5160-47511 X-Runtime: 0.211723 X-Via: 1.1 PS-TSN-01VPj38:1 (Cdn Cache Server V2.0), 1.1 CS-000-01Omz43:9 (Cdn Cache Server V2.0) X-Ws-Request-Id: 64a61d82_CS-000-01Omz43_5160-47511 ``` HEARTBLEED: 2023/07/06 01:49:14 139.224.8.231:443 - SAFE ---------- **3128:** ``` HTTP/1.1 400 Bad Request Server: squid/3.5.12 Mime-Version: 1.0 Date: Sun, 02 Jul 2023 21:18:08 GMT Content-Type: text/html;charset=utf-8 Content-Length: 3554 X-Squid-Error: ERR_INVALID_URL 0 Vary: Accept-Language Content-Language: en X-Cache: MISS from iZuf61q38vbvbbv2tmwuccZ X-Cache-Lookup: NONE from iZuf61q38vbvbbv2tmwuccZ:3128 Via: 1.1 iZuf61q38vbvbbv2tmwuccZ (squid/3.5.12) Connection: close ``` ---------- **8080:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server 1.0 X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Fri, 30 Jun 2023 04:25:58 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.224.8.231']

Name

123.129.217.85

Description

ISP: CHINA UNICOM China169 Backbone **OS:** None ---------- Hostnames: - git.vpsv.cn ---------- Domains: - vpsv.cn ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.6 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDIEuGy8DqC6HQU5/k/NF+Z28dz7gIOIlZZjm2q5TIuY+NKqRP/vy+o1qxck75oO9oX/+TFxpR8zm2rGNFTLozJcoBBvP6Wd3HFQN1p1nuS5Z1SjLT/5k/FZa8LKT8frvGhfqurMWRHALZswqRhXNYz7L39Zs52QWnJlCKHCYo5sLFRxKgOj5rtAVJNi2oA66cw+vUMJwSIMRhfuQ0fg1XJGG5c2nL+ITWsqxbfTbWx0W8DBjg+AIRv2yqkLU2TwrISXvJ2jx3wx20B2gDO+b2dKEMsLY0N4LBim7XWx3q+iCGZFnrBAMcCmT4DxA6OoEpWqvWYc7ATV7MEEyRlktDwN8UzuFUU qc9lN3Yw6XuafBYh5HKa2XF0OweNW2k/WTWEXfy5otyMBo22cd6LnWJdreKgXII8p+6uxVsf3Py2LWhh05Od9lyrnmKpeixtc3prpy3mBOreObEfr6ovEtjjX5D5PvIOnpxbfbh+g4C5SCD9GQoQpKCl1XS5aCMWt1s= Fingerprint: 52:76:1b:fd:aa:9d:62:d1:08:ff:ea:00:73:eb:16:3e 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 Date: Wed, 05 Jul 2023 12:02:47 GMT Content-Type: text/html Content-Length: 138 Last-Modified: Thu, 17 Nov 2022 18:51:13 GMT Connection: keep-alive ETag: "637682a1-8a" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Mon, 03 Jul 2023 09:56:45 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked

Connection: keep-alive Vary: Accept-Encoding Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647 Set-Cookie: i_like_gogs=593f83d36cde3046; Path=/; HttpOnly Set-Cookie: _csrf=eiUsDnxUtLA88I2r5LsKNYt7ugA6MTY4ODM3ODIwNTk1NzU2NTgxNg; Path=/; Domain=123.129.217.85; Expires=Tue, 04 Jul 2023 09:56:45 GMT; HttpOnly X-Content-Type-Options: nosniff X-Frame-Options: deny Cache-Control: no-cache ``` HEARTBLEED: 2023/07/03 09:57:04 123.129.217.85:443 - SAFE ---------- **3001:** ``` HTTP/1.1 200 OK Cache-Control: no-store, no-transform Content-Type: text/html; charset=UTF-8 Set-Cookie: i_like_gitea=4bc9a397649d8ee7; Path=/; HttpOnly; SameSite=Lax Set-Cookie: _csrf=V8AVYy1WDDlQhL_1YtVDXp8i-WM6MTY4ODM3NTE2NTY2MTM5NDk1MQ; Path=/; Expires=Tue, 04 Jul 2023 09:06:05 GMT; HttpOnly; SameSite=Lax Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN Date: Mon, 03 Jul 2023 09:06:05 GMT Transfer-Encoding: chunked 33bb
This website works better with JavaScript.
Logo
Explore Help
Sign In

