The Extended Reach of the Extension Trojan Campaign in the DNS

Table of Contents

Executive Report

The ReasonLabs Research Team uncovered a new widespread polymorphic malware campaign that forcefully installed extensions on users' systems. The Trojan comes in various forms ranging from simple adware extensions that hijack searches to more sophisticated malicious scripts that deliver local extensions to steal private data and execute various commands. The Extension Trojan has reportedly already affected at least 300,000 Google Chrome and Microsoft Edge users.

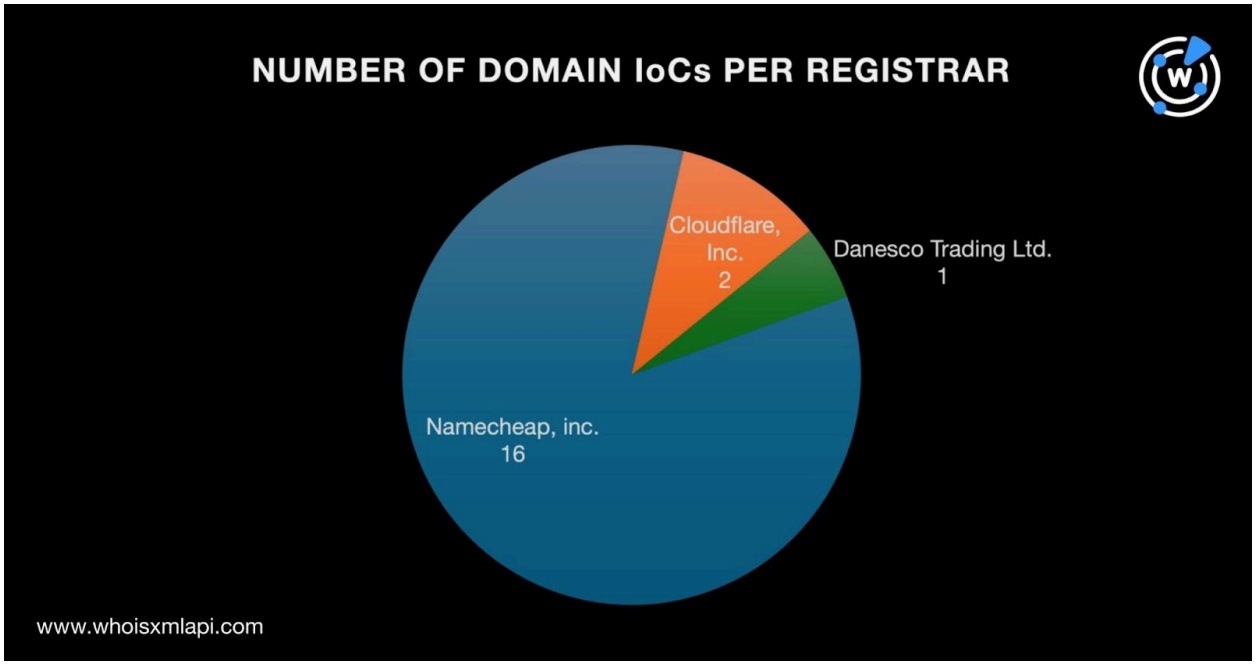
How far does the reach of the Extension Trojan campaign go in the DNS? The WhoisXML API research team sought to find out by expanding a list of 22 domains identified as indicators of compromise (IoCs). Our DNS deep dive led to the discovery of:

- 84 email-connected domains
- 28 IP addresses, //24 of which turned out to be malicious
- 38 string-connected domains

