A Closer Look at the Meduza Stealer through a DNS Deep Dive

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

Fortinet recently discovered a Meduza Stealer variant that has been taking advantage of the Microsoft Windows SmartScreen vulnerability CVE-2024-21412. The Meduza stealer lets remote attackers bypass the SmartScreen security warning dialog to deliver malicious files.

This particular campaign spreads malicious PDF files that exploit CVE-2024-21412 to download and execute malware like the Meduza Stealer. The final payload? Data stolen from victims' computers are sent to a command-and-control (C&C) server. It is also interesting to note that the threat actors designed PDF files to target specific regions, including North America, Spain, and Thailand.

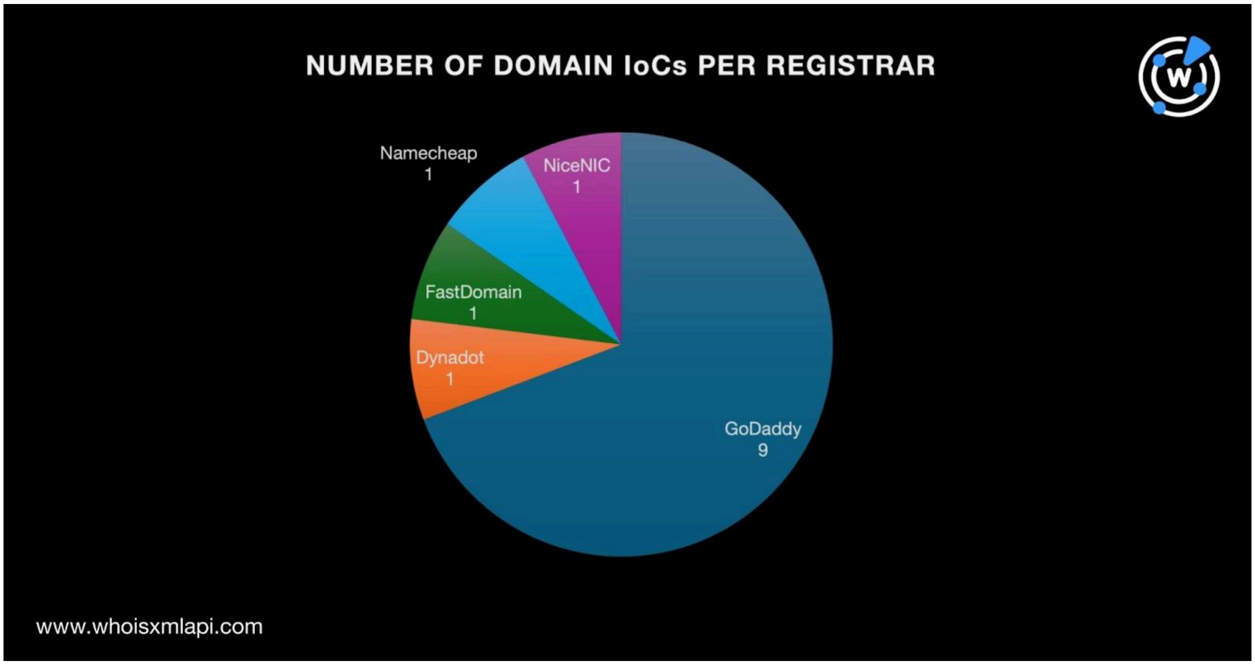
The researchers published their findings earlier this month, including 16 indicators of compromise (IoCs) comprising 13 domain names and three IP addresses. Using them as jump-off points for an IoC list expansion analysis, the WhoisXML API research team uncovered connected artifacts that have not yet been named, namely:

- Nine email-connected domains
- 18 additional IP addresses, 17 of which turned out to be malicious
- One IP-connected domain
- 149 string-connected domains, five of which turned out to be associated with various threats

