May 02 2024

NETMANAGEIT

Intelligence Report

Scaly Wolf's new loader: the right tool for the wrong job

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The report analyzes a recent campaign by the Scaly Wolf threat group targeting organizations in Russia and Belarus. The group employs phishing emails disguised as communications from government agencies, containing legitimate documents and password-protected archives with malicious executables. The executable is a loader that injects the White Snake stealer malware into the explorer.exe process, evading detection through anti-virtualization checks and kernel calls instead of WinAPI. The White Snake malware harvests credentials and sensitive data from compromised systems.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

66.42.56.128

Description

ISP: The Constant Company, LLC **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCq54gKqYol8xLANlFJI+wOzjnvDnu5Q33+zcSdrj/QhIwn p1w9D9BaPMpPf2fa8bry0S2gYm6K7Ugdk6qdToWeLAaMPQWfF8fXOzAKR56KSyRnKA+Ad6wFc/ xq 3voZbn0dLasINn8gIKR6YzGLaNdUMC0VjYhMrZc73Q98b6qaAP3B1j3DokhjGujAinkgq3OJ+kFz RxZFq7eevHM081tqEoxRMOEmXNgAcc25I5PeevgRZBMJxDs8LrJlBos2aeE5ADSjM5lQzKdQVc/Z vD1ouzvEqvgSLyK4lymDqrJtOzcXRK1kRO8Zve0eeOZQRuRr1NMGQdkbDUBch0dXzmMn Fingerprint: f7:07:e4:e5:7a:9b:6b:59:ec:60:95:99:c2:18:b2:92 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, 22 Apr 2024 01:03:59 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: Fri, 19 Apr 2024 03:13:35 GMT Transfer-Encoding: chunked ``` ---------- **8080:** ``` HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 14 Apr 2024 15:39:52 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

64.227.21.98

Description

ISP: DigitalOcean, LLC **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC3idUgugeKv7cMIJnZoFJwQYHlRJOiYxtTePhTCi2jJAM8cv6miW297vJWADd6sBvqJ0XdJgVIh4qEITMTvDwqk6c6nkgb+v//mrOWGhMNoAAkNwnbkcA8l11LJMrvGgLwtaiyAaOhYsiKrhyBhzymP86Cl74vGorr8EstIbneTBjWnBpqfFmyyxGxaVDWJ1LN7I8S96h0VcbPh0I2diFtQbaE60KDZcg/gV3jaI4ow4vbGEJ1fpWuw8Oycwz3gpmhgQZzoS6p5C+UyVAmACn6Ej7Mjrtt8l/EHjvQtnFBQ6cpUHsOJjHTRlTIHreSjgWSLnKMwXk6p0U8mNBaL/tV Fingerprint: 96:2b:aa:b3:b9:89:a9:02:9c:61:1f:24:82:27:f7:0e 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 kex-strict-s-v00@openssh.com 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/1.1 308 Permanent Redirect Date: Sat, 20 Apr 2024 21:31:00 GMT Server: Transfer.sh HTTP Server Content-Type: text/html; charset=utf-8 Location: https://64.227.21.98/ X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Content-Length: 57 ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Sat, 20

Apr 2024 21:31:03 GMT Server: Transfer.sh HTTP Server X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Content-Type: text/html; charset=utf-8 Vary: Accept-Encoding Transfer-Encoding: chunked ``` HEARTBLEED: 2024/04/20 21:31:09 64.227.21.98:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.227.21.98']

Name

45.61.136.52

Description

ISP: BL Networks **OS:** - ---------- Services: **21:** ``` 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 16:42. 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 Unable to read the indexed puredb file (or old format detected) - Try pure-pw mkdb 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 SPSV ESTP 211 End. ``` ---------- **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEUr8N43h2gywk3ek67vJT3A HC5NoxnoKRUCilUHeB0v04NDAor8GGM4Cdk0EA7QsHsuFpi7b6wOHw81S96VFbs= Fingerprint: 1f:47:ef:49:fe:4b:fb:a1:5b:dd:c9:86:08:9e:f2: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 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-

sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Fri, 19 Apr 2024 13:35:18 GMT Server: Apache Upgrade: h2 Connection: Upgrade, close Last-Modified: Tue, 12 Mar 2024 18:59:35 GMT ETag: "27e-6137b426333bc" Accept-Ranges: bytes Content-Length: 638 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **888:** ``` HTTP/1.1 403 Forbidden Date: Sun, 14 Apr 2024 03:45:28 GMT Server: Apache Content-Length: 261 Connection: close Content-Type: text/html; charset=iso-8859-1 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.61.136.52']

