Jul 19 2023

NETMANAGEIT

Intelligence Report

Ursnif campaign in Italy

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An investigation by Kostas from the DFIR Report covering an Ursnif campaign in Italy.

Confidence

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

15 / 100

Indicator

Name

109.105.198.129

Description

ISP: combahton GmbH **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDnzalSIBNrAX06mqQSl/8zW7fMw5JtNJO2rbb5nDVaCWHh DUPB46/g+9o9ELo+t1I36JpMiu/KvS73qKasuGEm5E/6ljMNarKaGbEqjuJC90CEpSsJYrIOzk5l l2j2ROFYlV+hqXO7h7b8ROm86JCCfucLIEhRfz1QIM2DyMbyre6kzKDrlj9hq2kK5YwDn/Dnru/0 SAbr8Knql8ykXWVxJbcvd9ogEtj3st21QRgOaWlgVYNOa7OnDkXQrGAq69uDOQIug90PaqG2Jcgs u2dwdK4/dbk11lHXKJDh1LiAGi4CyMR76jK7XLWdHKI4KxP87R46IrN8+HVBDZbSfOEx Fingerprint: 3c:ed:9a:83:d2:2c:ad:cf:a9:22:dd:e2:62:c2:15:67 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/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Sun, 09 Jul 2023 18:32:15 GMT Content-Type: text/html; charset=utf-8 Content-Length: 548 Connection: keep-alive Vary: Accept-Encoding ``` ---------- **443:** ``` ``` HEARTBLEED: 2023/07/10 15:08:55 109.105.198.129:443 - SAFE ---------- **3000:** ``` HTTP/1.1 200 OK X-Powered-By: Express Access-Control-Allow-Origin: * Accept-Ranges: bytes Cache-Control: public, max-age=0 Last-Modified: Fri, 23 Jun 2023 00:20:21 GMT ETag: W/"818-188e59f9588" Content-Type: text/html; charset=UTF-8

Content-Length: 2072 Date: Fri, 30 Jun 2023 18:54:42 GMT Connection: keep-alive Keep-Alive: timeout=5 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.105.198.129']

Name

http://delideta.com/pictures/

Pattern Type

stix

Pattern

[url:value = 'http://delideta.com/pictures/']

Name

185.82.127.183

Description

ISP: Sia Nano IT **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCxAan5dUYsRh90lV6IVufLvaun2dViKBgHGX/59NhSO4/r9zJR8Q1VBhB3lPNwHpArcsss5ra4XHdCR0+9AEiu9nnosT82eUDdhMzswkb6168IiMMLsMzi0ch7kffGt8oZyNFhNS/jMreElVhJdmkSGVP7WnxxQW0f5vk5bG055Wv+5D0u/besKkEeWoOt0pVeyB/yeSPon/J9wSOTqEa9sAaqD3BvAYy3k3GNj5zKWVRI79LEU+pw5vigrMz679PjPlsYdg/Tc2PpoxzhVC3SK9kA/eeCZQaO0U6D2/gP7HDVFUdy07j1WxPX2YTeLldzvgupMgQ9PzGbfrzijBdd

Fingerprint: 02:16:7c:c5:26:53:2a:a9:90:62:a2:99:80:d0:98:5c 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/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Thu, 13 Jul 2023 08:47:03 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Tue, 04 Jul 2023 19:46:40 GMT Connection: keep-alive ETag: "64a47720-264" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.82.127.183']

Name

http://109.105.198.129/pictures/...

Pattern Type

stix

Pattern

[url:value = 'http://109.105.198.129/pictures/...']