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.154.86.44']

Name

6acdf0c4393799a8408ffc4d6bc377c8a14f4faf

Description

Detects WhiteSnake Stealer XOR version

Pattern Type

yara

Pattern

rule WhiteSnakeStealer { meta: author = "RussianPanda" description = "Detects WhiteSnake Stealer XOR version" date = "7/5/2023" strings: $s1 = {FE 0C 00 00 FE 09 00 00 FE 0C 02 00 6F ?? 00 00 0A FE 0C 03 00 61 D1 FE 0E 04 00 FE} $s2 = {61 6e 61 6c 2e 6a 70 67} condition: all of ($s*) and filesize < 600KB }

Name

106.15.66.6

Description

ISP: Hangzhou Alibaba Advertising Co.,Ltd. **OS:** None ---------- Hostnames: - rancher-staging.yealinkops.com ---------- Domains: - yealinkops.com ---------- Services: **443:** ``` HTTP/1.1 200 OK Accept-Ranges: bytes Cache-Control: no-cache, no-store, must-revalidate Content-Length: 1735 Content-Type: text/html; charset=utf-8 Last-Modified: Mon, 29 Aug 2022 22:32:06 GMT X-Api-Cattle-Auth: false X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Date: Thu, 06 Jul 2023 15:33:44 GMT ``` HEARTBLEED: 2023/07/06 15:34:45 106.15.66.6:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '106.15.66.6']

Name

172.245.180.159

Description

ISP: ColoCrossing **OS:** None ---------- Hostnames: - 172-245-180-159-host.colocrossing.com - www.certinstall.top ---------- Domains: - certinstall.top - colocrossing.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCqRuFGLOjTmQWU6ESA901dcBGXE2oY0VhVtxM013YVU52N XzowY5YZcIejJgdRzm/ZEBVMwBdjVbIwlsi0mdl2eWhNZcXe/mnr4wMVCl1kUh2dwRMt4OwcqoaE gsXMdJX1+80a3KRqD+Maxa+ooAVHPHAri8mN8kjZRASOTBDwrbDuQPY7mggwutgm3pZ1zIAkB Rht c6nqey3+v6cz3nltvOOvTGyHDVYrpvOfiqwKJriZHIUP84ucGeeBB/zcOaGKMhBDOz/vYpLNKcEH 8PmdBAW8sxeVYqmqcYoXsqTgvP2jGDoGdspvHNQ3AGGp2xywDQLyfoplm0S8wiQyZc+X20HIH ifv QKZEOrKD/2ytNTkMmAo9H/riRuRMLkSr0WqwxKoKDRdPnWyHc4RTp0XqHEOjIVgtO0DMqETM1wQW 2Xo2lDGuOyufCkvvHo5pAPU5SAGmB4PUi0mzY6Ds7Bqo36Cg7XrZmPoeJV5irMctviXIsLcH4q3K yaMDD9CqrQ8= Fingerprint: c4:59:ca:b6:27:3d:aa:d6:bf:20:7f:e0:56:96:34:d2 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 ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Date: Mon, 26 Jun 2023 07:56:24 GMT Server: Apache Location: https://172.245.180.159/ Content-Length: 297 Connection: close Content-Type: text/html; charset=iso-8859-1 ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Wed, 05 Jul 2023 21:24:24 GMT Server: Apache Upgrade: h2 Connection: Upgrade, close Last-Modified: Wed, 29 Mar 2023 08:17:08 GMT ETag: "543-5f8059a2cbf9b" Accept-Ranges: bytes Content-Length: 1347 Vary: Accept-Encoding Content-Type: text/html ``` HEARTBLEED: 2023/07/05 21:24:48 172.245.180.159:443 - SAFE ---------- **888:** ``` HTTP/1.1 403