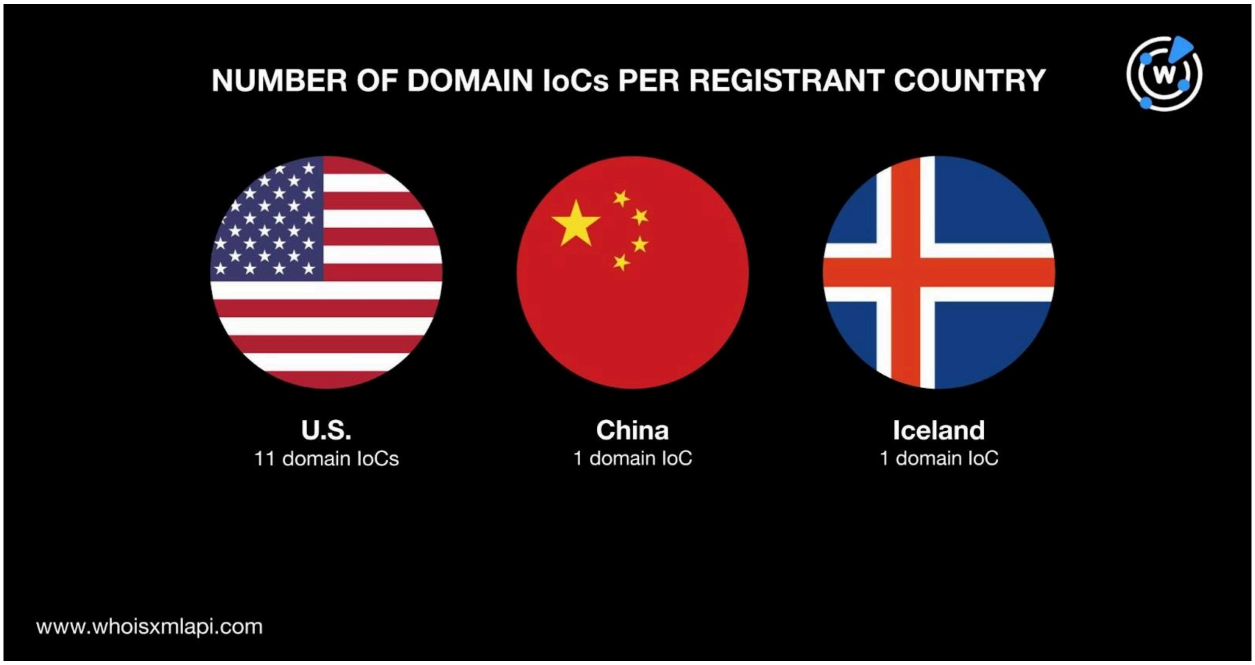
More on the Meduza Stealer Indicators of Compromise

First off, we sought to find more information about the published IoCs starting with a bulk WHOIS lookup for the 13 domains identified as IoCs. Our query led to these findings:

- A majority of them, 69% to be exact (nine domain IoCs), were registered with GoDaddy. The rest of the registrars—Dynadot, FastDomain, Namecheap, and NiceNIC—accounted for one domain IoC each.