Name

31.172.83.49

Description

ISP: firstcolo GmbH **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **443:** ``` ``` HEARTBLEED: 2023/07/18 16:07:22 31.172.83.49:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.172.83.49']

Name

173.44.141.199

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.44.141.199']

Name

91.201.65.64

Description

ISP: Melbikomas UAB **OS:** None ---------- Hostnames: - vm634652.melbi.space ---------- Domains: - melbi.space

---------- Services: **3306:** ``` MySQL: Protocol Version: 10 Version: 5.7.17-log Capabilities: 63487 Server Language: 33 Server Status: 2 Extended Server Capabilities: 33279 Authentication Plugin: mysql_native_password ``` ---------- **3401:** ``` RFB 003.008 Authentication disabled EY Barbara Microsoft Edge ae Questo PC Panda Dome a) VLC media player a Cestino FattureElett... na PDF Pannello di SCAD.MA... controllo E NERI a Adobe Acrobat rd CCleaner A EaseUS Todo Backup Free Lo Firefox VNC: Protocol Version: 3.8 Security Types: 1: None Geometry: 1920x1080 ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Fri, 14 Jul 2023 15:31:17 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows 10/Windows Server 2019 OS Build: 10.0.17763 Target Name: WIN-LIVFRVQFMKO NetBIOS Domain Name: WIN-LIVFRVQFMKO NetBIOS Computer Name: WIN-LIVFRVQFMKO DNS Domain Name: WIN-LIVFRVQFMKO FQDN: WIN-LIVFRVQFMKO ``` ---------- **8841:** ``` RFB 003.008 Authentication disabled VNC: Protocol Version: 3.8 Security Types: 1: None ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.201.65.64']

Name

http://avas1t.de/in/loginq/

Pattern Type

stix

Pattern

[url:value = 'http://avas1t.de/in/loginq/']

Name

152.89.198.29

Description

ISP: Chang Way Technologies Co. Limited **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQClwrEdqy+UcbYV633HHJI+C+1HTTyQZXhIcHjHh/OAuT93 fEa3kzPF11kFObaAxgJMBDhbN5vMd9VQOVWNGr1lAP13o/sDNDj672/KCKrOousN6dCIREjE6/RT /tPosCp5hEkVl2kjO4HWX9O0GNrSLE8UF4N5zY/IIJjGzExyrf5TvvYuesDiqgAALgt2TEaR1hCF onMf/zFUg1kSOsJK/O0VcWYxuSfWK2JYrpR7pPvFL2u4firWR7xNhBp4vu3YM26cK0fFEFIlzfj2 IYo32S/YDeDGHkSCUc6J+R+csXS13WoDPKxaYNsEgLfSHiEFz18H1zc9wbyDKKzg/ZL7iD6iNF41 WnCLNMXF7CVrgn41QzRYuY/+CqcYYI8Th1SOCs7wpwdqs1wniGs6lZDFvw3Z8bBo+uALYTd3f/2T FuBoY13QZmQhNdTf0Zb8mxPor2yhHCotvAMG9XHrxcqaVhT1U1ULDC4vA7Alx8PimRRY2QDQD1 JK zCTKADXVPMU= Fingerprint: 75:d3:e6:81:aa:27:2d:36:20:7d:34:07:3e:ad:41:18 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/1.1 404 Not Found Date: Tue, 18 Jul 2023 20:42:30 GMT Content-Type: text/plain Content-Length: 0 ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Date: Thu, 13 Jul 2023 12:05:24 GMT Content-Type: text/plain Content-Length: 0 Cobalt Strike Beacon: x86: beacon_type: HTTPS dns-beacon.strategy_fail_seconds: -1 dns-beacon.strategy_fail_x: -1 dns-beacon.strategy_rotate_seconds: -1 http-get.client: Cookie http-get.uri: 152.89.198.29,/__utm.gif http-get.verb: GET http-post.client: Content-Type: application/octet-stream id http-post.uri: /submit.php http-post.verb: POST maxgetsize: 1048576 port: 443 post-ex.spawnto_x64: %windir%\sysnative\rundll32.exe post-ex.spawnto_x86: %windir%\syswow64\rundll32.exe process-inject.execute: CreateThread SetThreadContext CreateRemoteThread RtlCreateUserThread process-inject.startrwx: 64 process-inject.stub: 222b8f27dbdfba8ddd559eeca27ea648 process-inject.userwx: 64 proxy.behavior: 2 (Use IE settings) server.publickey_md5: defb5d95ce99e1ebbf421a1a38d9cb64 sleeptime: 60000 useragent_header: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0) uses_cookies: 1 watermark: 1580103824 x64: beacon_type: HTTPS dns-beacon.strategy_fail_seconds: -1 dns-beacon.strategy_fail_x: -1 dns-beacon.strategy_rotate_seconds: -1 http-get.client: Cookie http-get.uri: 152.89.198.29,/g.pixel http-get.verb: GET http-post.client: Content-Type: application/octet-stream id http-post.uri:

