Oct 03 2023

NETMANAGEIT

Intelligence Report

Silent Push maps over 150 new Lumma C2 infostealer IOCs

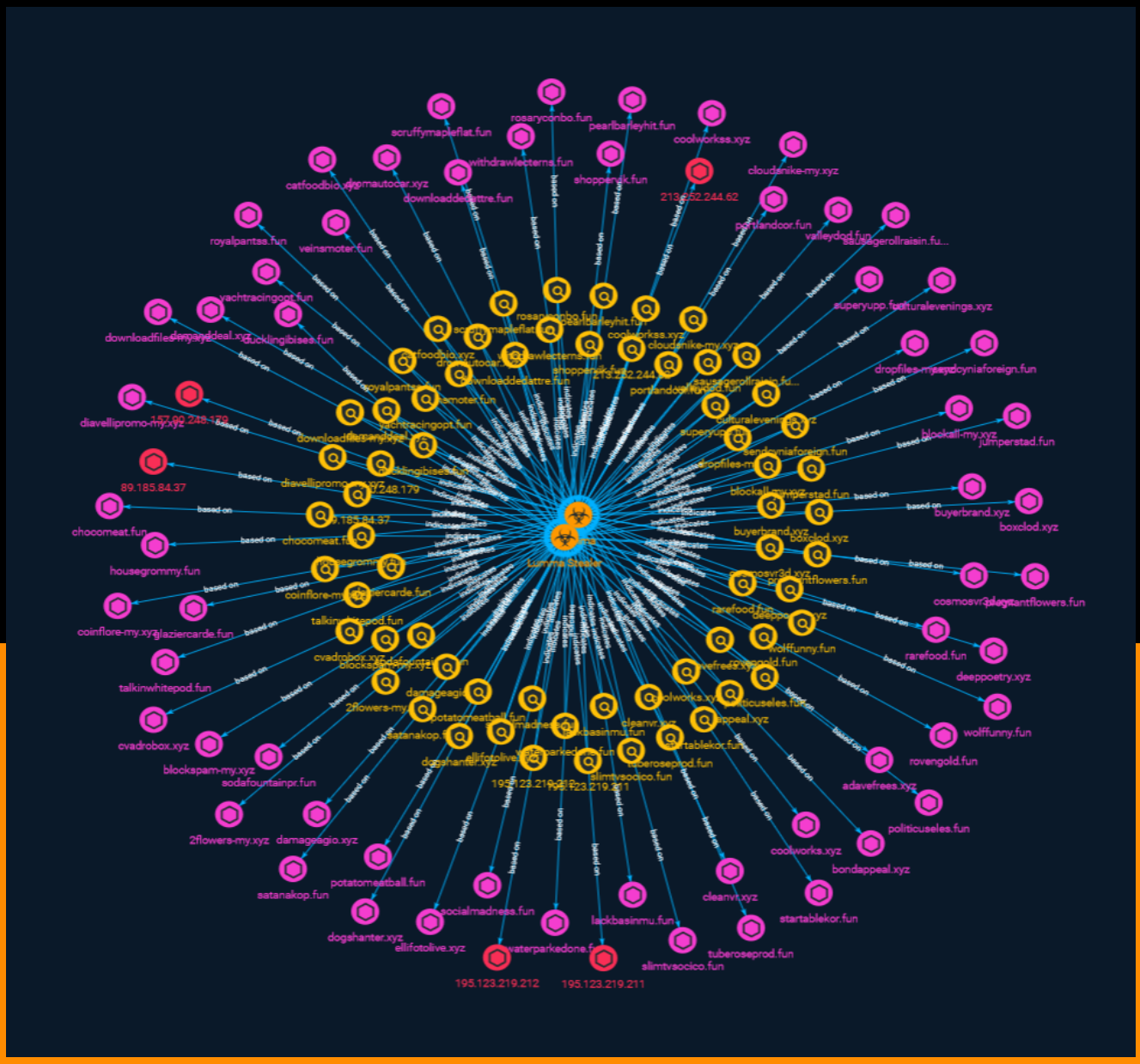

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Silent Push published a new blog regarding Lumma stealer. Lumma (also known as LummaC2) is an information stealer with strong links to Russian threat activity, that's been available on the dark web as a MaaS platform since 2022.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
blockspam-my.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'blockspam-my.xyz']
Name
talkinwhitepod.fun
Pattern Type
stix
Pattern
[domain-name:value = 'talkinwhitepod.fun']
Name
sausagerollraisin.fun

