Illuminating Lumma Stealer DNS Facts and Findings

Table of Contents

Executive Report

The Lumma Stealer, known for using the malware-as-a-service (MaaS) model, has figured in various campaigns targeting victims in countries like Argentina, Colombia, the U.S., the Philippines, and others since 2022.

Netskope Threat Labs analyzed a new campaign using fake CAPTCHAs to deliver the stealer and published their findings in "Lumma Stealer: Fake CAPTCHAs and New Techniques to Evade Detection." They identified 34 indicators of compromise (IoCs) in the process comprising 27 domains and seven subdomains.

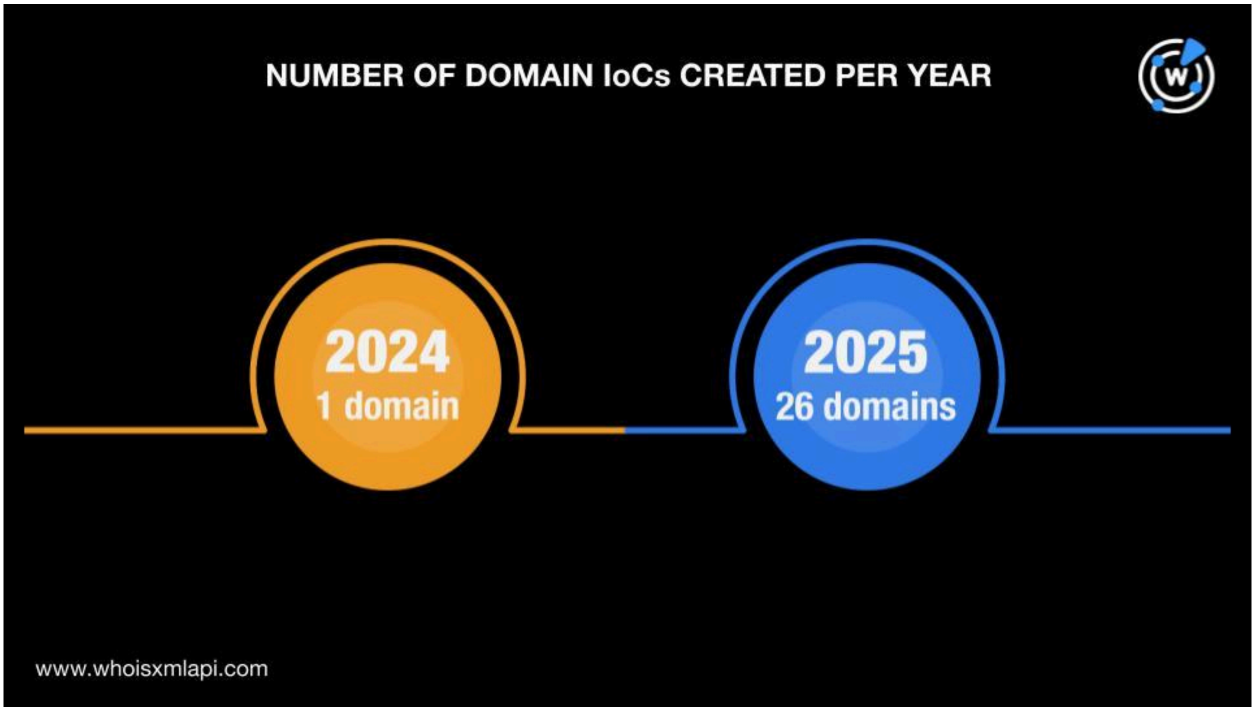
The WhoisXML API research team expanded the list of IoCs Netskope identified and uncovered:

- 25 IP addresses, 23 of which turned out to be malicious
- 228 string-connected domains, 18 of which have already been tagged as malicious
- 477 string-connected subdomains, two of which turned out to have already figured in malicious campaigns