/submit.php http-post.verb: POST maxgetsize: 1048576 port: 443 post-ex.spawnto_x64: %windir%\sysnative\rundll32.exe post-ex.spawnto_x86: %windir%\syswow64\rundll32.exe process-inject.execute: CreateThread SetThreadContext CreateRemoteThread RtlCreateUserThread process-inject.startrwx: 64 process-inject.stub: 222b8f27dbdfba8ddd559eeca27ea648 process-inject.userwx: 64 proxy.behavior: 2 (Use IE settings) server.publickey_md5: defb5d95ce99e1ebbf421a1a38d9cb64 sleeptime: 60000 useragent_header: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; LBBROWSER) uses_cookies: 1 watermark: 1580103824 ``` HEARTBLEED: 2023/07/13 12:06:04 152.89.198.29:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '152.89.198.29']

Name

173.44.141.237

Description

ISP: Eonix Corporation **OS:** None ---------- Hostnames: - 237.staticrdns.eonix.net ---------- Domains: - eonix.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCi7n9auJDcqViIMusv0G0BVMlbdMrscQzeSbcQCtebh5/8IdiqFJARgQsLZqGuoIvzaZsxooYqEseHrxhnqwRfgXlVph/eTTHNv1P4KyM+tdHHD073fWc/pnJkxXeTgG3X+rWd+146vaY8AtLj3Xp+RNq3RT5l1SxkvC7vnc/2yRW+0+FtZzzvestWwnKuJTnv2ixZhMg3FigE+vNlPEz3uXtlreRwV9rXCNo9eS9DAR9bfGpf9tTZNSYmpdahqdIWc+UwIDrSHcEgKvw6xHZt0yjKZ+TL0ZQ/KFQWXkm9emzbdk9s76UrRr3h4DlidwMW+IA0GgiY7ktvrMEa0BNcB5+KtcQvmVIbXD0MCzYu5RVaPh+GvI/r+czyVDycgCvVJbEGN/flyXtaaaNZhmSWPnkT06gFwYPqWH0WDbWXAHyPQS2dJS5xtEPqWIW0D7gbYWLybgA4Qx8e+gUQ1Sn0Oh8m7AdjskI/ewvf5MEhDnx9YmnAyGyD O0gJ8DZ0ins= Fingerprint: f8:33:06:cc:86:87:6e:a5:f3:e1:b6:06:2c:08:16:fa 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.44.141.237']

Name

http://itwicenice.com/pictures/

Pattern Type

stix

Pattern

[url:value = 'http://itwicenice.com/pictures/']

Name

91.212.166.44

Description

ISP: Proton66 OOO **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key:

AAAAB3NzaC1yc2EAAAADAQABAAABgQCdLZok4YX1JWUNm1K5+IgsV3PP6cBlmCaIjhGZPieksO9k
sTOU0BxEKoERPOc5yv0KZSk1+zBkz6h8/7W1Lsq7WqJ8aK/bDwcaioVqPeF3F2HZzqSgcc3XERoB
fhKG69USpCzFeKDugzcx4/+X+HGO7Hdll3fj9Qx+8qOu05MOA86puF9c1L+qECKDNTcv7JM1GoKE
mNsgxiz9J14qJQL8iai3qUu0KLezbgqlkcniXUsYhCe+Vx/8sXpcgPrO5z75OLBBDxJpWLP7G6Ze
Vck8noKMdWM2HNsE6IGlYyjb1NLPfeA2OuSqclcVfJOW3Dg6WKQvMVGkqTDFo8j5+oCj4sQaNb9
vM6EnYqSRPYNk4iAYOn7yIMHSKsaD6ZCF6cVJt86mafe2WnagDjQyYkjLdxZYlLki9LSqQUSduaf
PKd40P+47A5RxyeHTj8ym0C+ZPtD/idRxH4PKzVdS3PT2tRYyalxoGJU1QI+UhuoRcGRntPfm3//
mLNcGrentBc= Fingerprint: d6:7f:c9:1d:1e:2c:22:9c:3f:dc:55:a8:42:a9:b4:4a 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/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu) Date: Mon, 17 Jul 2023 00:30:31 GMT Content-Type: text/html;
charset=utf-8 Content-Length: 548 Connection: keep-alive Vary: Accept-Encoding ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.212.166.44']

Name

1324e7654a144c20637820a022d49c449cca1ff1d2c7e040bf23421d52146e93

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1324e7654a144c20637820a022d49c449cca1ff1d2c7e040bf23421d52146e93']

Name

894668791d06262dd16740235faa3b1672e2cb5cf171954f29abaca421c09265

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '894668791d06262dd16740235faa3b1672e2cb5cf171954f29abaca421c09265']

Name

http://31.172.83.49/pictures/...

Pattern Type

stix

Pattern

[url:value = 'http://31.172.83.49/pictures/...']

Name

170.130.165.159

Description

ISP: Eonix Corporation **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-

OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG44/tPgoQ9iJweQldacoWsX UgTLu/NHOfqJosAuOpooq3Q05u4oXlfijDI8jcPReSwcm61j9znPLCQwmLDzgc0= Fingerprint: 36:06:8b:3c:ad:71:34:2e:f4:50:b2:9b:ed:74:15:11 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/1.1 404 Not Found Date: Wed, 19 Jul 2023 07:28:47 GMT Server: Apache Content-Length: 0 Keep-Alive: timeout=10, max=100 Connection: Keep-Alive Content-Type: text/plain Cobalt Strike Beacon: x86: beacon_type: HTTPS dns-beacon.strategy_fail_seconds: -1 dns-beacon.strategy_fail_x: -1 dns-beacon.strategy_rotate_seconds: -1 http-get.client: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Referer: http://code.jquery.com/ Accept-Encoding: gzip, deflate __cfduid= Cookie http-get.uri: 170.130.165.159,/jquery-3.3.1.min.js http-get.verb: GET http-post.client: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Referer: http://code.jquery.com/ Accept-Encoding: gzip, deflate __cfduid http-post.uri: /jquery-3.3.2.min.js http-post.verb: POST jitter: 37 maxgetsize: 2801745 port: 443 post-ex.spawnto_x64: %windir%\sysnative\dllhost.exe post-ex.spawnto_x86: %windir%\syswow64\dllhost.exe process-inject.allocator: 1 process-inject.execute: ntdll:RtlUserThreadStart CreateThread NtQueueApcThread-s CreateRemoteThread RtlCreateUserThread process-inject.min_alloc: 17500 process-inject.startrwx: 4 process-inject.stub: c54eed2fbdc9655c0c13550f04c72c28 process-inject.userwx: 32 proxy.behavior: 2 (Use IE settings) server.publickey_md5: 523573131c780cc4e424ab4798e19299 sleeptime: 45000 stage.cleanup: 1 useragent_header: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko uses_cookies: 1 watermark: 674054486 x64: beacon_type: HTTPS dns-beacon.strategy_fail_seconds: -1 dns-beacon.strategy_fail_x: -1 dns-beacon.strategy_rotate_seconds: -1 http-get.client: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Referer: http://code.jquery.com/ Accept-Encoding: gzip, deflate __cfduid= Cookie http-get.uri: 170.130.165.159,/jquery-3.3.1.min.js http-get.verb: GET http-post.client: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Referer: http://code.jquery.com/ Accept-Encoding: gzip, deflate __cfduid http-post.uri: /jquery-3.3.2.min.js http-post.verb: POST jitter: 37 maxgetsize: 2801745 port: 443 post-ex.spawnto_x64: %windir%\sysnative\dllhost.exe post-ex.spawnto_x86: %windir%\syswow64\dllhost.exe process-inject.allocator: 1 process-inject.execute: ntdll:RtlUserThreadStart CreateThread NtQueueApcThread-s CreateRemoteThread RtlCreateUserThread process-inject.min_alloc: 17500 process-inject.startrwx: 4 process-inject.stub: c54eed2fbdc9655c0c13550f04c72c28 process-inject.userwx: 32 proxy.behavior: 2