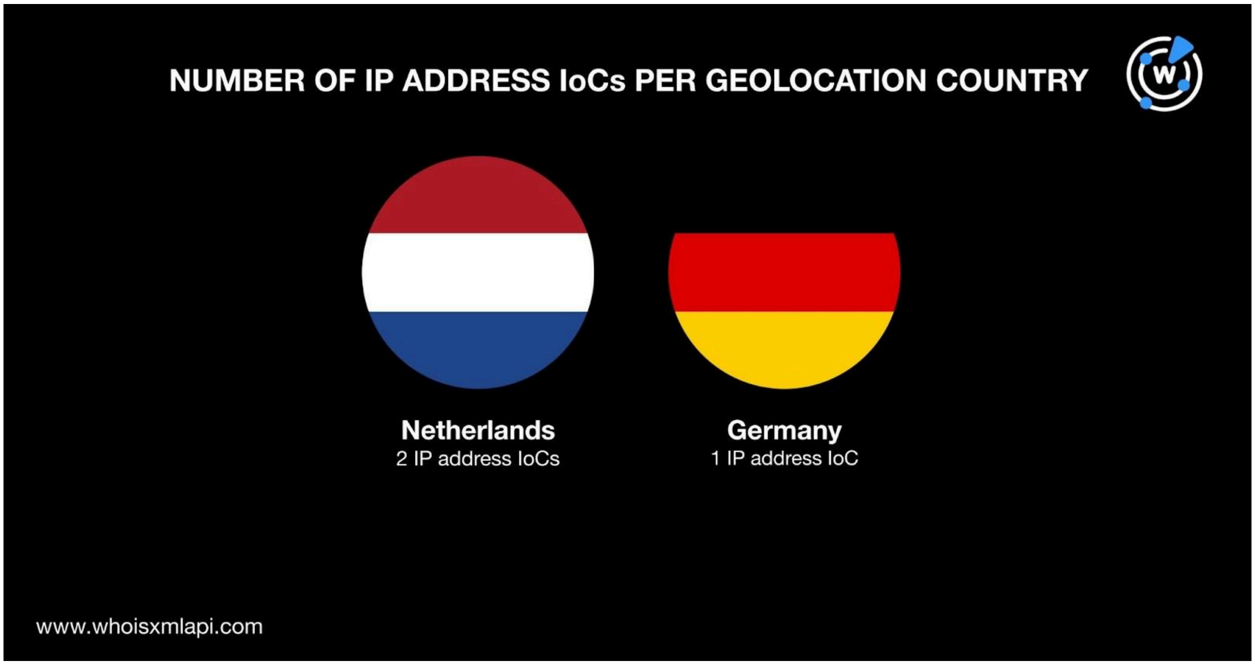


- One of the domain IoCs was old, created way back in 2016 while the other 12 were newly created, just this year.
- A majority of them, 85% to be exact (11 domain IoCs), were registered in the U.S. China and Iceland accounted for one domain IoC each.

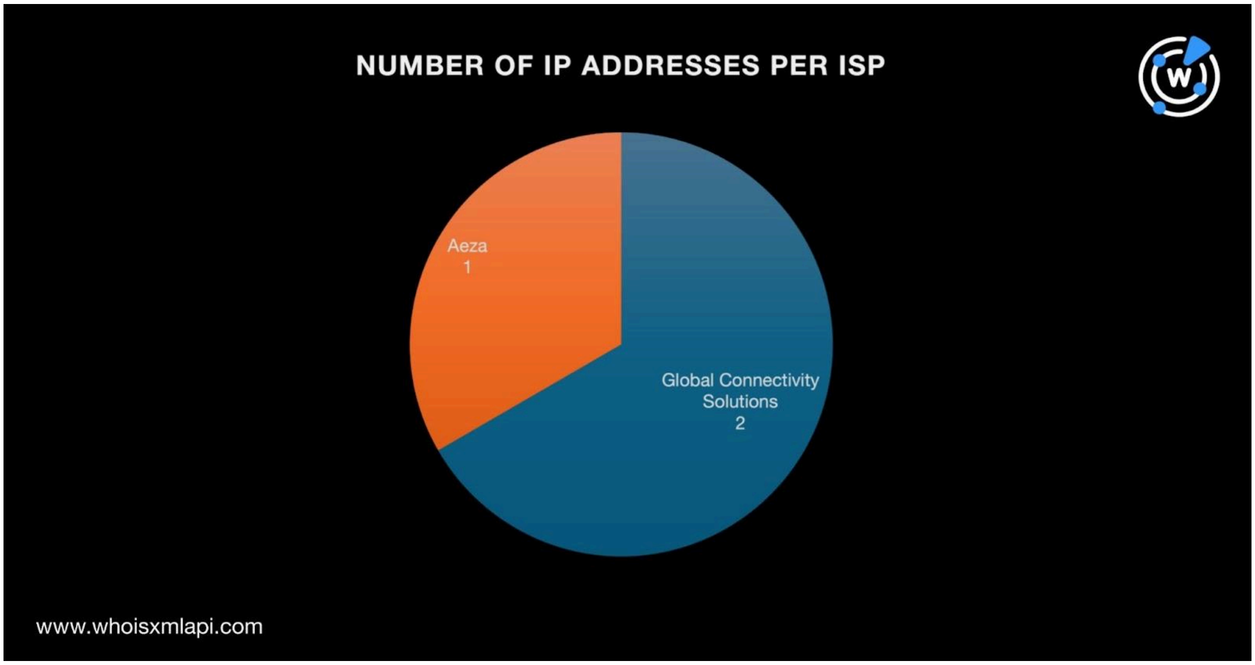


Next, we ran a bulk IP geolocation lookup for the three IP addresses identified as IoCs and found out that:

- They were split across two geolocation countries. Two of them were geolocated in the Netherlands while one originated from Germany.