Name

45.61.136.13

Description

ISP: BL Networks **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJH/imBRdcyY5jJh3jpCXmx/2VHZnorwzwhgqcuKITB0HCYc8cpBfu/8XCvkC0gToW+w1wWir5yD6CQz3GQ8n68= Fingerprint: be:4a:f7:49:0b:38:4d:24:7c:ae:40:53:71:b8:0e:54 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.61.136.13']

Name

23.248.176.37

Description

- **Zip Code:** N/A - **ISP:** Zenlayer - **ASN:** 21859 - **Organization:** IPVanish VPN - **Is Crawler:** False - **Timezone:** Asia/Taipei - **Mobile:** False - **Host:** 23.248.176.37 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** TW - **Region:** Taipei City - **City:** Taipei - **Latitude:** 25.04999924 - **Longitude:** 121.52999878

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.248.176.37']

Name

23.224.102.6

Description

- **Zip Code:** N/A - **ISP:** Cnservers LLC - **ASN:** 40065 - **Organization:** Cnservers LLC - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 23.224.102.6 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Los Angeles - **Latitude:** 34.04999924 - **Longitude:** -118.23999786

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.224.102.6']

Name

212.6.44.53

Description

ISP: SIA VEESP **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBB6l2QWNzZ8YggsYLdCsbX9C jwnqAPOQwvsWKT2wMRkAl11hcRtwOMdzTFsnyGCqrh6/eezMJjEroBgYOgAA+ik= Fingerprint: 84:bc:d9:0e:d6:6b:34:ac:df:1d:41:2d:d5:52:8b: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-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 kex-strict-s-v00@openssh.com Server Host Key Algorithms: ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.6.44.53']

Name

193.142.58.127

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Europe/Bucharest - **Mobile:** False - **Host:** 193.142.58.127 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RO - **Region:** Bucuresti - **City:** Bucharest - **Latitude:** 44.43000031 - **Longitude:** 26.10000038

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.142.58.127']

Name

185.119.118.59

Description

ISP: IPAX GmbH **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKDY1xe6+AYmRb2Yyss7faTnidGIuleVf/5suhZnEu4Wtp88IGpYMNqgHO0xKVP/f2cXbgloDaWmJxe/GqjvFWo= Fingerprint: 48:39:85:13:61:dc:94:21:06:b9:78:98:60:bc:ec:ce Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **25:** ``` 220 vosn.at ESMTP Postfix (Ubuntu) 250-vosn.at 250-PIPELINING 250-SIZE 10240000 250-VRFY 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 23 Apr 2024 09:18:44 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Wed, 01 Nov 2023 21:03:02 GMT ETag: "59-6091d98d3622c" Accept-Ranges: bytes Content-Length: 89 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Sun, 21 Apr 2024 08:05:55 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Wed, 01 Nov 2023 21:03:02 GMT ETag: "59-6091d98d3622c" Accept-Ranges: bytes Content-Length: 89 Vary: Accept-Encoding Content-Type: text/html ``` HEARTBLEED: 2024/04/21 08:06:09 185.119.118.59:443 - SAFE ---------- **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: Sat, 13 Apr 2024 12:21:19 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.119.118.59']

