Unloading MintsLoader IoCs Using DNS Intelligence

Table of Contents

Executive Report

Several American and European organizations across the energy, oil and gas, and legal sectors were recently targeted by a campaign leveraging MintsLoader, a malware loader that delivers malicious software to a victim's device. To evade detection, MintsLoader employs stealthy techniques, such as domain generation algorithm (DGA), to create new command-and-control (C&C) servers.

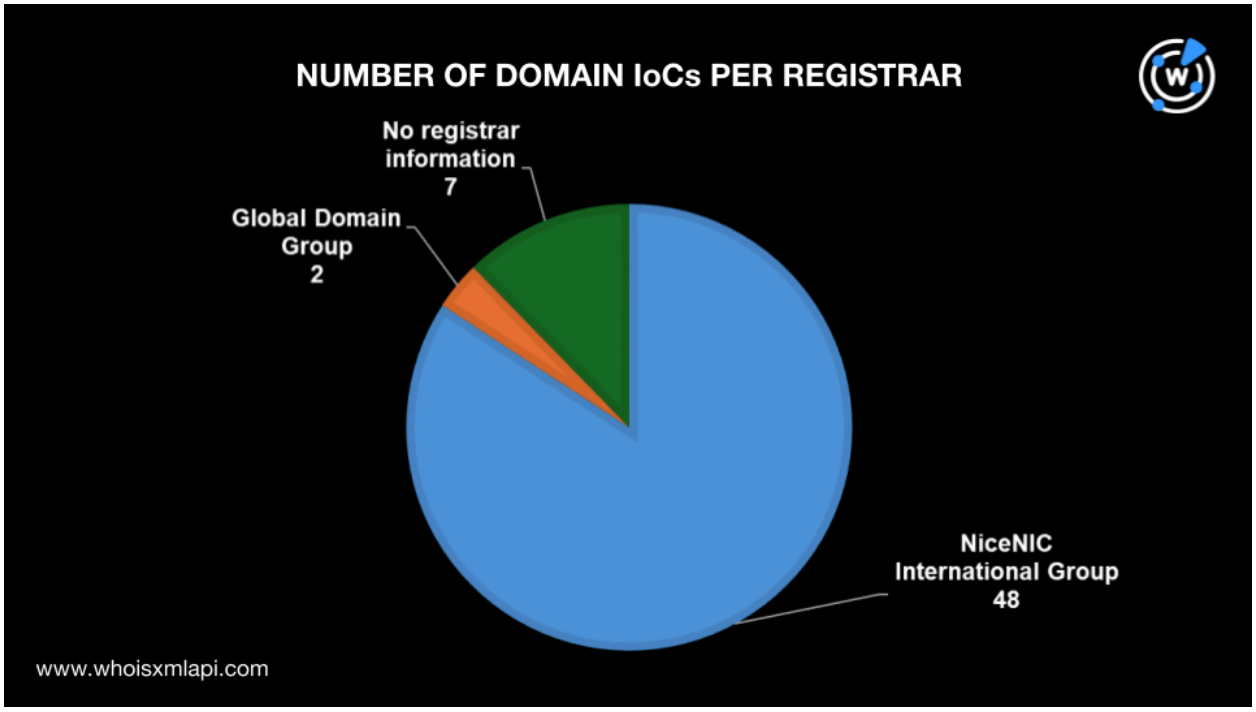
The eSentire Threat Response Unit (TRU) published 61 indicators of compromise (IoCs) involved in the ongoing MintsLoader campaign. The list comprised 57 domain names and four IP addresses, which the WhoisXML API research team analyzed and expanded. By the end of our analysis, we uncovered more threat artifacts, including:

- Two additional IP addresses, one of which turned out to be malicious
- 46 IP-connected domains, 27 of which were malicious
- 142 string-connected domains, 25 of which turned out to be malicious