Pattern Type
stix
Pattern
[domain-name:value = 'sausagerollraisin.fun']
Name
sodafountainpr.fun
Pattern Type
stix
Pattern
[domain-name:value = 'sodafountainpr.fun']
Name
dropfiles-my.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'dropfiles-my.xyz']
Name
pregnantflowers.fun

Pattern Type
stix
Pattern
[domain-name:value = 'pregnantflowers.fun']
Name
157.90.248.179
Pattern Type
stix
Pattern
[ipv4-addr:value = '157.90.248.179']
Name
buyerbrand.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'buyerbrand.xyz']
Name
portlandcor.fun

Pattern Type
stix
Pattern
[domain-name:value = 'portlandcor.fun']
Name
slimtvsocico.fun
Pattern Type
stix
Pattern
[domain-name:value = 'slimtvsocico.fun']
Name
shoppervik.fun
Pattern Type
stix
Pattern
[domain-name:value = 'shoppervik.fun']
Name
superyupp.fun

Pattern Type
stix
Pattern
[domain-name:value = 'superyupp.fun']
Name
coinflore-my.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'coinflore-my.xyz']
Name
veinsmoter.fun
Pattern Type
stix
Pattern
[domain-name:value = 'veinsmoter.fun']
Name
195.123.219.212

Pattern Type
stix
Pattern
[ipv4-addr:value = '195.123.219.212']
Name
2flowers-my.xyz
Pattern Type
stix
Pattern
[domain-name:value = '2flowers-my.xyz']
Name
jumperstad.fun
Pattern Type
stix
Pattern
[domain-name:value = 'jumperstad.fun']
Name
cloudsnike-my.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'cloudsnike-my.xyz']
Name
coolworkss.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'coolworkss.xyz']
Name
damageagio.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'damageagio.xyz']
Name
89.185.84.37

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.185.84.37']

Name

195.123.219.211

Description

ISP: ITL LLC **OS:** None ---------- Hostnames: - private-cloud-server.pro ---------- Domains: - private-cloud-server.pro ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAvXiwujKjgNpqTtlMlKmjeruKIWWyy5JsXFAuFVTncYW706ZFKCjBesrhGj4ipqTE4adPTcH4wHh6Malf+tuWk= Fingerprint: fd:1b:2b:68:7e:9e:f1:93:9d:d2:2c:bc:c8:d0:de:26 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 26 Sep 2023 14:06:13 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Sat, 01 Jul 2023 17:37:18 GMT ETag: "a11-5ff70628ae61f" Accept-Ranges: bytes Content-Length: 2577 Vary: Accept-Encoding Content-Type: text/html ``` ----------

Pattern Type

stix

Pattern
[ipv4-addr:value = '195.123.219.211']
Name
satanakop.fun
Pattern Type
stix
Pattern
[domain-name:value = 'satanakop.fun']
Name
royalpantss.fun
Pattern Type
stix
Pattern
[domain-name:value = 'royalpantss.fun']
Name
adavefrees.xyz
Pattern Type
stix

Pattern

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

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: Mon, 02 Oct 2023 13:32:08 GMT Server: Apache/2.4.41 (Ubuntu) Set-Cookie: PHPSESSID=i1e5mhtib3b38l6va05ld5jn60; 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

sendcyniaforeign.fun

Pattern Type

stix

Pattern

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

Name

blockall-my.xyz

Pattern Type

stix

Pattern

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

Name

rosaryconbo.fun

Pattern Type

stix

Pattern
[domain-name:value = 'rosaryconbo.fun']
Name
boxclod.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'boxclod.xyz']
Name
potatomeatball.fun
Pattern Type
stix
Pattern
[domain-name:value = 'potatomeatball.fun']
Name
glaziercarde.fun
Pattern Type
stix

Pattern

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

Name

rarefood.fun

Pattern Type

stix

Pattern

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

Name

downloadfiles-my.xyz

Pattern Type

stix

Pattern

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

Name

cleanvr.xyz

Pattern Type

stix

Pattern
[domain-name:value = 'cleanvr.xyz']
Name
ducklingibises.fun
Pattern Type
stix
Pattern
[domain-name:value = 'ducklingibises.fun']
Name
valleydod.fun
Pattern Type
stix
Pattern
[domain-name:value = 'valleydod.fun']
Name
tuberoseprod.fun
Pattern Type
stix