Name

154.26.128.6

Description

ISP: Contabo Asia Private Limited **OS:** CentOS Linux 7 (Core) (Linux 3.10.0-1160.71.1.el7.x86_64) ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAACAQC4Hb02XBnJdepazd3q4cTySobnkLM3Ahd2EB/M0tpiH1AO F4lDzxmCSmJp6a6jzI/w6D3SD9ED+e3P2FA5pegmPNFb2IXaF1gmPcmlY412y8gD7DcF8o+NYeitIzNLXOWhxkn3rFGLQRb9L7uNF8XXDf9Au/l35oeENusBzcT+SQPeupwq2DZXkP3n3kWtt9Ru0S3x+qG9cH5YMPD9iZHftytdEiC2GqewKu3+8ZVCh4sdJbRzRk5V7LWsWwZ7TEk2XUOdiiV2xaJ7+FONUTeYqo8QZ4nTiaU0Fkfp3MCoiPphTWweiAzvhhajlrTwlDlDXdBqmX61LeqV/93DGPs7MVKWJuH+O6baTac2gzwhhMX7/R6xMi6Rwmi12aJFj4bEogzheE6jwMf+uwk7iQPKuA8zGRopVqdBMKsx1GZl7vC4dg+CQ8aov6yM7SuVXyF7kRpssV/tSfVDLfuD2sWGPuRZTlVbf8N5w0VfYFV/a3ClXDIf/uiFFpdqq/VrbSyzXgx5uYEgn7NuFbQmyOt4I+6pLc6okuEzx1wpOppa7XTEknOee+uV0hYqAgn+oUipJbsxJBycyiWU17fKdxwi4qzKo1fFsO7zdN088A52QY6Vdji/nhTh39iF7YPOFrP3WW9OB4HBgZcYpr4x+xSfqlAgmdPopjOqu3YqW3Z7uw== Fingerprint: 54:93:63:ce:e3:3c:f9:09:f5:7f:3f:09:81:d2:75:24 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: nginx Date: Thu, 11 Apr 2024 02:25:43 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Fri, 14 Jan 2022 07:23:06 GMT Connection: keep-alive ETag: "61e124da-267" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 11 Apr 2024 14:01:53 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive X-Redirect-By: WordPress Location: https://www.counterstreamradio.org/ X-Cache: MISS ``` HEARTBLEED: 2024/04/11 14:02:07 154.26.128.6:443 - SAFE ---------- **9001:** ``` HTTP/1.1 403 Forbidden Content-Type: application/json Portainer-Agent: 2.19.2 Portainer-Agent-Api-Version: 2 Portainer-Agent-Platform: 1 Date: Sat, 13 Apr 2024 17:57:26 GMT Content-Length: 73 ``` HEARTBLEED: 2024/04/13 17:57:42 154.26.128.6:9001 - SAFE ---------- **9100:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Connection: close 400 Bad Request Prometheus Node Exporter: node_exporter_build_info: branch: HEAD goarch: amd64 goos: linux goversion: go1.21.4 revision: 7333465abf9efba81876303bb57e6fadb946041b tags: netgo osusergo static_build version: 1.7.0 node_os_info: id: centos id_like: rhel fedora name: CentOS Linux pretty_name: CentOS Linux 7 (Core) version: 7 (Core) version_id: 7

node_uname_info: domainname: (none) machine: x86_64 nodename: 40319a29cf9e release: 3.10.0-1160.71.1.el7.x86_64 sysname: Linux version: #1 SMP Tue Jun 28 15:37:28 UTC 2022 node_dmi_info: bios_date: 04/01/2014 bios_vendor: SeaBIOS bios_version: rel-1.16.1-0-g3208b098f51a-prebuilt.qemu.org chassis_vendor: QEMU chassis_version: pc-i440fx-7.2 product_name: Standard PC (i440FX + PIIX, 1996) product_version: pc-i440fx-7.2 system_vendor: QEMU node_network_info: docker0: address: 02:42:d3:a4:59:18 adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: docker0 operstate: down lo: address: 00:00:00:00:00:00 adminstate: up broadcast: 00:00:00:00:00:00 device: lo operstate: unknown veth24dca91: address: aa:d7:fb:b9:96:26 adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: veth24dca91 duplex: full operstate: up vethb40f77e: address: 1a:6b:ee:e0:1f:d2 adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: vethb40f77e duplex: full operstate: up br-a8c104e0677b: address: 02:42:20:59:a8:5e adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: br-a8c104e0677b operstate: up veth1d9e1a1: address: d6:80:7c:9d:40:d3 adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: veth1d9e1a1 duplex: full operstate: up eth0: address: 00:50:56:4f:74:b3 adminstate: up broadcast: ff:ff:ff:ff:ff:ff device: eth0 operstate: up ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.26.128.6']