Forbidden Date: Mon, 03 Jul 2023 22:21:07 GMT Server: Apache Content-Length: 264 Connection: close Content-Type: text/html; charset=iso-8859-1 ``` ---------- **8080:** ``` HTTP/1.1 200 OK Content-Length: 3617 Content-Type: text/html; charset=utf-8 Server: beegoServer:1.12.0 Set-Cookie: beegosessionID=f4a72670b1e7df5a7bce661693545dfb; Path=/; HttpOnly Date: Mon, 03 Jul 2023 19:32:35 GMT ``` ---------- **8099:** ``` HTTP/1.1 404 Not Found ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.245.180.159']

Name

216.250.190.139

Description

ISP: ipHouse **OS:** None ---------- Hostnames: - quark.iphouse.net - mirrors.iphouse.net ---------- Domains: - iphouse.net ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Sat, 01 Jul 2023 07:26:17 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ---------- **123:** ``` NTP protocolversion: 3 stratum: 0 leap: 3 precision: 0 rootdelay: 0.0 rootdisp: 0.0 refid: 1380013125 reftime: 0.0 poll: 3 ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 29 Jun 2023 15:36:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Strict-Transport-Security: max-age=63072000 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Referrer-Policy: strict-origin-when-cross-origin Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none' Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=(), interest-cohort=() Content-Security-Policy: default-src 'self' *.iphouse.net *.bootstrapcdn.com *.cloudflare.com ``` HEARTBLEED: 2023/06/29 15:36:12 216.250.190.139:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '216.250.190.139']

Name

85.8.181.218

Description

ISP: rainbow network limited **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHc/K31RJzed3hiRpJ6CxMRd1h3grHYyou4tyOHBs70OGyJih0gR3oXBpNl83uCTVBNNbnzBnE+8OOSbBU19b18= Fingerprint: c3:7a:64:af:e9:b6:66:b4:23:ae:f6:a1:80:bc:e8:c2 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: Transfer.sh HTTP Server Vary: Accept X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Mon, 19 Jun 2023 11:50:22 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ---------- **8080:** ``` HTTP/1.1 200 OK Cache-Control: no-cache, no-store, must-revalidate Content-Type: text/html; charset=utf-8 X-Xss-Protection: 1; mode=block Date: Sun, 02 Jul 2023 11:13:51 GMT Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.8.181.218']

Name

106.3.136.82

Description

ISP: China Mobile Communicaitons Corporation **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Wed, 28 Jun 2023 15:35:44 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '106.3.136.82']

Name

185.18.206.168

Description

ISP: Interhost Communication Solutions Ltd. **OS:** None ---------- Hostnames: - 168.206.interhost.net ---------- Domains: - interhost.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCpXZIuUlH878VUXLKwLWrmViJcspARzGBGJNOPIdvgRT CB oi8+axTgD7YfecRAM43NN7PfZvoovMCXO2ExjBQgHkzL6qIfgAPSS94DIQ1Ljl8EWj7IwwkR2w0+ TtViFkbgizFC5GeCuGpB/h9Ebl1pPMRW5JKSefVZeNzAAjxSLlNZyUmKs2cmvxvPgmVLk5ur1x2e

RN90PFOquFK7xFeiBQcO1V/o8jkWvVIW5Iwg76nyvv4H91AuXK5pgvmzKcPMDq3RTbgXeN+/2Njh M5801qy32JteQ7RWIIr8KQNgmo9LAQ0WY/P+n6CT/AYvyDq+Pl0KNw2gGySJ9FzdKXUDuizr+bsZ oPbIp8L54XrMWgfFc5nru3c5pti67PdRVbM0fPYONC/ Eb48GWGZw4R5UL2mKaba0WWF98cq7unBv vgcZAwMfk89enTfJTILe0c2OGC9nlGCjm6R+0DPM6cOhDtT8iFLVtoy6TlEcRMopjgQez7mS+Qno sGqTgEP1tX0= Fingerprint: fa:3a:6d:d7:90:78:28:c8:c6:60:a7:0b:aa:23:93:78 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 ``` ---------- **8080:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server Vary: Accept X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Wed, 05 Jul 2023 08:28:32 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.18.206.168']

Name

45.132.96.113

Description

ISP: FEELB SARL **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGsq0cRrXfFEbq2TzFNHzLwz EV1rhk9KjXDDXrLeF34EtYerpafUs2GXwFkipb25tiyhKBgbURsRrZOIjd1zry8= Fingerprint: ed:ab:a5:23:21:74:c9:9e:07:31:bb:21:5c:b1:18:df 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: Transfer.sh HTTP Server X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Tue, 20 Jun 2023 10:17:56 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.132.96.113']