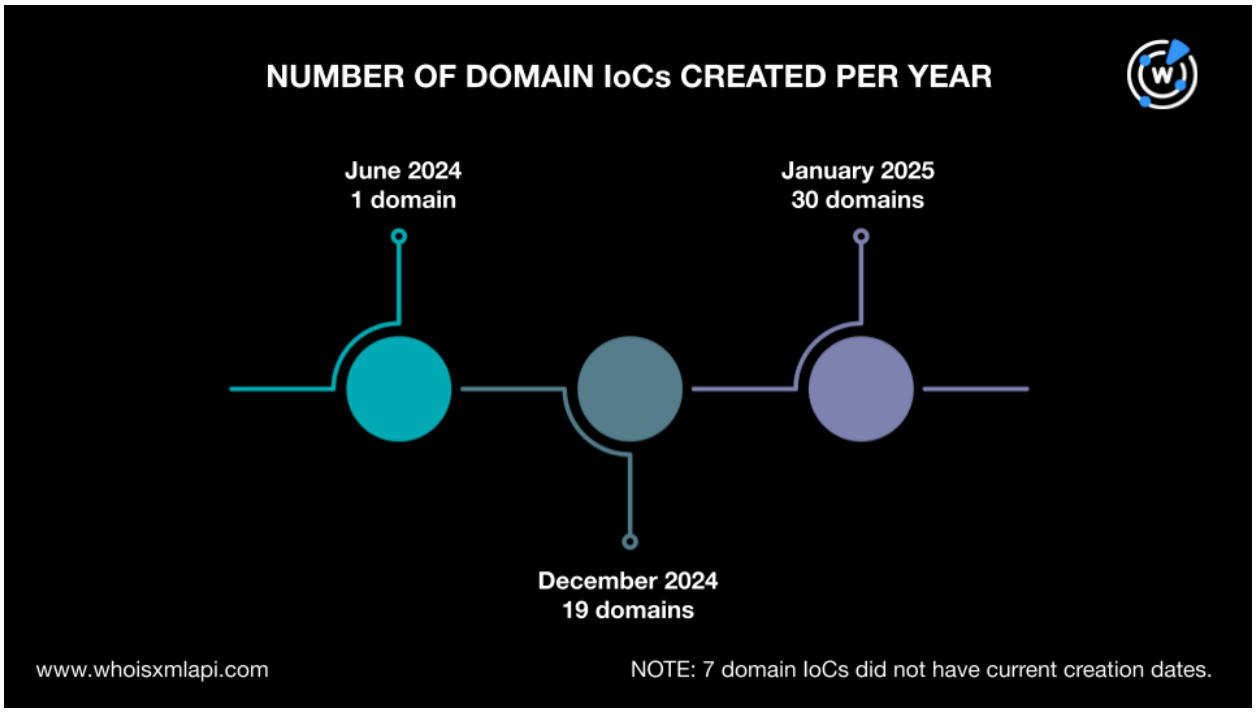
A Closer Look at the IoCs

This part of our investigation aimed to identify the characteristics of the IoCs. To begin, we queried the 57 domains tagged as IoCs on Bulk WHOIS API and found that only 50 had current WHOIS records. Here's a breakdown of their record details.

- A total of 48 domains were administered by NiceNIC International Group, while the other two were under Global Domain Group.



- Almost all of the domain IoCs were created between December 2024 and January 2025. More than half of the domain IoCs, 30 to be exact, were registered in January 2025, 19 were created in December 2024, and one was registered in June 2024. Seven domain IoCs did not have current creation dates.



- All other WHOIS data points, including registrant name, email address, organization, and country, have been redacted for privacy.

A DNS Chronicle API query for the 57 domains tagged as IoCs revealed that only 35 had historical IP resolutions. They collectively posted a total of 94 IP resolutions over time. The IoC xaides[.]com recorded the earliest IP resolution date—26 November 2021. This was a telltale sign that the domain was old and possibly only reregistered on its current WHOIS creation date—2 January 2025. DNS Chronicle API further revealed that the domain IoC immediately resolved to an IP address a few hours after it was reregistered.

