Oct 28 2023

NETMANAGEIT

Intelligence Report

Various actors actively deploying Lumma Stealer in multiple campaigns

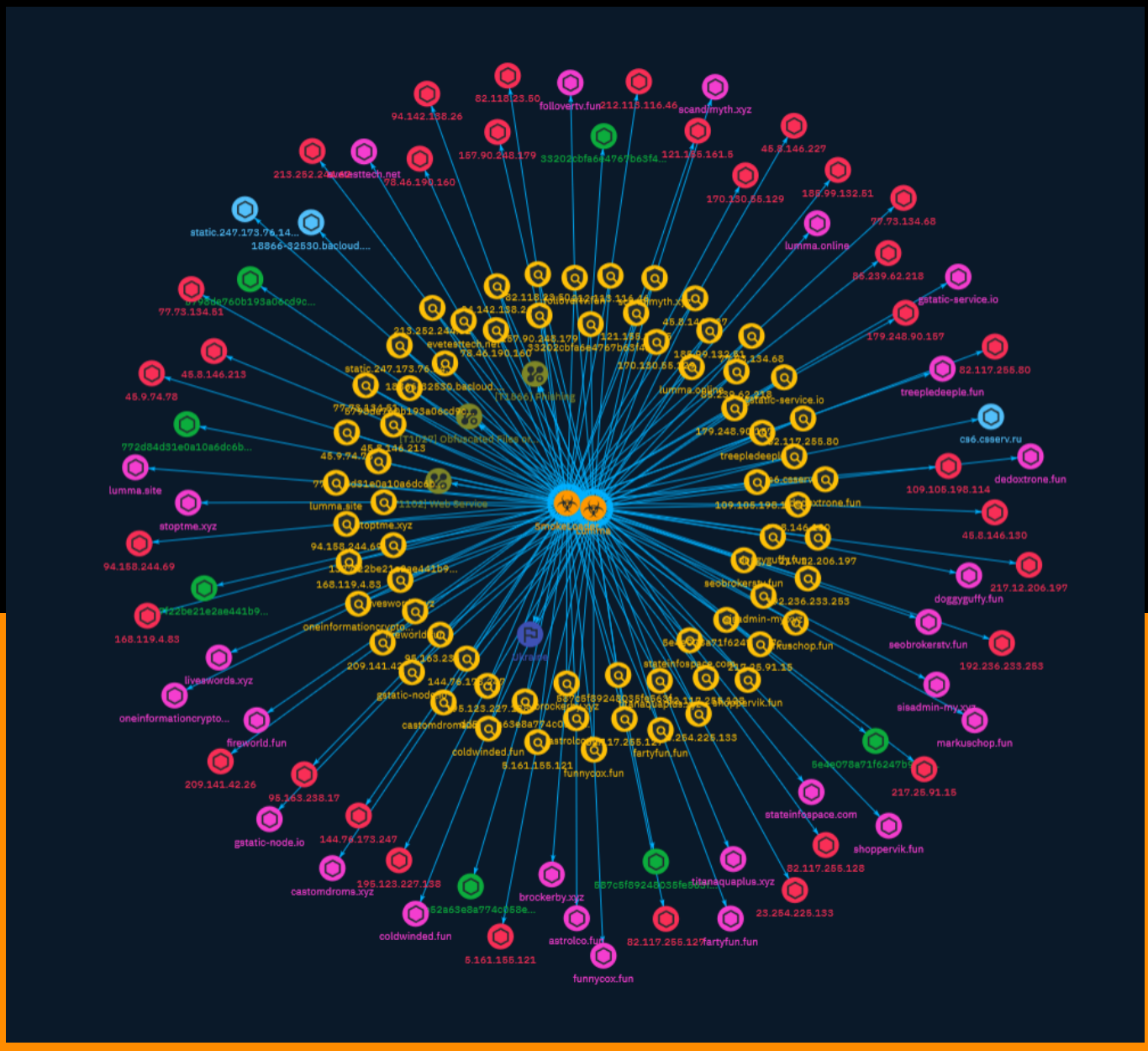

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A report on Lumma Stealer, a malware-as-a-service sold through Telegram and Russian-speaking forums, has been published by the European Union's cyber security agency, Intrinsec.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

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).

