A DNS Investigation of the Phobos Ransomware 8Base Attack

circleid.com/posts/20240530-a-dns-investigation-of-the-phobos-ransomware-8base-attack

By **WhoisXML API** (Sponsored Post) A Domain Research, Whois, DNS, and Threat Intelligence API and Data Provider

- May 30, 2024
- Views: 4,478

Intel-Ops researchers recently discovered that the 8Base Ransomware Group has been using Phobos ransomware to infect their targets' networks. 8Base has reportedly been active since mid-2023.

The Phobos operators have been selling the ransomware's multiple variants (e.g., Eking, Eight, Elbie, Devos and Faust) via the ransomware-as-a-service (RaaS) model. In the past, various groups utilized the ransomware to infect several targets, including county governments, emergency service providers, educational institutions, public healthcare service providers, and other critical infrastructure entities, successfully collecting ransom amounting to millions of U.S. dollars.

Sixty-three indicators of compromise (IoCs) comprising 46 domains and 17 IP addresses were made public in relation to the 8Base Phobos ransomware attack featured in this post. The WhoisXML API research team expanded the IoC list in a bid to find other potentially connected artifacts and uncovered:

- 368 email-connected domains
- Three additional IP addresses, one of which is already tagged as malicious
- 13 IP-connected domains

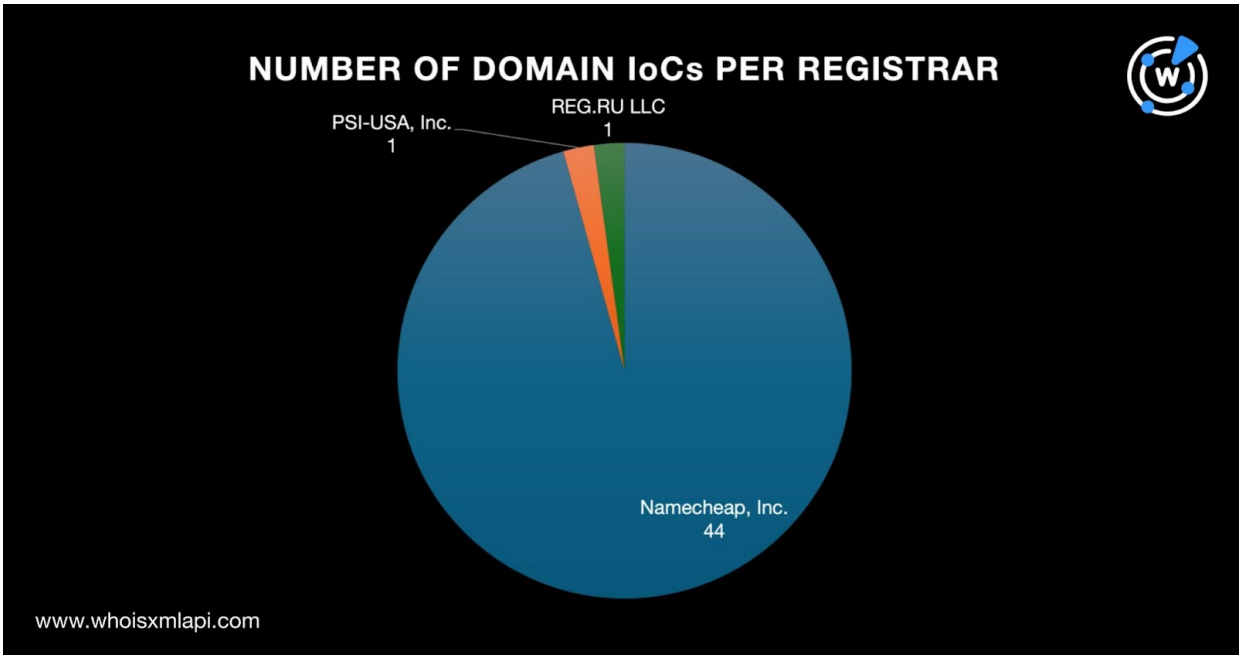
- 20 string-connected domains

A sample of the additional artifacts obtained from our analysis is available for download from our website.