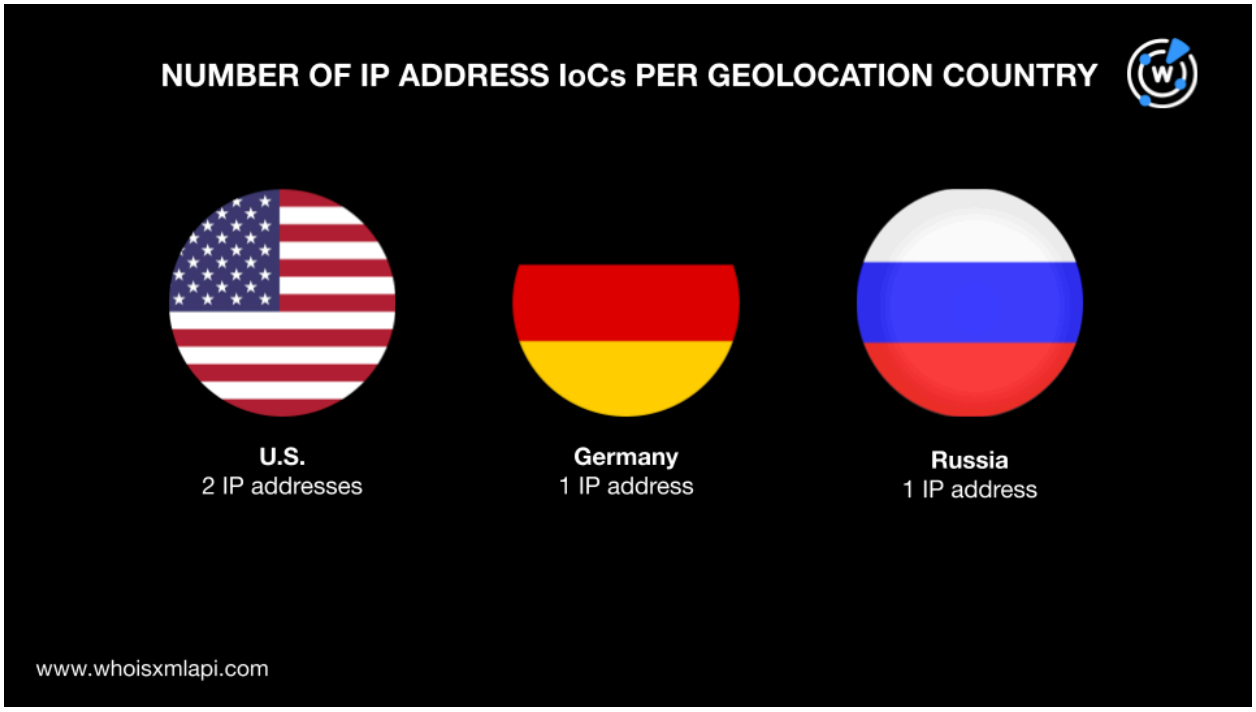
Short mobilization windows between WHOIS creation and IP resolution were common among the other domain IoCs. The table below shows the current total number of IP resolutions, current WHOIS creation dates, and first and last IP resolution dates for five other domain IoCs.

DOMAIN IoC	TOTAL NUMBER OF IP RESOLUTIONS	CURRENT WHOIS CREATION DATE	FIRST IP RESOLUTION DATE	LAST IP RESOLUTION DATE
rosettahome[.]top	20	15 June 2024	16 June 2024	4 February 2025
nfuvueibzi4[.]top	2	3 January 2025	4 January 2025	7 January 2025
sdubvlbbuz3vzzz[.]top	2	19 December 2024	20 December 2024	25 December 2024
hjbamcnnkmfjbld[.]top	2	24 January 2025	24 January 2025	25 January 2025
bidjdlegcnincee[.]top	2	27 January 2025	27 January 2025	28 January 2025

Note that according to eSentire, MintsLoader is an ongoing campaign. Hence, we detected active IP resolutions for the IoCs on the day of the DNS Chronicle API queries.

Our Bulk IP Geolocation Lookup query on the four IP addresses tagged as IoCs revealed that:

- Two IP addresses were geolocated in the U.S., one in Russia, and another in Germany.



- Only one IP address had an ISP on record, namely, Hostinger.

We then queried the four IP addresses on DNS Chronicle API, which revealed that three had historical domain resolutions. Altogether, they posted 113 domain resolutions over time. The IP address 45[.]61[.]136[.]138 recorded the earliest first domain resolution date (i.e., 2 March 2022) and had a total of 79 domain resolutions up until 17 January 2025.

IoC List Expansion Analysis Findings

The next part of our investigation pivoted off the IoCs and the abovementioned characteristics to look for more threat artifacts. As our first step, we queried the 57 domains tagged as IoCs on DNS Lookup API and found that seven actively resolved to two IP addresses after duplicates and those already identified as IoCs were filtered out.

Threat Intelligence API queries for the two additional IP addresses revealed that one of them was malicious, having been associated with malware attacks. A bulk IP geolocation lookup for the two additional IP addresses showed that:

- They were geolocated in the U.S.
- None of them had ISPs on record, similar to most of the IP addresses tagged as IoCs.