- Two of the IP address IoCs were administered by Global Connectivity Solutions while one was under Aeza.



Expanding the List of Meduza Stealer Indicators of Compromise

To find artifacts potentially connected to Meduza Stealer, we first queried the 13 domain IoCs on WHOIS History API. The results showed that they had four email addresses in their historical WHOIS records, two of which were public.

Using the two public email addresses as Reverse WHOIS API search terms led to the discovery of nine email-connected domains after filtering out duplicates and the IoCs.

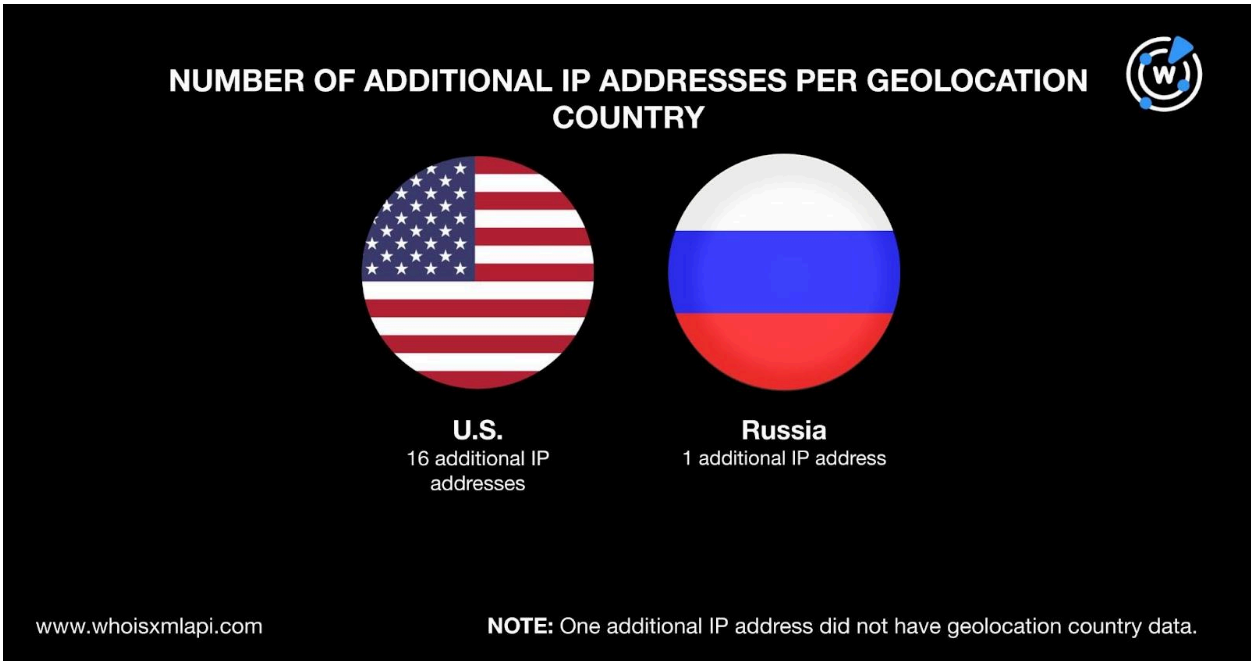
Next, we queried the 13 domain IoCs on DNS Lookup and found out that while three did not have active IP resolutions, the remaining 10 resolved to 18 IP addresses not yet on the original IoC list. Threat Intelligence Lookup showed that 17 of them were associated with various threats. Take a look at five examples below.