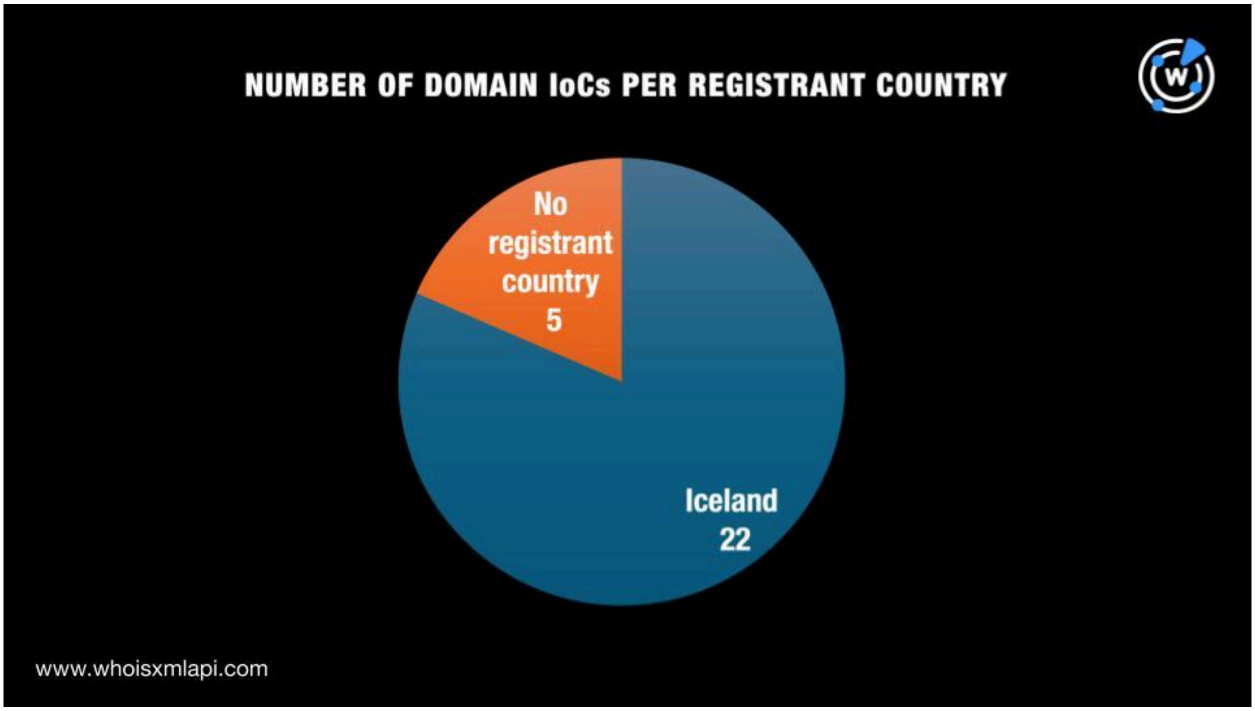
Facts about the Lumma IoCs

We kicked off our in-depth analysis by querying the 27 domains tagged as IoCs on Bulk WHOIS API. The results showed that:

- They were created between 2024 and 2025. Specifically, one domain was created in 2024 while the remaining 26 were created in 2025.



- They were all registered with Namecheap.
- A majority of them, 22 to be exact, were registered in Iceland while the remaining five did not have registrant country information in their current WHOIS records.



Next, we queried the 27 domains identified as IoCs on DNS Chronicle API and discovered that only 26 recorded historical IP resolutions. Altogether, the 26 domains had 342 IP resolutions to date. The domain royaltyfree[.]pics had the oldest initial IP resolution date—10 October 2019. Take a look at the DNS histories of five other domains below.

DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
bestinthemarket[.]com	63	11 June 2020
dokedok[.]shop	4	16 January 2025
gustavu[.]shop	8	19 January 2025
luxeorbit[.]shop	14	14 January 2025
rezomof[.]shop	6	17 January 2025

Lumma IoC List Expansion Findings

To uncover possibly connected artifacts, we began by querying the 27 domains tagged as IoCs on WHOIS History API. The results revealed that six of them had 17 email addresses in their historical WHOIS records after duplicates were filtered out. A closer look at the 17 email addresses after duplicates were filtered out showed that four were public email addresses.

