WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

On the DNS Trail of the Foxit PDF Bug Exploitation Attackers

Table of Contents

Executive Report

Check Point Research reported a Foxit PDF Reader vulnerability that threat actors have begun exploiting, putting the application's users at risk. When exploited, the bug triggers security warnings that may deceive unsuspecting users into executing harmful commands.

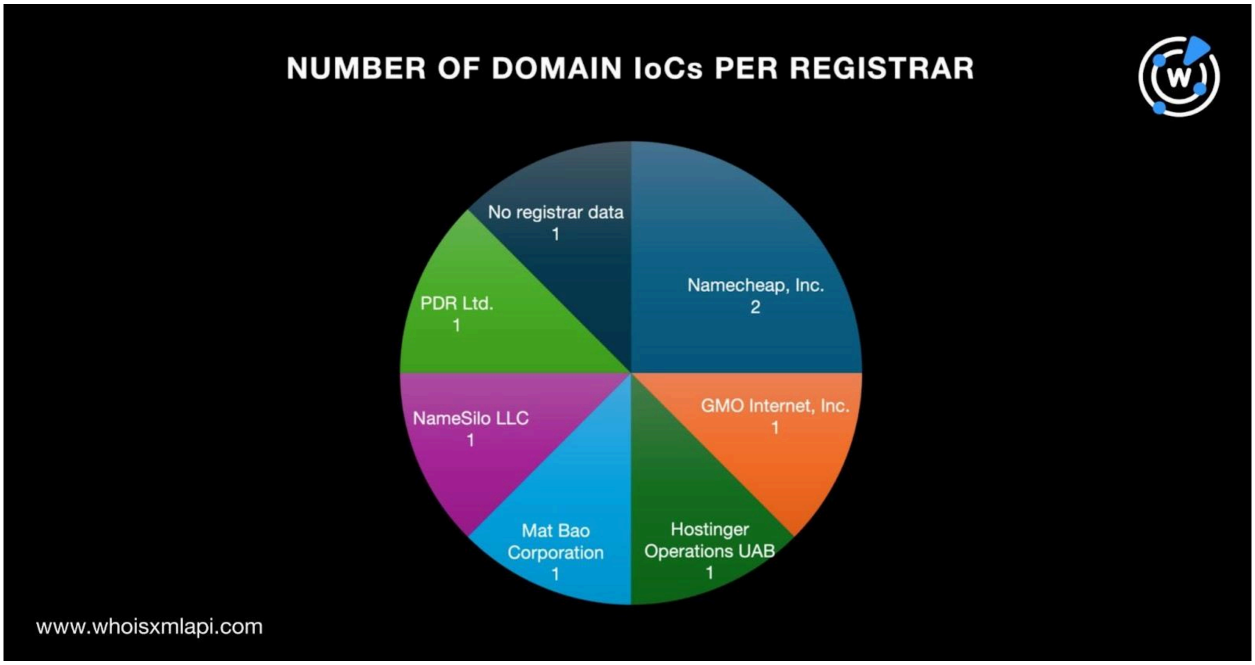
The WhoisXML API research team, in a bid to shed more light on the issue by uncovering more potential attack vectors, thus expanded a public list of indicators of compromise (IoCs). We specifically analyzed eight domain names and one IP address that led to the discovery of:

- 55 registrant-connected domains, two of which turned out to be malicious
- One email-connected domain
- Eight additional IP addresses, six of which turned out to be malicious
- 44 string-connected domains

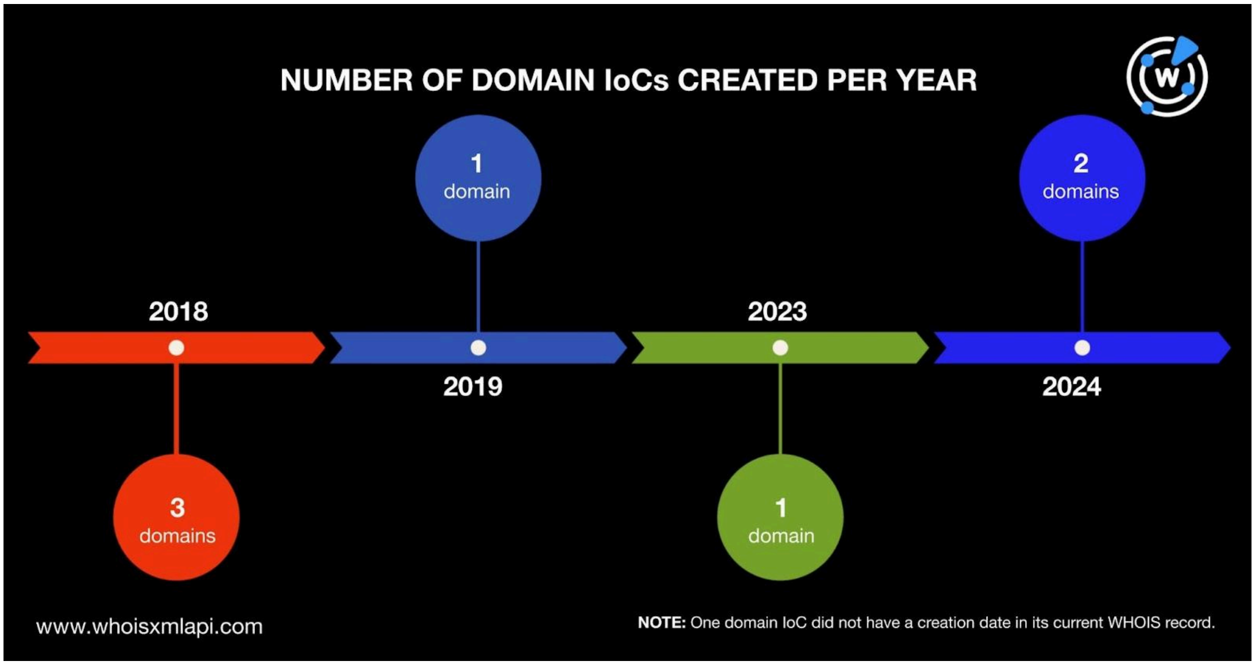
More on the Foxit PDF Reader Vulnerability Exploitation IoCs