Pattern
[domain-name:value = 'tuberoseprod.fun']
Name
downloaddedattre.fun
Pattern Type
stix
Pattern
[domain-name:value = 'downloaddedattre.fun']
Name
pearlbarleyhit.fun
Pattern Type
stix
Pattern
[domain-name:value = 'pearlbarleyhit.fun']
Name
waterparkedone.fun
Pattern Type
stix

Pattern
[domain-name:value = 'waterparkedone.fun']
Name
dromautocar.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'dromautocar.xyz']
Name
lackbasinmu.fun
Pattern Type
stix
Pattern
[domain-name:value = 'lackbasinmu.fun']
Name
cvadrobox.xyz
Pattern Type
stix

Pattern
[domain-name:value = 'cvadrobox.xyz']
Name
withdrawlecterns.fun
Pattern Type
stix
Pattern
[domain-name:value = 'withdrawlecterns.fun']
Name
deeppoetry.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'deeppoetry.xyz']
Name
diavellipromo-my.xyz
Pattern Type
stix

Pattern

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

Name

rovengold.fun

Pattern Type

stix

Pattern

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

Name

socialmadness.fun

Pattern Type

stix

Pattern

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

Name

housegrommy.fun

Pattern Type

stix

Pattern

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

Name

bondappeal.xyz

Pattern Type

stix

Pattern

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

Name

demanddeal.xyz

Pattern Type

stix

Pattern

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

Name

coolworks.xyz

Pattern Type

stix

Pattern
[domain-name:value = 'coolworks.xyz']
Name
cosmosvr3d.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'cosmosvr3d.xyz']
Name
chocomeat.fun
Pattern Type
stix
Pattern
[domain-name:value = 'chocomeat.fun']
Name
wolffunny.fun
Pattern Type
stix

Pattern

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

Name

dogshanter.xyz

Pattern Type

stix

Pattern

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

Name

yachtracingopt.fun

Pattern Type

stix

Pattern

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

Name

startablekor.fun

Pattern Type

stix

Pattern

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

Name

catfoodbio.xyz

Pattern Type

stix

Pattern

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

Name

culturalevenings.xyz

Pattern Type

stix

Pattern

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

Name

ellifotolive.xyz

Pattern Type

stix

Pattern
[domain-name:value = 'ellifotolive.xyz']
Name
scruffymapleflat.fun
Pattern Type
stix
Pattern
[domain-name:value = 'scruffymapleflat.fun']
Name
politicuseles.fun
Pattern Type
stix
Pattern
[domain-name:value = 'politicuseles.fun']

Malware

Name
lumma

Name
Lumma Stealer

Domain-Name

Value
coinflore-my.xyz
cloudsnike-my.xyz
socialmadness.fun
dromautocar.xyz
sendcyniaforeign.fun
glaziercarde.fun
rosaryconbo.fun
slimtvsocico.fun
chocomeat.fun
catfoodbio.xyz
yachtracingopt.fun
veinsmoter.fun
valleydod.fun

sodafountainpr.fun

demanddeal.xyz

bondappeal.xyz

lackbasinmu.fun

dropfiles-my.xyz

2flowers-my.xyz

rarefood.fun

pregnantflowers.fun

cvadrobox.xyz

deeppoetry.xyz

coolworks.xyz

downloadfiles-my.xyz

boxclod.xyz

ellifotolive.xyz

culturalevenings.xyz

politicuseles.fun

royalpantss.fun

ducklingibises.fun

satanakop.fun

portlandcor.fun

adavefrees.xyz

blockspam-my.xyz

cosmosvr3d.xyz

tuberoseprod.fun

withdrawlecterns.fun

blockall-my.xyz

waterparkedone.fun

superyupp.fun

potatomeatball.fun

talkinwhitepod.fun

jumperstad.fun

rovengold.fun

pearlbarleyhit.fun

buyerbrand.xyz

housegrommy.fun

shoppervik.fun

startablekor.fun
scruffymapleflat.fun
downloaddedattre.fun
cleanvr.xyz
coolworkss.xyz
wolffunny.fun
damageagio.xyz
sausagerollraisin.fun
dogshanter.xyz
diavellipromo-my.xyz

IPv4-Addr

Value
213.252.244.62
195.123.219.211
157.90.248.179
195.123.219.212
89.185.84.37

External References

- https://otx.alienvault.com/pulse/651ae4a4171e2bdcd776a3df
- https://www.silentpush.com/blog/lummac2