Next, we queried the four public email addresses on Reverse WHOIS API in hopes of uncovering email-connected domains. Unfortunately, none of them appeared in the current WHOIS records of other domains.

After that, we queried the 27 domains identified as IoCs on DNS Lookup API and found that 12 of them resolved to 25 IP addresses after duplicates were filtered out.

A Threat Intelligence API query for the 25 IP addresses revealed that 23 have already figured in various malicious campaigns. Here are five examples.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]112[.]1	Attack Command and control (C&C) Generic threat Phishing Suspicious activity

	Malware distribution
104[.]21[.]48[.]1	Attack C&C Generic threat Phishing Suspicious activity Malware distribution
104[.]21[.]79[.]100	Malware distribution
172[.]67[.]136[.]25	Malware distribution Suspicious activity
172[.]67[.]202[.]216	Generic threat Malware distribution Phishing

We then queried the 25 IP addresses on Bulk IP Geolocation Lookup and discovered that all of them were geolocated in the U.S. and administered by Cloudflare.

Next, we attempted to look for IP-connected domains by querying the 25 IP addresses on Reverse IP API. While all of them resolved domains, none seem to be dedicated, halting our search, as shared infrastructures typically contain many false positives.

After that, we searched for domains that started with the text strings found in the 27 domains identified as IoCs using Domains & Subdomains Discovery. Only these 19 strings appeared in other domains:

- bestinthemarket.
- celebrationshub.
- crystaltreasures.
- dokedok.
- edidos.
- espiano.
- googlsearchings.
- gustavu.
- iconcart.
- jazmina.
- joopshoop.
- luxeorbit.
- milta.
- norpor.
- oliveroh.
- retrosome.
- royaltyfree.
- sharethewebs.
- towercrash.

Specifically, the 19 text strings also appeared at the start of 228 string-connected domains after duplicates and those already tagged as IoCs were filtered out.

A Threat Intelligence API query for the 228 string-connected domains showed that 18 have already been weaponized for various campaigns. Take a look at five examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREATS
googlsearchings[.]art	Generic threat Malware distribution
googlsearchings[.]quest	Generic threat Malware distribution
googlsearchings[.]site	Generic threat Malware distribution
royaltyfree[.]cfd	Generic threat Malware distribution
royaltyfree[.]online	Generic threat Malware distribution

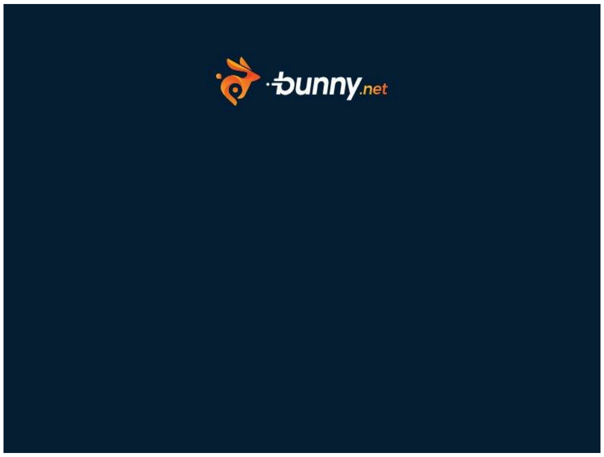
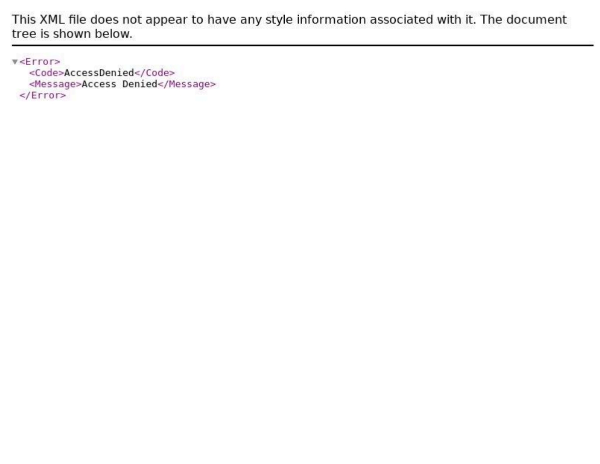
Our search for string-connected web properties did not end there, though. We also looked for subdomains that started with text strings found in the seven subdomains identified as IoCs. We uncovered subdomains that started with these five strings:

- bazaar.
- sos-at-
- sos-bg-
- sos-ch-
- sos-de-

In particular, we uncovered 477 string-connected subdomains after duplicates and those already tagged as IoCs were filtered out.

A Threat Intelligence API query for the 477 string-connected subdomains revealed that two of them are already considered malicious. An example would be sos-ch-gva-2-exo-io[.]b-cdn[.]net, which was associated with malware distribution.

Lastly, a Screenshot API query for the two malicious subdomains showed that both remained accessible to date. Take a look at their screenshots below.

	This XML file does not appear to have any style information associated with it. The document tree is shown below. ▼<Error> <Code>AccessDenied</Code> <Message>Access Denied</Message> </Error>
Screenshot of malicious subdomain sos-ch-gva-2-exo-io[.]b-cdn[.]net	**Screenshot of malicious subdomain sos-de-fra-1[.]exo[.]io**

Note that the two malicious subdomains also had the string exo[.]io like six of the subdomains identified as IoCs.

—

Our expansion analysis for the 34 Lumma IoCs (i.e., 27 domains and seven subdomains) led to the discovery of 730 potentially connected artifacts comprising 25 IP addresses, 228 string-connected domains, and 477 string-connected subdomains. Security teams may especially want to be wary of 43 of the artifacts we found as they have already been tagged as malicious to date.

If you wish to learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample IP Addresses

- 104[.]21[.]112[.]1
- 104[.]21[.]16[.]1
- 104[.]21[.]32[.]1
- 104[.]21[.]32[.]202
- 104[.]21[.]45[.]147
- 104[.]21[.]48[.]1
- 104[.]21[.]52[.]184
- 104[.]21[.]58[.]67
- 104[.]21[.]64[.]1
- 104[.]21[.]67[.]12
- 104[.]21[.]79[.]100
- 104[.]21[.]80[.]1

Sample String-Connected Domains

- bestinthemarket[.]online
- bestinthemarket[.]org
- bestinthemarket[.]site
- celebrationshub[.]co[.]in
- celebrationshub[.]com
- celebrationshub[.]in
- celebrationshub[.]net
- celebrationshub[.]top
- crystaltreasures[.]at
- crystaltreasures[.]co
- crystaltreasures[.]co[.]uk
- crystaltreasures[.]com
- crystaltreasures[.]com[.]au
- dokedok[.]com
- dokedok[.]store
- edidos[.]best
- edidos[.]com
- espiano[.]com
- espiano[.]com[.]tw
- espiano[.]de
- espiano[.]es
- espiano[.]eu
- googlsearchings[.]art
- googlsearchings[.]click
- googlsearchings[.]guru
- googlsearchings[.]quest
- googlsearchings[.]sbs
- gustavu[.]com
- gustavu[.]com[.]br
- gustavu[.]store
- iconcart[.]com
- iconcart[.]store
- iconcart[.]tk
- iconcart[.]xyz
- jazmina[.]co[.]uk
- jazmina[.]com
- jazmina[.]com[.]au
- jazmina[.]dk
- jazmina[.]fun
- joopshoop[.]com
- luxeorbit[.]com
- luxeorbit[.]online
- luxeorbit[.]site
- milta[.]africa
- milta[.]at
- milta[.]be
- milta[.]by
- milta[.]cf
- norpor[.]com
- norpor[.]in[.]th
- norpor[.]no
- norpor[.]xyz
- oliveroh[.]com
- retrosome[.]com