As per usual, we began our in-depth analysis with a bulk WHOIS lookup for the eight domains tagged as IoCs, which revealed that:

- Two domain IoCs (omagle-chat-secure[.]com and mailservicess[.]com) had public registrant names in their current WHOIS records. Another two (omagle-chat-secure[.]com and sealingshop[.]click) had public registrant organizations.
- Seven domain IoCs were spread across six registrars—two with Namecheap, Inc. and one each with GMO Internet, Inc.; Hostinger Operations UAB; Mat Bao Corporation; NameSilo LLC; and PDR Ltd. One domain IoC did not have a registrar in its current WHOIS record.

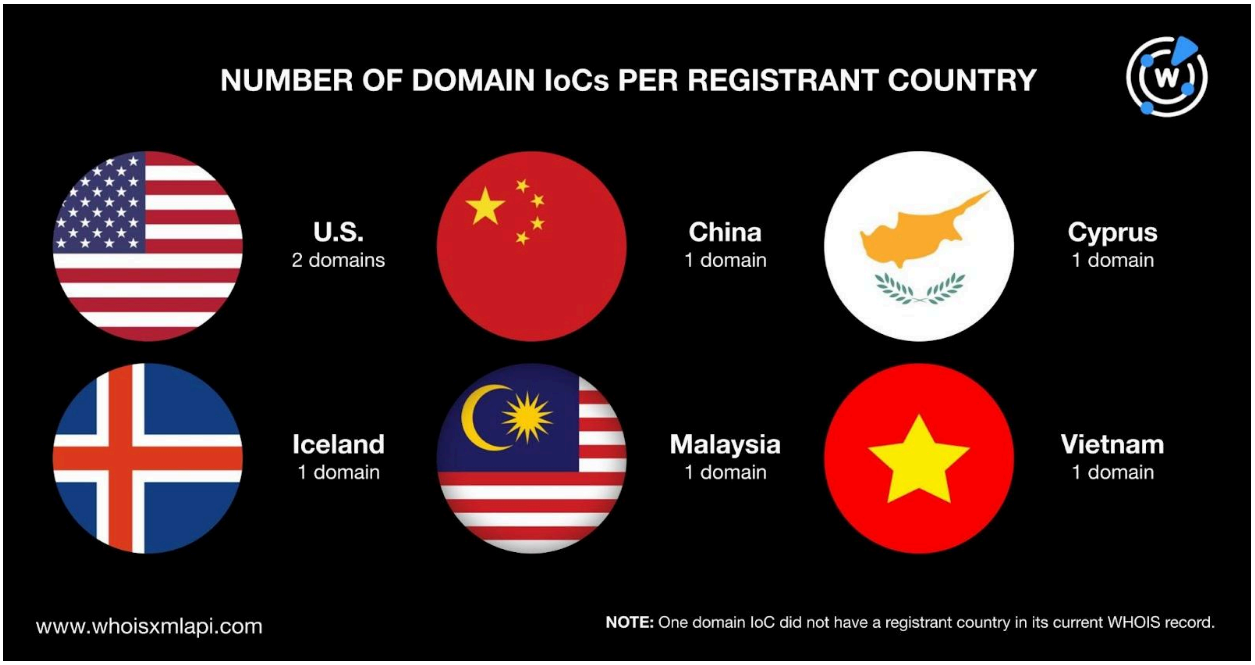


- The actors behind the attack used a combination of old and new domains created between 2018 and 2024. Three domain IoCs were created in 2018, two in 2024, and one each in 2019 and 2023. One domain IoC did not have a creation date in its current WHOIS record.



NOTE: One domain IoC did not have a creation date in its current WHOIS record.