Behind the 8Base Phobos Ransomware Attack IoCs

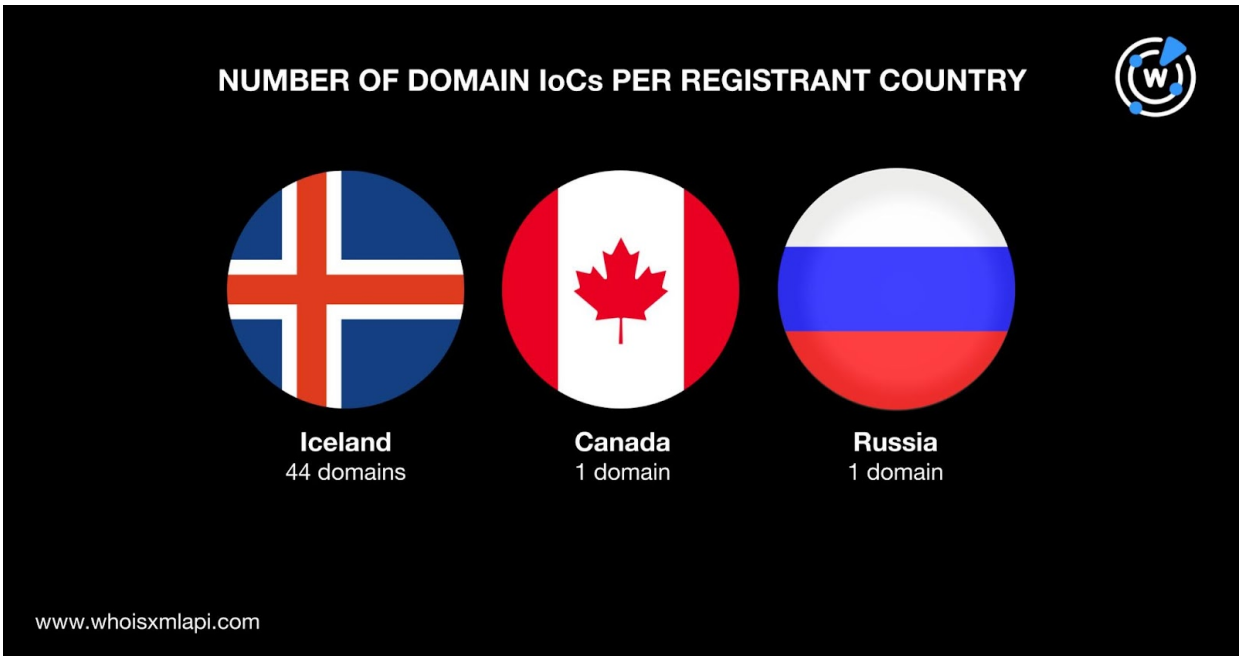
As per usual, we sought to find more information about the 63 IoCs. We began by subjecting the 46 domains identified as IoCs to a bulk WHOIS lookup, which revealed that:

- The domain IoCs were spread across three registrars. A huge chunk of them, 44 to be exact, were registered with Namecheap, Inc. One domain IoC each was registered with PSI-USA, Inc. and REG.RU LLC.