We then queried the six IP addresses—four tagged as IoCs and two additional—on Reverse IP API and discovered that five of them could be dedicated hosts while one did not have any domain resolution.

Altogether, the six IP addresses hosted 46 domain names after duplicates and those already identified as IoCs were filtered out. Threat Intelligence API revealed that 27 of the IP-connected domains were already associated with malware campaigns.

We then searched for other domains that contained similar text strings as those tagged as IoCs using Reverse WHOIS Search and Domains & Subdomains Discovery.

Keep in mind that according to eSentire, MintsLoader used DGA-created domains. In particular, they generated 15-character-long domains under the .top TLD. To find similar-looking .top domains, we used Reverse WHOIS Search. We further limited the search to .top domains registered with NiceNIC International Group to avoid as many false positives as possible. We found 105 .top domains whose second-level domains (SLDs) comprised 15 characters and were created from 1 January 2025 onward.

For the non-DGA-created IoCs, we used the following text strings on Domains & Subdomains Discovery:

- rosettahome
- xaides
- usbkits

The strings appeared in 37 other domains after duplicates, those already identified as IoCs, and the IP-connected domains were filtered out. In total, we found 142 string-connected domains.

Threat Intelligence API queries for the string-connected domains showed that 25 have already been tagged as malicious. Specifically, they were associated with malware distribution.

—

Our analysis of the 61 MintsLoader IoCs led to the discovery of 190 connected artifacts comprising two additional IP addresses, 46 IP-connected domains, and 142 string-connected domains. A total of 53 artifacts have already figured in malicious campaigns so far.

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 Additional IP Addresses

- 104[.]238[.]61[.]8

Sample IP-Connected Domains

- z-v2-072974[.]kailib[.]com
- xaides[.]com
- www[.]magicsoulciety[.]com
- www[.]lionofjudahbiblecenter[.]com
- smtp[.]magicsoulciety[.]com
- smtp[.]lionofjudahbiblecenter[.]com
- shd9inbjz4[.]top
- sdubvlbbuz3vzzz[.]top
- rosettahome[.]top
- rosettahome[.]cn
- poubnxu3jubz[.]top
- pop[.]magicsoulciety[.]com
- pop[.]lionofjudahbiblecenter[.]com
- ohunhebzhbu3[.]top
- nuvye89bjz4[.]top
- nubxz4ubhxz9i[.]top
- nhjndjemlimakmk[.]top
- ngub8zb38ib[.]top
- nfuvueibzi4[.]top
- mirugby[.]com

Sample String-Connected Domains

- rosettahomespot[.]club
- rosettahome[.]online
- xaidestnelf[.]tk
- xaidesign[.]tech
- xaidesignsllc[.]com
- xaides[.]info
- xaidesign[.]online
- xaidesign[.]nu
- xaidesk[.]com
- xaidesol[.]ml
- xaidesigns[.]com
- xaidesign[.]eu
- xaidesona[.]ga
- xaides[.]ph
- xaidesoundhahenre[.]tk
- xaidesign[.]se
- xaidesign[.]com
- usbkits[.]co
- idhglmmnaimdhlj[.]top
- anldfaggmdbglen[.]top
- gbkiafbmhbmbkkl[.]top
- nlafhhiffkceadc[.]top
- mdinjlkfcajkjck[.]top
- fnnkcnemajnnaja[.]top
- jjdgdeffjimfgne[.]top
- kvocxcanjnxskwu[.]top
- ikebnbckbjlmfjf[.]top
- nlcjlhcnffdgdgk[.]top

- u9oaqye2mww19fx[.]top
- pqs25br9gmn7d4f[.]top
- nbdh41c4epg7il7[.]top
- l8tuy7wfpnb2zsr[.]top
- ghggfjkgdahjina[.]top
- h06dneez9qmkoeq[.]top
- 1r44zklfp4caq35[.]top
- ghecbjcmdfghfkg[.]top
- pincocasino7777[.]top
- prawam-v-moskve[.]top
- ndkdmkenbjlmmfe[.]top
- fnbagmmgneabdmi[.]top
- lpz28af45yzn4js[.]top
- casino-riobet7y[.]top
- mjflaafmmmeehfm[.]top
- fmnljjmaeihehge[.]top
- dfbkbmbceaafmec[.]top
- ffjihcnfkhihlmd[.]top
- casinosvavada7w[.]top
- vavada-casino7s[.]top
- lbnfbehmicmkceh[.]top
- afnfdijahijefmh[.]top