Indicator

Name
5798de760b193a06cd9cb1c197feae081e2cff84ba5514a53ad313341b95663e
Description
Balance Sheet#37553.html
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5798de760b193a06cd9cb1c197feae081e2cff84ba5514a53ad313341b95663e']
Name
funnycox.fun
Pattern Type
stix
Pattern

[domain-name:value = 'funnycox.fun']

Name

45.8.146.227

Description

CC=US ASN=AS44477 Stark Industries Solutions Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.8.146.227']

Name

dd5b52a63e8a774c058e558aa7e983d6aa51f560ba3f01829287c4b85081b884

Description

Lumma – Executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dd5b52a63e8a774c058e558aa7e983d6aa51f560ba3f01829287c4b85081b884']

Name
85.239.62.218
Description
CC=GB ASN=AS62240 Clouvider Limited
Pattern Type
stix
Pattern
[ipv4-addr:value = '85.239.62.218']
Name
45.8.146.213
Description
CC=US ASN=AS44477 Stark Industries Solutions Ltd
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.8.146.213']
Name
treepledeeple.fun

Pattern Type

stix

Pattern

[domain-name:value = 'treepledeeple.fun']

Name

castomdroms.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'castomdroms.xyz']

Name

157.90.248.179

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.179.248.90.157.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDXeiA/CbPuRi8prlfKQvWVZLZMN+nX1qkFswpeO2g1A3St yjgMxMj7YnyTqiPBDmDVZRzFgBLQuPUt9MEGuydeEBFc7SYy2k6oVuy+PVW2v20NMBF5hT1lAdtq nYkiyMONq3bSKnh+7/THK/x93BONucjmQVLSkD8y0gOdKCrk2pK0Jl4WCqP1lOsPVLfE7gHDzJ+y zh3HqrW4XsLHe3Ex4/gk5X420mHzxsxDl511I/hiE0cWBOQ5b6YOIohTieZV+dguM0mOTiCuLpgZ lBW+t+tyPjYRIoPSzvBH462iUBJFRk62ygTHSZPtt90hGvrNVhtpTdjVokIj/tkKPydt Fingerprint: 6c:e9:d3:b9:9c:78:14:b9:69:b9:52:43:2a:b9:0b:bc 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 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: Tue, 24 Oct 2023 13:35:29 GMT Server: Apache/2.4.38 (Debian) Set-Cookie: PHPSESSID=3h9t16c35i3sohkvom42c82uin; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Content-Length: 3347 Content-Type: text/html; charset=UTF-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '157.90.248.179']

Name

seobrokerstv.fun

Pattern Type

stix

Pattern

[domain-name:value = 'seobrokerstv.fun']

Name

77.73.134.51

Description

CC=KZ ASN=AS207713 Global Internet Solutions LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '77.73.134.51']

Name

82.117.255.127

Description

ISP: GREEN FLOID LLC **OS:** None ---------- Hostnames: - findingcurve.store ---------- Domains: - findingcurve.store ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCzYX6vb2hLW334eCS5zn4jEE8VgD06fc4SECLnlIdIM1eb I2NliGIzb4d2KV6sF0QJKbJwASCSIXgOjQBUeaoxx0Wm5a0ARB6xup2u0acjolo2ATe8NfHUBmlg 5LFQSBVi3kpnjwnIWO5jMkOE9EtKw12N4A0noyx2MS7kHLj/wPigq0xOjT9wV4iFYmogumMvIeaL pd09KupUrgYs7bwPsapAl1GRLQL1FPXIoJChZrhYmyY2tiOLO4/29asZatf8rzpGKvO7s6trJ/3b Y83C+sVmmQpBDZEPDSclkdTFcioPxENBsvWmEUeYu1tKq7XQEuKJSoV3WGuZWUPCqWIj Fingerprint: 68:bf:04:ca:44:5a:eb:11:3e:2f:d3:5a:39:8e:7a:c7 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 ``` ---------- **25:** ``` 220 mail.findingcurve.store ESMTP service ready 250-

mail.findingcurve.store says hello 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250-8BITMIME 250-AUTH CRAM-MD5 250-AUTH=CRAM-MD5 250-XACK 250-SIZE 0 250-VERP 250 DSN ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Mon, 23 Oct 2023 12:20:37 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 1888 Content-Type: text/html; charset=UTF-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '82.117.255.127']