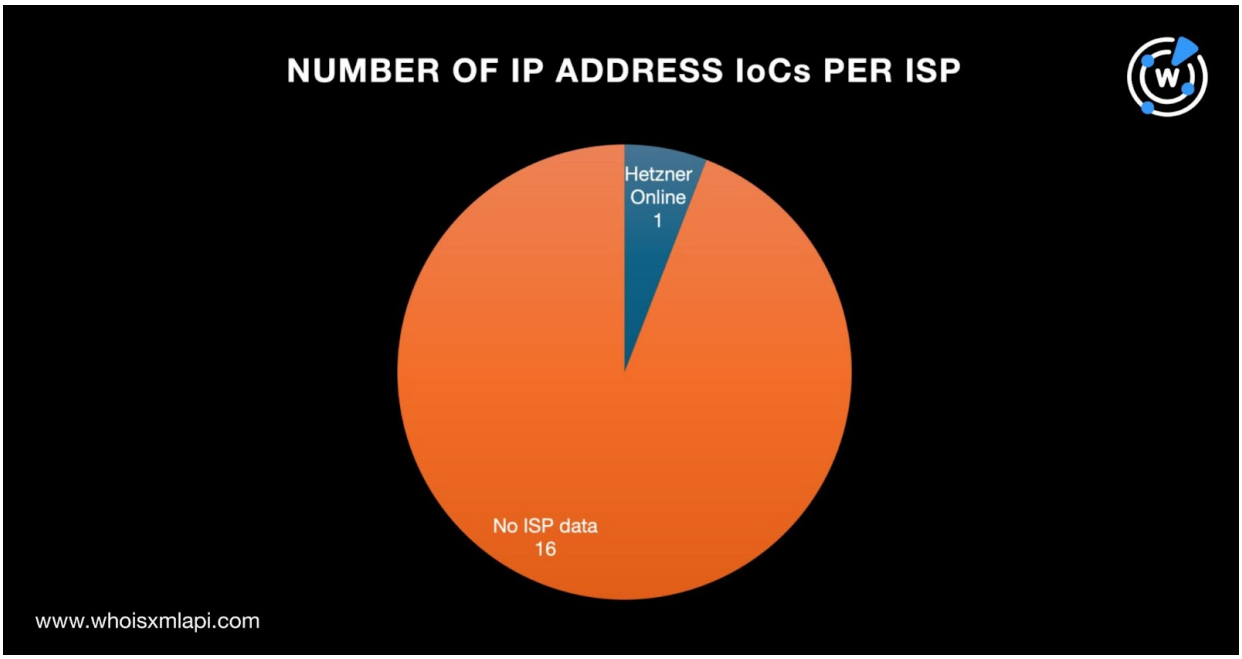
- All 46 domain IoCs were created in 2023, specifically between 9 June and 13 November, making them all fairly new when they were weaponized.

- A majority of the domain IoCs, 44 to be exact, were registered in Iceland. One domain IoC each was registered in Canada and Russia.



Next, we performed a bulk IP geolocation lookup for the 17 IP addresses identified as IoCs and found that:

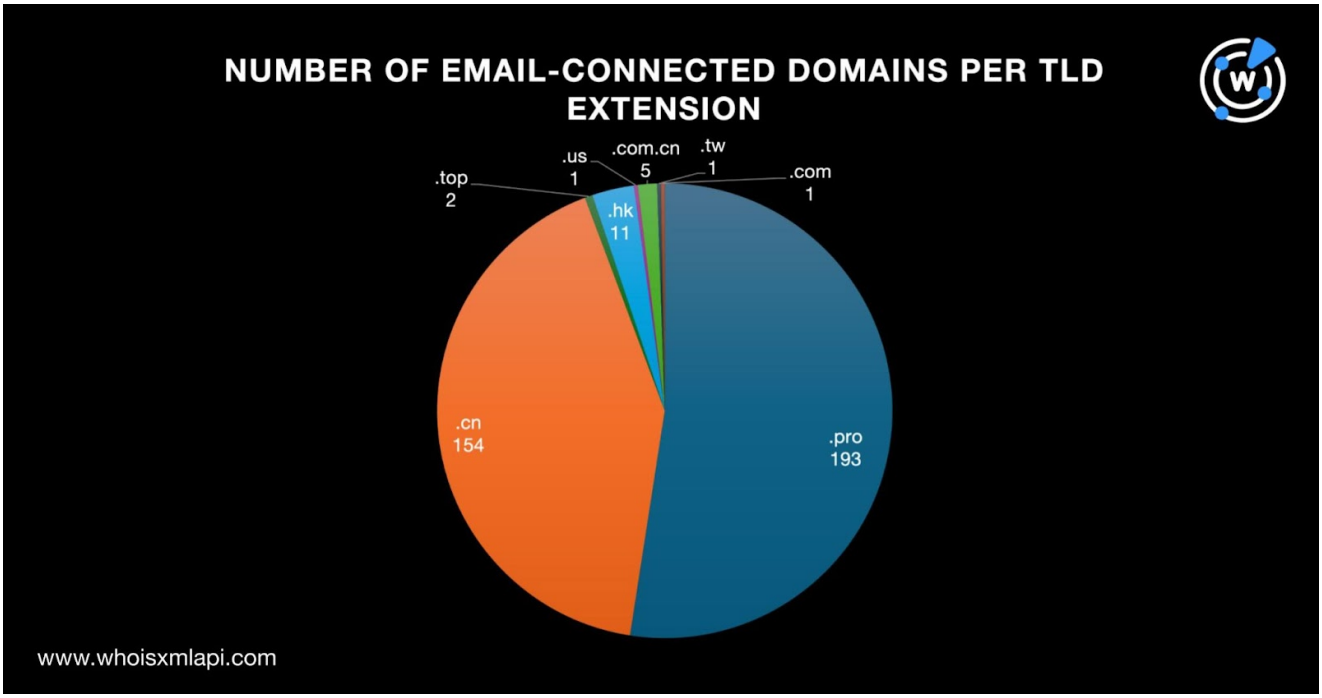
- All 17 IP address IoCs were geolocated in Germany.
- Only one of the IP address IoCs has a public ISP—Hetzner Online.