Name

149.88.44.159

Description

ISP: CreeperHost LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCmo1uC/MP1X/gHiY8dHzT/GPWXvDbtS+syyVTKNXtm9oJW
BVDfwlJ7fLqnTyOOUGmdMHAghL63c0aXGDrSjJrBIOV/j7dOEQGWx4D5WqqpaS/MqfM4XOxD969M
AFPcUTFqx6ujucYj5Ocjk7TZllHl2SDPTRgQdM4l7sUmx52VuoGjFpwX2P2NQGixhSK/epXo8bmi
pu7RPHC4T3hTl+0wBhpdtl6YLYo5Cqnsf7QBLniT9T4ob6EUXl712nFo1xX+GlhX4XisP04p2Gkr
2nepRDTdnZXysj/U8pmfEnX7c8d7Qv+5JH5aVPKN+yq4X9SL4mZ8n7KZ9xJWEDAfaWhh Fingerprint: 9d:4e:a2:fe:1d:35:f9:dd:b4:65:58:28:2f:da:5d:01 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 1.0 X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Thu, 11 Apr 2024 14:28:28 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '149.88.44.159']

Name

cbabd91fb0c1c83867f71e8df19c131ac6fb3b3f3f74765bc24924cb9d51ad41

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cbabd91fb0c1c83867f71e8df19c131ac6fb3b3f3f74765bc24924cb9d51ad41']

Name

93948c7fb89059e1f63af04feef0a0834b65b18ffaf6610b419adbc0e271e23d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '93948c7fb89059e1f63af04feef0a0834b65b18ffaf6610b419adbc0e271e23d']

Name

10330fcc378db73346501b2a26d2c749f51cacd962b54c62aa017dd9c1ed77c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10330fcc378db73346501b2a26d2c749f51cacd962b54c62aa017dd9c1ed77c3']

Name

144.126.132.141

Description

ISP: Nubes, LLC **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAACAQDzumuyLIPyeJh3jvcignfOhsQiN3PdO7cd0SlOEvY7BCDfmTZs+Uli8ED1zmk5sFp2sRn2vQySuu5I9Ma6iY1WG4C+DH3yghVJmKDf9D/G2YBLIGX+DufJ8MvQRpr/CUt91iCnansWbzu8lYwgCQ19FmlgTfSxOUcscfDhMHkzcHjtbRb08JxnPF207Z9F1/oolzMoHpu+1AfjxMlmKU2Vm4LyodaZH8ZtG3Ah4tj1Yiv1PrSv4Lj3UWHcUqq5n/EsXrgRQgFNdj3yelNUnhvwFjjhzns6aoFNTdww6mzIa1U2cQ3Ei6s44h0Qg8dLaG3/IvofbGsGXxLzbKGLO8cL9XjG2P1s

FMm1Gtf3am5SYXg9ExbLnTCej+swflZhlgP1tqfHSzBXN/dP06F96OxSWFSxm67bQiPRR9zY3ty/7tmfkekCS7zh9ALO8sLYfQfLxI8WyAksG7lF4eAi7bnBDplK9G8dZhq8XiDxcT6IWaL7T61ryAsbfYXYV932BNxon7yqYrpisnKoMbCKaTWEkP+o/yPeSpI6uTcNN7i5YoalTz66X3r9uIxCoMZbI3aoJ7s9eFdJmUsiGeHZ8RyRBYAiUyE/gH8boTttmI+Ld0rMYwaawm3VWd8i9RxH62cu7uGshStzUbniDdosJgYWzGVkum1YRHLsCNn6KlAaTw== Fingerprint: af:3c:b6:db:87:ca:3b:1e:06:fa:fa:34:65:b3:d4:b9 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/1.1 404 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 Date: Mon, 22 Apr 2024 15:46:47 GMT Connection: keep-alive Keep-Alive: timeout=5 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '144.126.132.141']