Name

195.123.227.138

Description

ISP: ITL LLC **OS:** None ---------- Hostnames: - vps.hostry.com ---------- Domains: - hostry.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCfTAmzBZPxrLDzucq0XeUyJb/SXYO4Rpb0VWyzaszuGLEpnSnx6FmZF97at7fQvJ6ovE8S3a4fdqvtuLFNbX1M= Fingerprint: 89:6b:2b:e5:ae:ef:0b:0d:15:a7:b8:e8:6d:52:61:2f 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.123.227.138']

Name

cs6.csserv.ru

Pattern Type

stix

Pattern

[hostname:value = 'cs6.csserv.ru']

Name

shoppervik.fun

Pattern Type

stix

Pattern

[domain-name:value = 'shoppervik.fun']

Name

stateinfospace.com

Pattern Type

stix

Pattern

[domain-name:value = 'stateinfospace.com']

Name

77.73.134.68

Description

CC=KZ ASN=AS207713 Global Internet Solutions LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '77.73.134.68']

Name

astrolco.fun

Pattern Type

stix

Pattern

[domain-name:value = 'astrolco.fun']

Name

82.118.23.50

Description

CC=PL ASN=AS204957 Green Floid LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '82.118.23.50']

Name

217.12.206.197

Description

CC=PL ASN=AS204957 Green Floid LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.12.206.197']

Name

stoptme.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'stoptme.xyz']

Name

772d84d31e0a10a6dc6b7bb9bc2f71e135260e95a79e18b2145d53f678639232

Description

Request for Proposal (RFP)#51982.html

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '772d84d31e0a10a6dc6b7bb9bc2f71e135260e95a79e18b2145d53f678639232']

Name

95.163.238.17

Description

CC=RU ASN=AS197695 Domain names registrar REG.RU, Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.163.238.17']

Name

121.155.161.5

Description

CC=KR ASN=AS4766 Korea Telecom

Pattern Type

stix

Pattern

[ipv4-addr:value = '121.155.161.5']

Name

587c5f89248035fe563f06a8b991f081418e6013cc0e77f9e052de59b758c1c1

Description

dober.css

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '587c5f89248035fe563f06a8b991f081418e6013cc0e77f9e052de59b758c1c1']

Name

209.141.42.26

Description

CC=US ASN=AS53667 PONYNET

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.141.42.26']

Name

33202cbfa6e4767b63f4dd9eb5b653d32761aa80f0ee11eaba822e0f444f3ad7

Description

Business License#60674.html

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '33202cbfa6e4767b63f4dd9eb5b653d32761aa80f0ee11eaba822e0f444f3ad7']

Name

82.117.255.128

Description

CC=RO ASN=AS204957 Green Floid LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '82.117.255.128']

Name

213.252.244.62

Description

ISP: Informacines sistemos ir technologijos, UAB **OS:** None ---------- Hostnames: - 18866-32530.bacloud.info ---------- Domains: - bacloud.info ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDcybBVoL/m7usA9gb1CVSeZUvWVlohLTxb0ta70CvjvEvYlWOplWfR0kiE7tIx8+YRLLSABU+tSdMHkyAM9sraHlwLFKo5jwODlP7uKM5pE3uUnp+ez789bU0bxHeIipHFotM5ESCQ5M3r6hwcvEASexjruyO91w9hTOMnUwFBic/c/Ym0dnAofYOQmG+mQpBbLL5LJqnfE5qfw9LGR3gME+XpTWEWQEmWyoPvj4LVAohcLqJmfXw42yaiifMj/0vbEiyklz3FGpny+Ra9fY+7qNNPs5tlf7dj/UqnFY6334ptslFQORcvKyBb9IZOjIofJ7O4EyEzYbKBMM0rOh0j Fingerprint: e2:eb:3c:6a:ca:ba:79:2b:00:69:c4:11:ab:ae:02:9c 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 Date: Sun, 22 Oct 2023 00:45:36 GMT Server: Apache/2.4.41 (Ubuntu) Set-Cookie: PHPSESSID=0e2k86j9hcqp7ig11bh2jdgphj; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Content-Length: 3347 Content-Type: text/html; charset=UTF-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.252.244.62']

Name

gstatic-service.io

Pattern Type

stix

Pattern

[domain-name:value = 'gstatic-service.io']