Expanding on the 8Base Phobos Ransomware Attack Infrastructure

To find out if 8Base had other domains and IP addresses in its attack infrastructure, we expanded the list of IoCs starting with WHOIS History API queries for the 46 domain IoCs. That led to the discovery of four email addresses from their historical WHOIS records. Three of the four email addresses were public.

Reverse WHOIS API queries for the three public email addresses provided us with 368 connected domains after duplicates and the IoCs were filtered out. Close to 200 of the email-connected domains, 193 to be exact, sported the .pro ngTLD extension, akin to one domain IoC. The 175 remaining email-connected domains, meanwhile, were spread across seven TLD extensions, specifically .cn, .hk. .com.cn, .top, .com, .tw, and .us.



A bulk WHOIS lookup for the 368 email-connected domains showed that 144 were, like the domain IoCs, created in 2023.

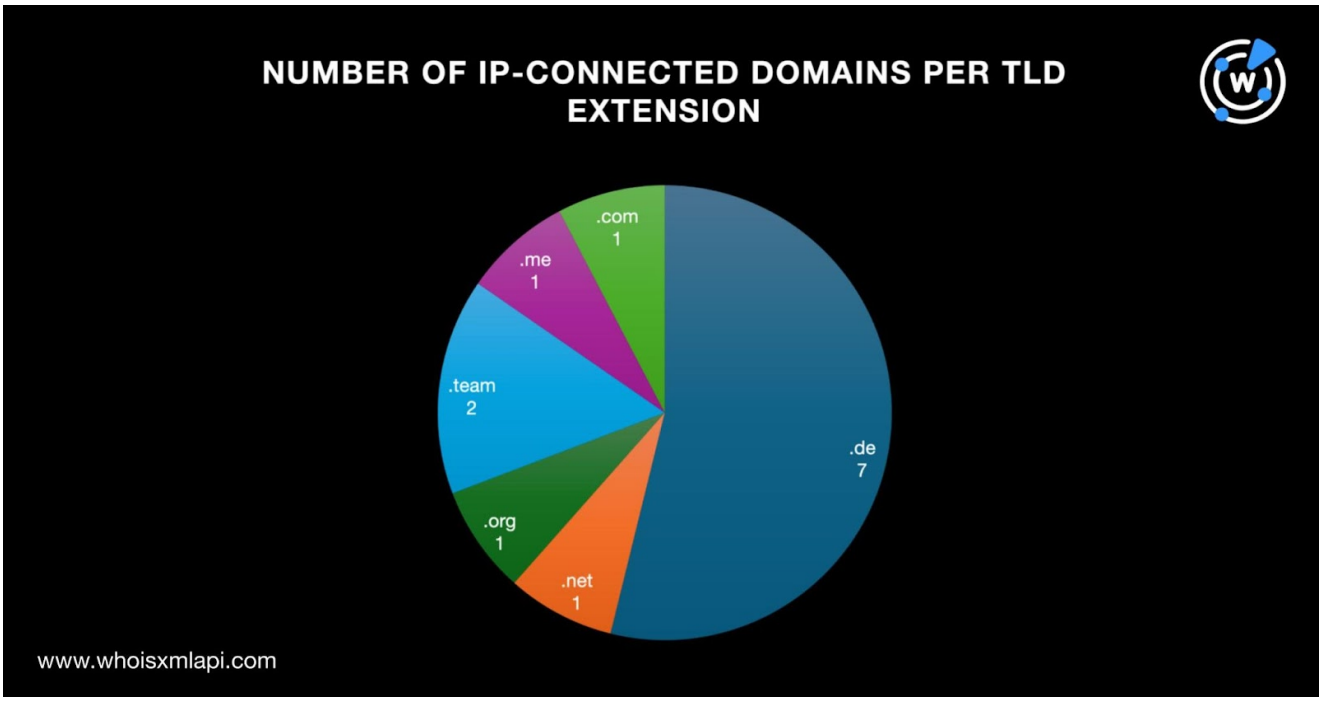
Next, we ran DNS lookups for the 46 domains identified as IoCs and found that some of them resolved to three IP addresses that are not in the current IoC list.