ADDITIONAL IP ADDRESS	ASSOCIATED THREAT TYPES
104[.]21[.]28[.]44	Generic Malware Phishing
104[.]21[.]40[.]167	Malware

104[.]21[.]44[.]3	Generic Malware
104[.]21[.]78[.]134	Malware Phishing Suspicious
104[.]21[.]95[.]244	Attack Generic Malware Phishing

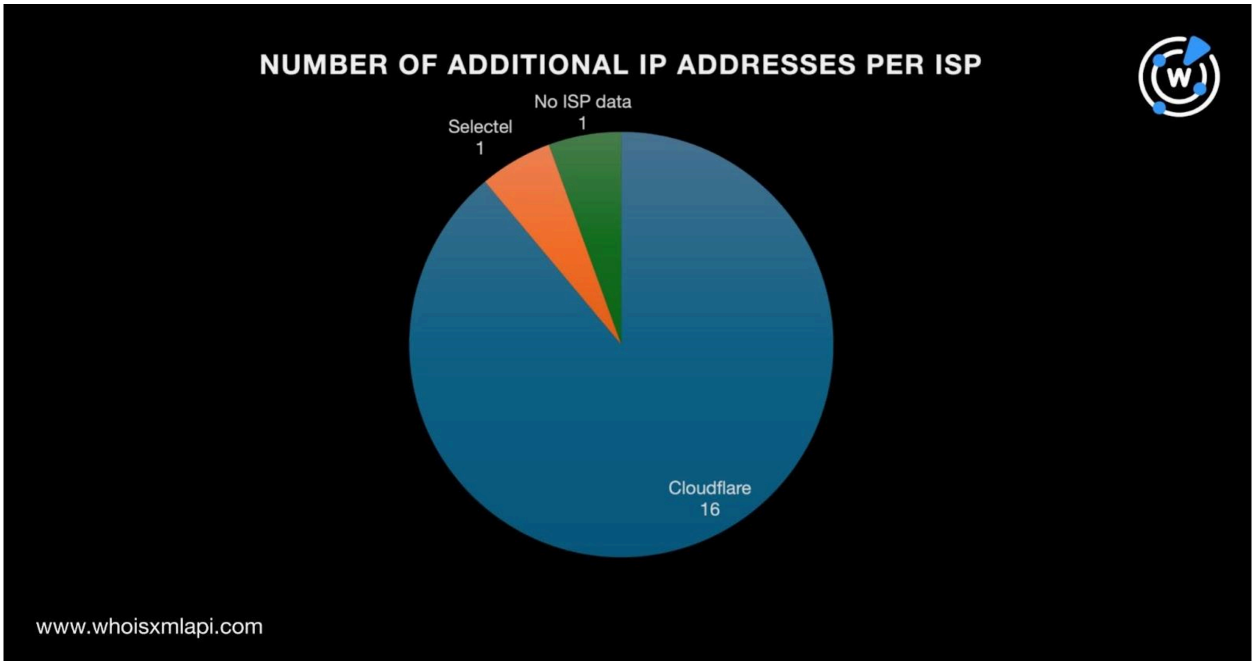
A bulk IP geolocation lookup for the 18 additional IP addresses revealed that:

- They were spread across two geolocation countries. The U.S. accounted for 16 IP addresses while one was geolocated in Russia. One other IP address did not have geolocation country data.


NUMBER OF ADDITIONAL IP ADDRESSES PER GEOLOCATION COUNTRY

NOTE: One additional IP address did not have geolocation country data.

- Cloudflare administered a majority of the additional IP addresses, 16 to be exact. One was managed by Selectel and another one did not have ISP information.



It is interesting to note that none of the 18 additional IP addresses shared the geolocation countries and ISPs of the three IP address IoCs.
Next, we queried the 21 IP addresses (three identified as IoCs and 18 additional ones) on Reverse IP Lookup and found that only one could be dedicated. The sole possibly dedicated IP address was shared by one domain—vaultcybersec[.]in—after filtering out duplicates, the IoCs, and the email-connected domains.