- royaltyfree[.]ai
- royaltyfree[.]am
- royaltyfree[.]app
- royaltyfree[.]at
- royaltyfree[.]au
- sharethewebs[.]art
- sharethewebs[.]fun
- sharethewebs[.]online
- sharethewebs[.]ph
- sharethewebs[.]pics
- towercrash[.]com[.]au
- towercrash[.]vg

Sample String-Connected Subdomains

- bazaar[.]0-0000-0000-0000-6855-f960[.]valtaf[.]ad[.]nl
- bazaar[.]0-1107ds1-nks[.]mail[.]shein[.]com
- bazaar[.]001[.]int[.]ad[.]smartnews[.]net
- bazaar[.]0228953[.]wixsite[.]com
- bazaar[.]0c9a81-all-3[.]preview-collector[.]scopely[.]io
- bazaar[.]1-159164-1647925395456-705[.]rt[.]yammer[.]com
- bazaar[.]1-48249364481-272305995777-299[.]rt[.]yammer[.]com
- bazaar[.]1[.]athenacase[.]dns[.]apps[.]dev[.]lifeomic[.]com
- bazaar[.]125560[.]wixsite[.]com
- bazaar[.]15[.]reddit[.]com
- bazaar[.]1766852[.]wixsite[.]com
- bazaar[.]18cailynrose[.]wixsite[.]com
- bazaar[.]19webbchr1[.]wixsite[.]com
- bazaar[.]1ce[.]media-media-simplycomputermerchants[.]wordpress[.]net
- bazaar[.]21677104[.]hs-sites[.]com
- bazaar[.]3047184[.]hs-sites[.]com
- bazaar[.]3cxhysing[.]sip[.]is
- bazaar[.]3liteimage[.]as[.]me
- bazaar[.]4517[.]dev[.]atg[.]se
- bazaar[.]77-164-186-148boardstage3partner77-164-186-149boardstage3-io[.]fixed[.]kpn[.]net
- bazaar[.]788555[.]xrr[.]azurite[.]mobi
- bazaar[.]788555[.]xrr[.]bonsai-tree[.]ch
- bazaar[.]788555[.]xrr[.]tracksoftinc[.]com
- bazaar[.]788555[.]xrr[.]wheatleylaw[.]com
- bazaar[.]91186[.]proxy-http[.]us[.]proxy-http[.]us[.]immersivelabs[.]com
- sos-at-detection-training[.]eventbrite[.]com
- sos-at-powershell-training[.]eventbrite[.]com
- sos-at-redteamops-training[.]eventbrite[.]com
- sos-at-vie-1[.]exoscale-cdn[.]com
- sos-at-vie-1[.]fortnite[.]com
- sos-at-vie-1[.]lodgify[.]com
- sos-at-vie-2[.]exoscale-cdn[.]com
- sos-bg-sof-1[.]exoscale-cdn[.]com
- sos-ch-dk-2[.]bilinfo[.]net
- sos-ch-dk-2[.]cartax[.]com
- sos-ch-dk-2[.]exoscale-cdn[.]com
- sos-ch-dk-2[.]mobilevikings[.]be
- sos-ch-gva-2-exo-io[.]b-cdn[.]net
- sos-ch-gva-2[.]exoscale-cdn[.]com
- sos-ch-gva-2[.]iridium-remsupport[.]ru
- sos-ch-gva-2[.]sos-cdn[.]net
- sos-ch-lsn[.]pixeleez[.]ch
- sos-ch-lsn[.]swissnubes[.]ch
- sos-de-fra-1[.]bilinfo[.]net

- sos-de-fra-1[.]bokundemo[.]com
- sos-de-fra-1[.]exo[.]io
- sos-de-fra-1[.]exoscale-cdn[.]com
- sos-de-fra-1[.]iridium-repair-center[.]ru
- sos-de-fra-1[.]locationrater[.]com
- sos-de-fra-1[.]mixpanel[.]org