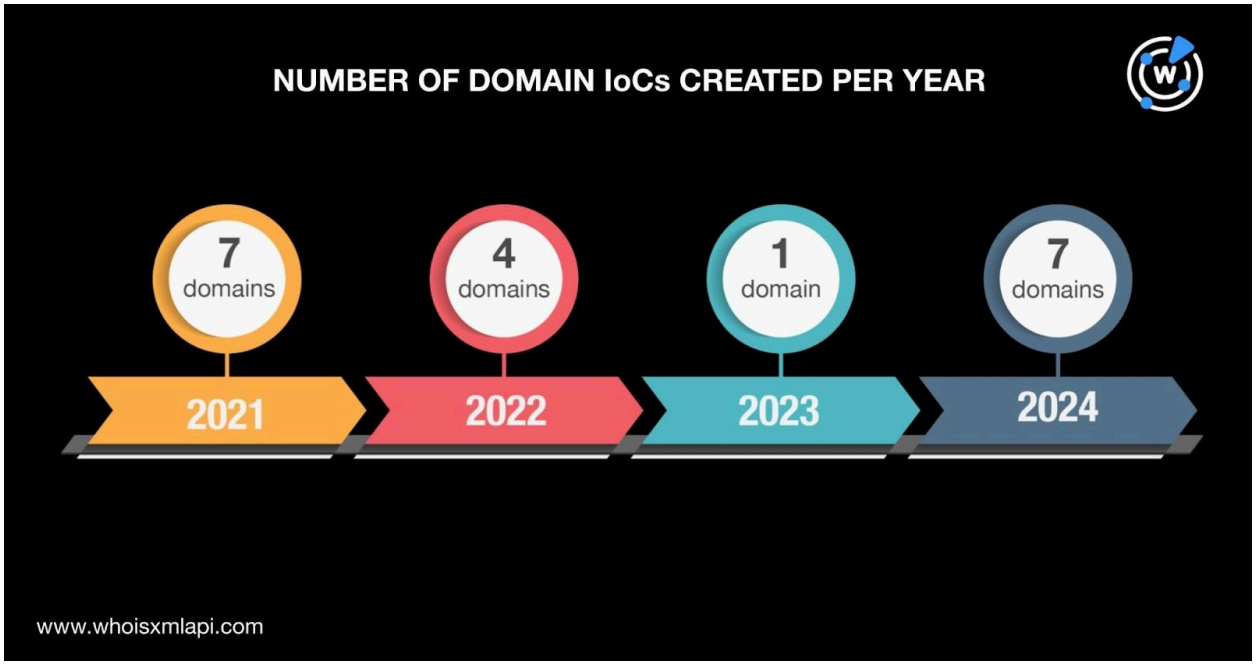
More Information about the IoCs

As per usual, we began our analysis by attempting to know more about the IoCs. We queried the 22 domains tagged as IoCs on Bulk WHOIS Lookup and found that:

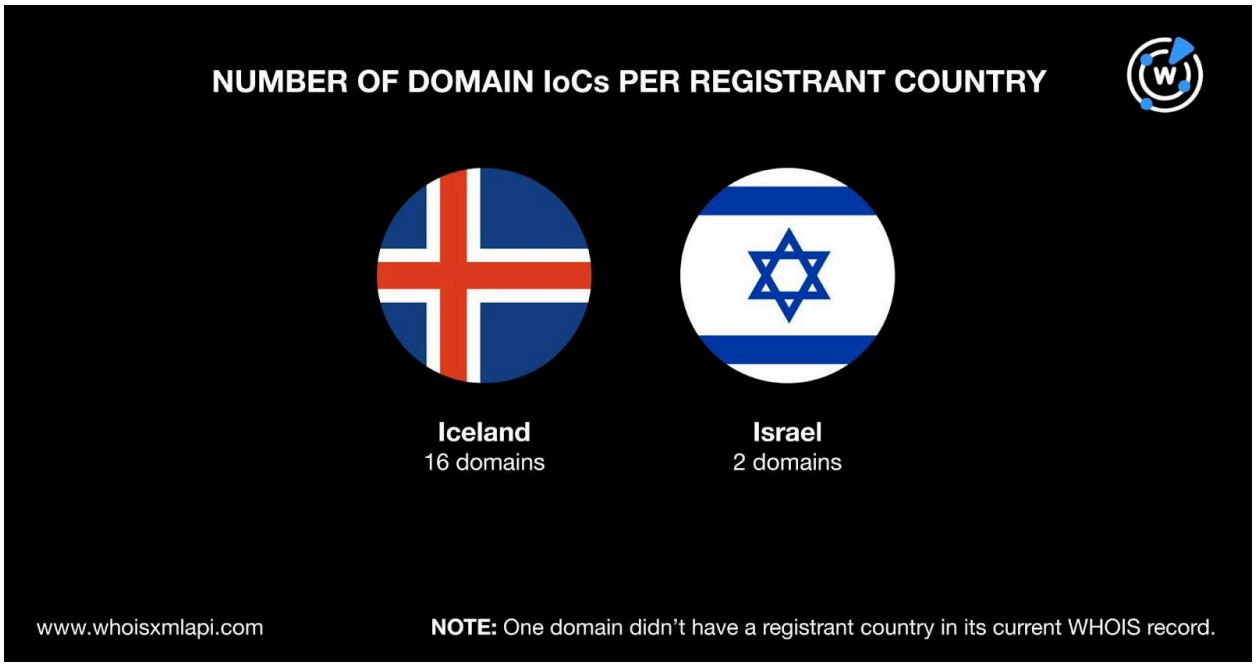
- Only 19 of them had public current WHOIS record data.
- Namecheap, Inc. was the top registrar, accounting for 16 domain IoCs. The three remaining IoCs were split among two other registrars—Cloudflare, Inc. administered two while Danesco Trading Ltd. managed one.



- The threat actors used domains newly registered when they were weaponized starting in 2021 around the time the trojan was first seen. Seven domain IoCs each were created in 2021 and 2024. Four were created in 2022 and one in 2023.



- A majority of the domain IoCs, 16 to be exact, were registered in Iceland. Two were registered in Israel and one didn't have a registrant country in its current WHOIS record.



IoC List Expansion Results

In a bid to find more artifacts possibly connected to the Extension Trojan, we queried the 20 domains identified as IoCs on WHOIS History API. That led to the discovery of 26 email addresses in their historical WHOIS records, four of which were public.