Name

104.248.208.221

Description

ISP: DigitalOcean, LLC **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_9.0 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJpiRgOiZNYUOAtRQXVaR79gw7akd1DqBRvKFjcj7K36RfFpXJa9mGk2aalE7YDSg9em7BBTHvrMX+xbeyjRSqo= Fingerprint: b9:56:0e:15:b1:c5:50:2e:c9:e1:ec:e2:58:fc:26:3d 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 kex-strict-s-v00@openssh.com Server Host Key Algorithms: ecdsa-sha2-nistp256 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr MAC Algorithms: hmac-sha2-256-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.248.208.221']

Name

216.250.190.139

Description

CC=US ASN=AS7753 GREENCLOUD

Pattern Type

stix

Pattern

[ipv4-addr:value = '216.250.190.139']

Name

206.189.109.146

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[ipv4-addr:value = '206.189.109.146']

Name

192.99.196.191

Description

CC=CA ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.99.196.191']

Name

164.90.185.9

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type
stix
Pattern
[ipv4-addr:value = '164.90.185.9']
Name
107.161.20.142
Description
CC=US ASN=AS3842 RAMNODE
Pattern Type
stix
Pattern
[ipv4-addr:value = '107.161.20.142']
Name
185.217.98.121
Description
WhiteSnake Stealer botnet C2 server (confidence level: 100%)
Pattern Type
stix

Pattern
[ipv4-addr:value = '185.217.98.121']
Name
116.202.101.219
Description
WhiteSnake Stealer botnet C2 server (confidence level: 100%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '116.202.101.219']

Malware

Name
White Snake

Name
infostealer

Intrusion-Set

Name
Scaly Wolf

Attack-Pattern

Name
T1012
ID
T1012
Description
Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
Name
T1036.004
ID
T1036.004

Description

Adversaries may attempt to manipulate the name of a task or service to make it appear legitimate or benign. Tasks/services executed by the Task Scheduler or systemd will typically be given a name and/or description.(Citation: TechNet Schtasks)(Citation: Systemd Service Units) Windows services will have a service name as well as a display name. Many benign tasks and services exist that have commonly associated names. Adversaries may give tasks or services names that are similar or identical to those of legitimate ones. Tasks or services contain other fields, such as a description, that adversaries may attempt to make appear legitimate.(Citation: Palo Alto Shamoon Nov 2016) (Citation: Fysbis Dr Web Analysis)

Name

T1003.001

ID

T1003.001

Description

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550). As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system. For example, on the target host use procdump: * `procdump -ma lsass.exe lsass_dump` Locally, mimikatz can be run using: * `sekurlsa::Minidump lsassdump.dmp` * `sekurlsa::logonPasswords` Built-in Windows tools such as `comsvcs.dll` can also be used: * `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full`(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector) Similar to [Image File Execution Options Injection](https://attack.mitre.org/techniques/T1546/012), the silent process exit mechanism can be abused to create a memory dump of `lsass.exe` through Windows Error Reporting (`WerFault.exe`).(Citation: Deep Instinct LSASS) Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any

logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014) The following SSPs can be used to access credentials: * Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package. * Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. (Citation: TechNet Blogs Credential Protection) * Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later. * CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

Name

T1497

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

Name

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

T1005

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation:

show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Name

T1559.001

ID

T1559.001

Description

Adversaries may use the Windows Component Object Model (COM) for local code execution. COM is an inter-process communication (IPC) component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces.(Citation: Fireeye Hunting COM June 2019) Through COM, a client object can call methods of server objects, which are typically binary Dynamic Link Libraries (DLL) or executables (EXE).(Citation: Microsoft COM) Remote COM execution is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM).(Citation: Fireeye Hunting COM June 2019) Various COM interfaces are exposed that can be abused to invoke arbitrary execution via a variety of programming languages such as C, C++, Java, and [Visual Basic](https://attack.mitre.org/techniques/T1059/005).(Citation: Microsoft COM) Specific COM objects also exist to directly perform functions beyond code execution, such as creating a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), fileless download/execution, and other adversary behaviors related to privilege escalation and persistence.(Citation: Fireeye Hunting COM June 2019)(Citation: ProjectZero File Write EoP Apr 2018)