Threat intelligence lookups for the three additional IP addresses revealed that one—45[.]89[.]127[.]159—was seemingly associated with malware distribution.

And like the 17 IP addresses identified as IoCs, a bulk IP geolocation lookup for the three additional IP addresses showed they all originated from Germany even though only one—88[.]198[.]21[.]27—had public ISP data. It was administered by Hetzner Online.

Next, we ran reverse IP/DNS lookups for 20 IP addresses in total (17 identified as IoCs and three additional from the DNS lookups) and found that 10 of them could be dedicated hosts. The 10 remaining IP addresses showed no results.

Altogether the 10 possibly dedicated IP addresses hosted 13 domains after duplicates, the IoCs, and the email-connected domains were filtered out. More than half of the IP-connected domains, seven to be exact, sported the .de ccTLD extension, consistent with the geolocation lookup results. The six remaining IP-connected domains, meanwhile, were spread across five TLD extensions, specifically .com, .me, .net, .org, and .team. Note that .net was also used by one domain IoC.



A bulk WHOIS lookup for the 13 IP-connected domains showed that like the domain IoCs, four were created in 2023.

To cover all the bases, we then looked for other domains starting with the same text strings seen among the domain IoCs using Domains & Subdomains Discovery. We uncovered 20 domains after filtering out duplicates, the IoCs, and email- and IP-connected domains containing these seven strings:

- **advserv.**
- **amx15.**
- **amx395.**
- **amx55.**
- **blogserv.**
- **mexstat.**
- **mxtmx.**

Given that they only used different TLD extensions from the domains identified as IoCs, they could be weaponized for similar attacks. It is also interesting to note that **serv** appeared in 12 of the string-connected domains in combination with **adv** or **blog**. 8Base could be using supposed advertising or blog servers or services as a social engineering ruse.

Throughout our investigation, interesting similarities between the IoCs and potentially connected artifacts stood out, namely:

- Extensive use of the .pro TLD extension like one of the domain IoCs
- About a third each of the email- and IP-connected domains were created in 2023 like the domain IoCs
- Potential ties to Germany as it has been named as a geolocation country, the sole ISP seen in DNS records is based in the country, and many connected domains used .de as TLD extension

---

Our further investigation of the latest 8Base Phobos ransomware attack led to the discovery of 404 potentially connected web properties. We specifically found 401 email-, IP-, and string-connected domains and three IP addresses.

If you wish to perform a similar investigation or 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.*

By **WhoisXML API, A Domain Research, Whois, DNS, and Threat Intelligence API and Data Provider**

Whois API, Inc. (WhoisXML API) is a big data and API company that provides domain research & monitoring, Whois, DNS, IP, and threat intelligence API, data and tools to a variety of industries.

Visit Page

Filed Under

Comments

Commenting is not available in this channel entry.

> I make a point of reading CircleID. There is no getting around the utility of knowing what thoughtful people are thinking and saying about our industry.

Related