Name

b41a609768ddf959cae8951c7ae04a8e198b60d2

Description

detects WhiteSnake Stealer RC4 version

Pattern Type

yara

Pattern

rule WhiteSnakeStealer { meta: author = "RussianPanda" description = "detects WhiteSnake Stealer RC4 version" date = "7/5/2023" strings: $s1 = {73 68 69 74 2e 6a 70 67} $s2 = {FE 0C ??

00 20 00 01 00 00 3F ?? FF FF FF 20 00 00 00 00 FE 0E ?? 00 38 ?? 00 00 00 FE 0C} $s3 = "qemu" wide $s4 = "vbox" wide condition: all of ($s*) and filesize < 300KB }

Name

212.87.204.197

Description

ISP: Delis LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Content-Security-Policy: default-src 'none' X-Content-Type-Options: nosniff Content-Type: text/html; charset=utf-8 Content-Length: 139 Set-Cookie: connect.sid=s%3AH11uW6RFZeN3FJnJzPtgchxmdRubPZuB.C3ZkFXF%2FD3qMbnJmbSt7ZMfZnzl9BFxcobIq4oyiESQ; Path=/; HttpOnly Date: Sat, 01 Jul 2023 03:57:12 GMT Connection: keep-alive Keep-Alive: timeout=5 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.87.204.197']

Name

81.24.11.40

Description

ISP: Cyso Group B.V. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **4000:** ``` HTTP/1.1 400 Bad Request Connection: close ``` ---------- **8080:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server Vary: Accept X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Mon, 03 Jul 2023 14:33:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '81.24.11.40']

Name

154.31.165.232

Description

ISP: STARCLOUD GLOBAL PTE., LTD. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCjOe48mzMFqM83ohKN4tHoDmmBZfhe1RkHLD53WGqD2Nr3 LXfArwmVUKuN6k5asGx8uw7O+q1CGbIR09vbH3TjFMmyfOLzIGPTDtXF6fixs9Qhc0qs/YA94iH8 5S32w7qVc9kYPCbDSKSLOLziHJQ1JeQzYAbifUUsGl5oYsb92dJBsCQuC4Fs+ukMGc2efmGrnV0z ebl81R7KfCnrKYti0aWejOKO+MFWt+05CM2NbW6NU7JO46jWA9DjM3gYB+KLJ+qUIqUjIb6jhEi5 Ps8ZVrnqkn9XFdyR9bgj5crhvmDPjXIOtWyt3VOcuECAqDjKLWg4Cg8Ku74k8Ssg6SD7 Fingerprint: 74:7e:2a:31:63:15:76:8f:18:48:14:b4:db:12:b9:a6 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Mon, 03 Jul 2023 11:17:12 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ---------- **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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.31.165.232']

Name

8.130.31.155

Description

ISP: Hangzhou Alibaba Advertising Co.,Ltd. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Sun, 02 Jul 2023 00:48:08 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ---------- **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 ``` ----------

Pattern Type

stix

Pattern

```
[ipv4-addr:value = '8.130.31.155']
```

Attack-Pattern

Name
TA0028
ID
TA0028
Name
TA0037
ID
TA0037

StixFile

Value
c219beaecc91df9265574eea6e9d866c224549b7f41cdda7e85015f4ae99b7c7
f7b02278a2310a2657dcca702188af461ce8450dc0c5bced802773ca8eab6f50

IPv4-Addr

Value
212.87.204.197
185.18.206.168
123.129.217.85
106.3.136.82
172.104.152.202
154.31.165.232
116.196.97.232
66.42.56.128
212.154.86.44
212.87.204.196
106.15.66.6
45.132.96.113
81.24.11.40

139.224.8.231
8.130.31.155
85.8.181.218
172.245.180.159
5.181.12.94
216.250.190.139

External References

- https://otx.alienvault.com/pulse/64a719c5406fa509bd3b3e38
- https://russianpanda.com/2023/07/04/WhiteSnake-Stealer-Malware-Analysis/