Name

T1566.001

ID

T1566.001

Description

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution. (Citation: Unit 42 DarkHydrus July 2018) Spearphishing may also involve social engineering techniques, such as posing as a trusted source. There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Name

T1497.001

ID

T1497.001

Description

Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Specific checks will vary based on the target and/or

adversary, but may involve behaviors such as [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047), [PowerShell](https://attack.mitre.org/techniques/T1059/001), [System Information Discovery](https://attack.mitre.org/techniques/T1082), and [Query Registry](https://attack.mitre.org/techniques/T1012) to obtain system information and search for VME artifacts. Adversaries may search for VME artifacts in memory, processes, file system, hardware, and/or the Registry. Adversaries may use scripting to automate these checks into one script and then have the program exit if it determines the system to be a virtual environment. Checks could include generic system properties such as host/domain name and samples of network traffic. Adversaries may also check the network adapters addresses, CPU core count, and available memory/drive size. Once executed, malware may also use [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) to check if it was saved in a folder or file with unexpected or even analysis-related naming artifacts such as `malware`, `sample`, or `hash`. Other common checks may enumerate services running that are unique to these applications, installed programs on the system, manufacturer/product fields for strings relating to virtual machine applications, and VME-specific hardware/processor instructions.(Citation: McAfee Virtual Jan 2017) In applications like VMWare, adversaries can also use a special I/O port to send commands and receive output. Hardware checks, such as the presence of the fan, temperature, and audio devices, could also be used to gather evidence that can be indicative a virtual environment. Adversaries may also query for specific readings from these devices.(Citation: Unit 42 OilRig Sept 2018)

Name

T1053.005

ID

T1053.005

Description

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task. The deprecated [at](https://attack.mitre.org/software/S0110) utility could also be abused by adversaries (ex: [At](https://attack.mitre.org/techniques/T1053/002)), though `at.exe` can not access tasks

created with `schtasks` or the Control Panel. An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent) Adversaries may also create "hidden" scheduled tasks (i.e. [Hide Artifacts](https://attack.mitre.org/techniques/T1564)) that may not be visible to defender tools and manual queries used to enumerate tasks. Specifically, an adversary may hide a task from `schtasks /query` and the Task Scheduler by deleting the associated Security Descriptor (SD) registry value (where deletion of this value must be completed using SYSTEM permissions).(Citation: SigmaHQ)(Citation: Tarrask scheduled task) Adversaries may also employ alternate methods to hide tasks, such as altering the metadata (e.g., `Index` value) within associated registry keys.(Citation: Defending Against Scheduled Task Attacks in Windows Environments)

Country

Name
Russian Federation

Name
Belarus

Region

Name
Eastern Europe

Name
Europe

IPv4-Addr

Value
66.42.56.128
64.227.21.98
45.61.136.52
45.61.136.13
23.248.176.37
23.224.102.6
212.6.44.53
193.142.58.127
185.119.118.59
154.26.128.6
149.88.44.159
144.126.132.141
104.248.208.221

216.250.190.139
206.189.109.146
192.99.196.191
164.90.185.9
107.161.20.142
116.202.101.219
185.217.98.121

StixFile

Value
cbabd91fb0c1c83867f71e8df19c131ac6fb3b3f3f74765bc24924cb9d51ad41
93948c7fb89059e1f63af04feef0a0834b65b18ffaf6610b419adbc0e271e23d
10330fcc378db73346501b2a26d2c749f51cacd962b54c62aa017dd9c1ed77c3

External References

- https://bi-zone.medium.com/scaly-wolfs-new-loader-the-right-tool-for-the-wrong-job-0b36d4c20c88
- https://otx.alienvault.com/pulse/6633a7d33e50ab19ed022c7e