Name

5e4e078a71f6247b9e7c4569ec90a7ddec5f7bece465fc0c177587d920cd5aac

Description

Employee Contract_14212.html

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e4e078a71f6247b9e7c4569ec90a7ddec5f7bece465fc0c177587d920cd5aac']

Name

scandimyth.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'scandimyth.xyz']

Name

lumma.online

Pattern Type

stix

Pattern

[domain-name:value = 'lumma.online']

Name

liveswords.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'liveswords.xyz']

Name

18866-32530.bacloud.info

Pattern Type

stix

Pattern

[hostname:value = '18866-32530.bacloud.info']

Name

23.254.225.133

Description

CC=US ASN=AS54290 HOSTWINDS

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.254.225.133']

Name

168.119.4.83

Description

CC=DE ASN=AS24940 Hetzner Online GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '168.119.4.83']

Name

144.76.173.247

Description

CC=DE ASN=AS24940 Hetzner Online GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '144.76.173.247']

Name

brockerby.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'brockerby.xyz']

Name

212.113.116.46

Description

CC=DE ASN=AS210644 Aeza International Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.113.116.46']

Name

109.105.198.114

Description

CC=ES ASN=AS211826 Istqrar for Servers Services Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.105.198.114']

Name

170.130.55.129

Description

ISP: Eonix Corporation **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '170.130.55.129']

Name

78.46.190.160

Description

CC=DE ASN=AS24940 Hetzner Online GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '78.46.190.160']

Name

fireworld.fun

Pattern Type

stix

Pattern

[domain-name:value = 'fireworld.fun']

Name

followertv.fun

Pattern Type

stix

Pattern

[domain-name:value = 'followertv.fun']

Name

179.248.90.157

Description

CC=BR ASN=AS26615 TIM SA

Pattern Type

stix

Pattern

[ipv4-addr:value = '179.248.90.157']

Name

coldwinded.fun

Pattern Type

stix

Pattern

[domain-name:value = 'coldwinded.fun']

Name

185.99.132.51

Description

CC=NZ ASN=AS61138 Zappie Host LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.99.132.51']

Name

markuschop.fun

Pattern Type

stix

Pattern

[domain-name:value = 'markuschop.fun']

Name

94.158.244.69

Description

CC=US ASN=AS39798 MivoCloud SRL

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.158.244.69']

Name

sisadmin-my.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'sisadmin-my.xyz']

Name

gstatic-node.io

Description

Win32/Lumma

Pattern Type

stix

Pattern

[domain-name:value = 'gstatic-node.io']

Name

static.247.173.76.144.clients.your-serve.de

Pattern Type

stix

Pattern

[hostname:value = 'static.247.173.76.144.clients.your-serve.de']

Name

192.236.233.253

Description

CC=US ASN=AS54290 HOSTWINDS

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.236.233.253']

Name

1377f22be21e2ae441b97eb6323198f963cfa0e246de83f00631cf6e9ba279e8

Description

doberman.min.js

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1377f22be21e2ae441b97eb6323198f963cfa0e246de83f00631cf6e9ba279e8']

Name

45.8.146.130

Description

CC=US ASN=AS44477 Stark Industries Solutions Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.8.146.130']

Name

217.25.91.15

Description

ISP: Artnet Sp. z o.o. **OS:** None ---------- Hostnames: - 1179229-cd76916.tw1.ru ---------- Domains: - tw1.ru ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDRyiteml7dpRMh2wvQpbZOU6fRqYezvfGSawszJ6mzqkqu F6hM/BxeMnM8MfMt17eSbHPjC56BJ0LCcZDfJJ+faBlAEfpeOt8Ny0lu7riVTFzu1eX1g3swQTfdv7D21MQC/lilmaiSQytZVC+MD7aoGCsjoQgojptYFtYQLq8S9E56OwRgmCv+/ZZ3gvFLVrf9Goe5tESwnW7/V9yg5xAs9eaWZrR+RQ4AfbuV79lnWm0gh2F0l9AjvwhFdw1l/nfI5m43aH9RNEkqZDWH qZIp8RUSo6lKsfu3rRW9y1STgFVbGaYFV0W0JpuwQ9mB3rTfi8D8Ud/xsorm8I7BwI+VV9VKk5CC LuJ1um4rypmmEqkppiuSEe6XKJAeeGIphz1hc8miYRohfJ1AYQ/3ye98QR5BkZoWzZ3JwRG5pEyD PFbUyMEilyFGBzalnxfOIOpz/Ut+1i+e82X6ldNXCsDXX7U08zZ2dj1YGjhrVuV26oCtQCFuyaay T07/N/9t7kk= Fingerprint: 16:c4:31:bb:a9:90:c0:d6:b0:c9:64:34:0d:cd:25:4f 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: Mon, 23 Oct 2023 22:22:24 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Fri, 06 Jan