To cover all the bases, we scoured the DNS for string-connected domains using these parameters:

- Starts with the exact strings that appeared in the IoCs, namely, **21centuryart.**, **answerrsdo.**, **pbdbj.**, **pbpbj.**, **pcvcf.**, **pcvvf.**, **pddbj.**, **pdddj.**, **pdddk.**, **pqdrf.**, **proffyrobharborye.**, **ptdrf.**, and **scratchedcards.**
- Starts with **p** and ends with **.xyz** added between 1 June 2024 and 15 June 2024 limited to nine characters each to find .xyz domains made up of five random characters akin to nine of the domain IoCs (pbdbj[.]xyz, pbpbj[.]xyz, pcvcf[.]xyz, pcvvf[.]xyz, pddbj[.]xyz, pdddj[.]xyz, pdddk[.]xyz, pqdrf[.]xyz, and ptdrf[.]xyz)

We uncovered 149 string-connected domains after filtering out duplicates, the IoCs, and the email- and IP-connected domains. Five of them turned out to be associated with malware-instigated attacks according to Threat Intelligence API.

As our last step, we conducted WHOIS record comparisons between the 13 domain IoCs and all the 159 connected domains (i.e., email-, IP-, and string-connected). We discovered that:

- 84 connected domains shared the domain IoCs' registrars
- 76 of them were created in 2024 akin to a majority of the domain IoCs
- 86 connected domains were registered in the same countries as the domain IoCs

We also noticed that one of the 13 domain IoCs—scratchedcards[.]com—had public registrant information (email address and registrant name and organization). These details were also found in the current WHOIS records of seven connected domains, namely:

- crushblend[.]com
- jasonzbornik[.]com
- jzbornik[.]com
- hiveiowa[.]com
- nexusentertainmentarts[.]com
- radiohive[.]net
- scarletsnowmusic[.]com

—

Our in-depth analysis of the latest Meduza Stealer campaign using 16 IoCs made up of 13 domains and three IP addresses as jump-off points led to the discovery of 177 potentially connected artifacts comprising nine email-connected domains, 18 additional IP addresses, one IP-connected domain, and 149 string-connected domains. It is also worth noting that 22 of the connected web properties have already been weaponized for various malicious campaigns.

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

- cr5mff[.]com
- crushblend[.]com
- hiveiowa[.]com
- jasonzbornik[.]com
- jzbornik[.]com

Sample String-Connected Domains

- 21centuryart[.]co[.]uk
- 21centuryart[.]net
- abkpbdbj[.]cn
- apbdbj[.]loan
- appcvvf[.]com
- bpbpbj[.]tw
- bpcvvf[.]work
- bppbpbj[.]cn
- cpbpbj[.]cn
- cpbpbj[.]net
- dkpddbj[.]com
- enptdrf[.]loan
- fvpddbj[.]cn
- gpcvcf[.]top
- gtepbdbj[.]icu
- hcptdrf[.]loan
- hdpddbj[.]ga
- hgxpcvvf[.]shop
- hpddbj[.]ga
- jlpbpbj[.]com
- jpddbj[.]com
- lpbpbj[.]icu
- lrpdddj[.]cn
- lzupdddj[.]site
- mhcpdddj[.]com
- mypbdbj[.]cn
- npdddk[.]work
- p-bit[.]xyz
- p5c6k[.]xyz
- p6wt2n3hbkgmwmcnriokxvqnlnei2obcs6lckffpqdrf[.]fm
- pacot[.]xyz
- padrf[.]xyz
- pafib[.]xyz
- pahec[.]xyz
- palmi[.]xyz
- papac[.]xyz
- parai[.]xyz
- pasfa[.]xyz
- pbdbj[.]com
- pbpbj[.]com
- pbpbj[.]loan
- pbuah[.]xyz
- pc661[.]xyz
- pc662[.]xyz
- pc663[.]xyz
- pc665[.]xyz
- pc668[.]xyz
- pcabh[.]xyz
- pcvvf[.]cn
- pddbj[.]com

Sample Malicious String-Connected Domains

- pmtqe[.]xyz
- prhys[.]xyz
- prxhn[.]xyz