(Use IE settings) server.publickey_md5: 523573131c780cc4e424ab4798e19299 sleeptime: 45000 stage.cleanup: 1 useragent_header: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko uses_cookies: 1 watermark: 674054486 ``` HEARTBLEED: 2023/07/19 07:29:01 170.130.165.159:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '170.130.165.159']

Name

6e8b848e7e28a1fd474bf825330bbd4c054346ad1698c68e7a59dd38232a940a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e8b848e7e28a1fd474bf825330bbd4c054346ad1698c68e7a59dd38232a940a']

Malware

Name
Trojan:Win32/Ursnif

Attack-Pattern

Name

VNC

ID

T1021.005

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely control machines using Virtual Network Computing (VNC). VNC is a platform-independent desktop sharing system that uses the RFB (“remote framebuffer”) protocol to enable users to remotely control another computer’s display by relaying the screen, mouse, and keyboard inputs over the network.(Citation: The Remote Framebuffer Protocol) VNC differs from [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) as VNC is screen-sharing software rather than resource-sharing software. By default, VNC uses the system's authentication, but it can be configured to use credentials specific to VNC.(Citation: MacOS VNC software for Remote Desktop)(Citation: VNC Authentication) Adversaries may abuse VNC to perform malicious actions as the logged-on user such as opening documents, downloading files, and running arbitrary commands. An adversary could use VNC to remotely control and monitor a system to collect data and information to pivot to other systems within the network. Specific VNC libraries/implementations have also been susceptible to brute force attacks and memory usage exploitation.(Citation: Hijacking VNC)(Citation: macOS root VNC login without authentication)(Citation: VNC Vulnerabilities)(Citation: Offensive Security VNC Authentication Check)(Citation: Attacking VNC Servers PentestLab)(Citation: Havana authentication bug)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Country

Name
Italy

StixFile

Value
894668791d06262dd16740235faa3b1672e2cb5cf171954f29abaca421c09265
1324e7654a144c20637820a022d49c449cca1ff1d2c7e040bf23421d52146e93
6e8b848e7e28a1fd474bf825330bbd4c054346ad1698c68e7a59dd38232a940a

IPv4-Addr

Value
173.44.141.237
31.172.83.49
170.130.165.159
173.44.141.199
109.105.198.129
152.89.198.29
185.82.127.183
91.201.65.64
91.212.166.44

Url

Value
http://31.172.83.49/pictures/...
http://itwicenice.com/pictures/
http://delideta.com/pictures/
http://109.105.198.129/pictures/...
http://avas1t.de/in/loginq/

External References

- https://otx.alienvault.com/pulse/64b7cdb9fe627a02501b2be1
- https://kostas-ts.medium.com/ursnif-vs-italy-il-pdf-del-destino-5c83d6281072