2023 18:13:19 GMT Connection: keep-alive ETag: "63b864bf-264" Accept-Ranges: bytes ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.25.91.15']

Name

lumma.site

Pattern Type

stix

Pattern

[domain-name:value = 'lumma.site']

Name

titanaquaplus.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'titanaquaplus.xyz']

Name

5.161.155.121

Description

CC=US ASN=AS213230 Hetzner Online GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.161.155.121']

Name

94.142.138.26

Description

CC=RU ASN=AS211409 Shelter LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.142.138.26']

Name

dedoxtrone.fun

Pattern Type

stix

Pattern

[domain-name:value = 'dedoxtrone.fun']

Name

evetesttech.net

Pattern Type

stix

Pattern

[domain-name:value = 'evetesttech.net']

Name

82.117.255.80

Description

CC=RO ASN=AS204957 Green Floid LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '82.117.255.80']

Name
fartyfun.fun
Pattern Type
stix
Pattern
[domain-name:value = 'fartyfun.fun']
Name
45.9.74.78
Description
CC=SC ASN=AS204603 Aeza Group LLC
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.9.74.78']
Name
doggyguffy.fun
Pattern Type
stix

Pattern
[domain-name:value = 'doggyguffy.fun']
Name
oneinformationcrypto.com
Pattern Type
stix
Pattern
[domain-name:value = 'oneinformationcrypto.com']

Country

Name
Ukraine

Malware

Name
Lumma

Name
SmokeLoader

Domain-Name

Value
seobrokerstv.fun
sisadmin-my.xyz
oneinformationcrypto.com
gstatic-service.io
lumma.site
dedoxtrone.fun
stateinfospace.com
stoptme.xyz
scandimyth.xyz
coldwinded.fun
fireworld.fun
brockerby.xyz
titanaquaplus.xyz

treepledeeple.fun
fartyfun.fun
liveswords.xyz
follovertv.fun
funnycox.fun
lumma.online
shoppervik.fun
gstatic-node.io
evetesttech.net
astrolco.fun
doggyguffy.fun
markuschop.fun
castomdroms.xyz

StixFile

Value
33202cbfa6e4767b63f4dd9eb5b653d32761aa80f0ee11eaba822e0f444f3ad7
587c5f89248035fe563f06a8b991f081418e6013cc0e77f9e052de59b758c1c1
5e4e078a71f6247b9e7c4569ec90a7ddec5f7bece465fc0c177587d920cd5aac
dd5b52a63e8a774c058e558aa7e983d6aa51f560ba3f01829287c4b85081b884
5798de760b193a06cd9cb1c197feae081e2cff84ba5514a53ad313341b95663e
1377f22be21e2ae441b97eb6323198f963cfa0e246de83f00631cf6e9ba279e8
772d84d31e0a10a6dc6b7bb9bc2f71e135260e95a79e18b2145d53f678639232

Hostname

Value
static.247.173.76.144.clients.your-serve.de
cs6.csserv.ru
18866-32530.bacloud.info

IPv4-Addr

Value
217.25.91.15
94.158.244.69
95.163.238.17
82.117.255.80
209.141.42.26
213.252.244.62
45.8.146.130
78.46.190.160
77.73.134.68
195.123.227.138
94.142.138.26
185.99.132.51
45.8.146.213

85.239.62.218
82.117.255.127
157.90.248.179
170.130.55.129
168.119.4.83
217.12.206.197
82.117.255.128
77.73.134.51
45.8.146.227
5.161.155.121
109.105.198.114
192.236.233.253
144.76.173.247
212.113.116.46
23.254.225.133
179.248.90.157
121.155.161.5
45.9.74.78

82.118.23.50

External References

- https://otx.alienvault.com/pulse/6531428c62ae987b76cc3191
- https://www.intrinsec.com/wp-content/uploads/2023/10/TLP-CLEAR-Lumma-Stealer-EN-Information-report.pdf