Querying the four public email addresses on Reverse WHOIS API allowed us to uncover 84 email-connected domains after filtering out duplicates and the IoCs.

Next, we subjected the 20 domain IoCs to DNS lookups that provided us with 28 IP addresses. Threat intelligence lookups for them showed that 24 were associated with various threats. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPE
104[.]21[.]3[.]7	Attack Malware Phishing Suspicious
104[.]21[.]17[.]222	Generic Malware Phishing

104[.]21[.]24[.]148	Malware Phishing
172[.]67[.]129[.]252	Attack Malware Phishing Suspicious
104[.]21[.]32[.]227	Attack Generic Phishing

A bulk IP geolocation lookup for the 28 IP addresses revealed that they all shared the same geolocation country (i.e., the U.S.) and ISP (i.e., Cloudflare).

Next, reverse IP lookups for the 28 IP addresses enabled us to determine that they were all shared hosts, apart from being tunneled. Case in point? All of the IP addresses pointed to the U.S. as their origin even if the domain IoCs they hosted were registered in Iceland and Israel.

As the final step in our expansion analysis, we searched the DNS for domains that started with the same text strings as the IoCs using Domains & Subdomains Discovery. Only 15 of the 20 text strings, however, appeared in other domains. After removing duplicates, the IoCs, and the email-connected domains, we were left with 38 string-connected domains.

Are the Most Popular Browser Search Extensions at Risk?

A closer look at the 22 domains identified as IoCs led us to conclude that the threat actors could have specifically targeted browser search extensions for this particular campaign, given that 12 of them contained the text string **search**. That said, we obtained a list of the most popular search browser plug-ins.

We then scoured the DNS for domains that contained the nine brands on the list to see how many already exist and could be weaponized for similar attacks, if they haven't already. We used the following strings as search terms on Domains & Subdomains Discovery:

- **searchthecurrentsite.**
- **wikipediasearch.**
- **wolframalpha.**
- **simplesearch.**
- **tineye.**
- **searchall.**
- **multipletabssearch.**
- **invisiblehand.**
- **giphy.**

We limited our searches to those that fit the parameters **Domains only**, **Starts with**, and **Added since January 1, 2021** since the threat first emerged in 2021. We found 166 branded domains for all strings except one (i.e., **searchthecurrentsite.**).

Based on comparisons with developer details we obtained via web searches, only two of the branded domains could be publicly attributed to the developer of one of the browser extensions (i.e., TinEye). Note that we used the developer's name, company, or the WHOIS record details for their official domain names. Should threat actors get their hands on these web properties, they could weaponize them for attacks riding on the popularity of the search plug-ins.

—

Our IoC list expansion analysis for the Extension Trojan led to the discovery of 150 potentially connected artifacts comprising 84 email-connected domains, 28 IP addresses, and 38 string-connected domains. A total of 86% of the IP addresses also turned out to be malicious.

In relation to browser extension abuse akin to what the Extension Trojan did, we also looked for possible signs of typosquatting in the DNS. We investigated nine of the most used plug-ins and found that the names of eight of them appeared in more than a hundred domains. Also, only 1% of the branded domains could be publicly attributed to the plug-ins' owners. The remaining 99% could thus figure in typosquatting-enabled cyber attacks.

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 Email-Connected Domains

- 7mmwetsuit[.]com
- adultdomainpages[.]com
- adultvoyager[.]com
- allbootycalls[.]com
- arsenallacrosse[.]com
- asiancablenetwork[.]com
- bootlegclips[.]com
- bootycallcity[.]com

- breastimplantscanada[.]com
- broncobeat[.]org
- broncoslacrosse[.]org
- call4prize[.]com
- call4scores[.]com
- citydirectmarketing[.]com
- collegedrinkingames[.]com
- countrywideflorists[.]com
- crowdedcause[.]org
- crowdedcauses[.]org
- deanpickle[.]com
- domainers[.]xxx

Sample IP Addresses

- 104[.]21[.]17[.]222
- 104[.]21[.]24[.]148
- 104[.]21[.]3[.]7
- 104[.]21[.]32[.]227
- 104[.]21[.]41[.]228
- 104[.]21[.]42[.]105
- 104[.]21[.]43[.]9
- 104[.]21[.]46[.]173
- 104[.]21[.]55[.]85
- 104[.]21[.]60[.]226
- 104[.]21[.]61[.]35
- 104[.]21[.]65[.]31
- 104[.]21[.]7[.]213
- 104[.]21[.]9[.]85

Sample String-Connected Domains

- microsearch[.]ae
- microsearch[.]blog
- microsearch[.]ca
- microsearch[.]cloud
- microsearch[.]cn
- search-good[.]ru
- search-good[.]tk
- simplenewtab[.]info
- simplenewtab[.]xyz
- sslwindows[.]be
- sslwindows[.]tk
- yoursearchbar[.]com