- Seven domain IoCs were registered in six countries—two in the U.S. and one each in China, Cyprus, Iceland, Malaysia, and Vietnam. One domain IoC did not have a registrant country in its current WHOIS record.



NOTE: One domain IoC did not have a registrant country in its current WHOIS record.

An IP geolocation lookup for the sole IP address named as an IoC showed it was geolocated in Singapore with OVHcloud as its ISP.

Following the Foxit PDF Reader Bug Exploitation IoC Breadcrumbs

Our closer look behind the IoCs began with reverse WHOIS searches for the registrant names and organizations using the **Advanced**, **Exact match**, and **Historic** parameters. The queries provided us with 55 registrant-connected domains after duplicates and the IoCs were filtered out. Threat intelligence lookups for them revealed that two—contracsupport[.]click and facebook-helper[.]click—were associated with phishing.

It is also interesting to note that five of the registrant-connected domains contained three popular brand names, albeit misspelled and could be weaponized for other attacks. One of them, in fact, already figured in a phishing campaign—facebook-helper[.]click, as mentioned above. The other brand-containing domains are shown in the table below.

BRAND-CONTAINING REGISTRANT-CONNECTED DOMAIN	POPULAR BRAND POSSIBLY BEING MIMICKED

facebook-helper[.]click	Facebook
grammasly[.]com grammasly[.]xyz	Grammarly
metabusiness[.]mom support-meta-page-ick[.]com	Meta

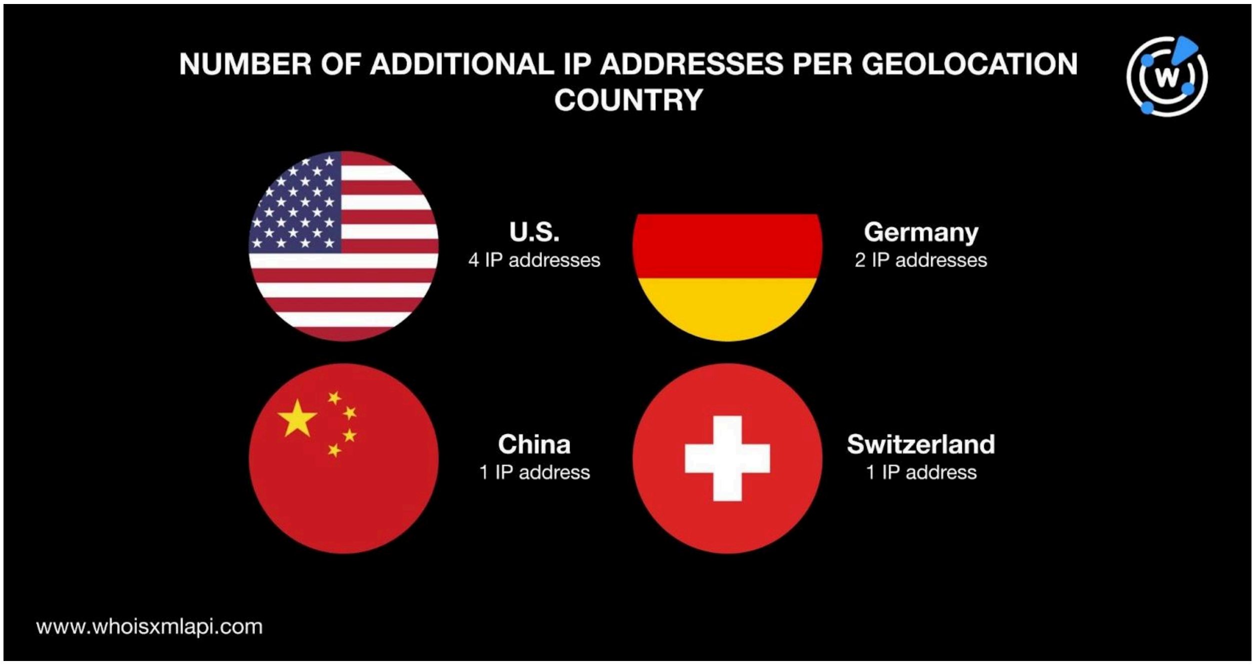
Next, we performed WHOIS History API queries for the eight domains identified as IoCs and found 26 email addresses in their historical WHOIS records. Four of the email addresses were public after duplicates were removed. Reverse WHOIS API showed they also appeared in the current WHOIS record of one email-connected domain—potfarmrehashed[.]info—after we filtered out duplicates, the IoCs, and the registrant-connected domains. Like domain IoC shellobj[.]run, email-connected domain potfarmrehashed[.]info did not have current WHOIS record details.

We then did DNS lookups for the eight domains named as IoCs, which revealed that they resolved to eight IP addresses after we removed duplicates and the IoC. Six of them turned out to be associated with between two and three threats each. The table below shows a couple of examples.

IP ADDRESS	ASSOCIATED THREATS
104[.]21[.]36[.]187	Generic Malware Phishing
172[.]67[.]134[.]54	Generic Phishing
172[.]67[.]198[.]144	Generic Malware Phishing

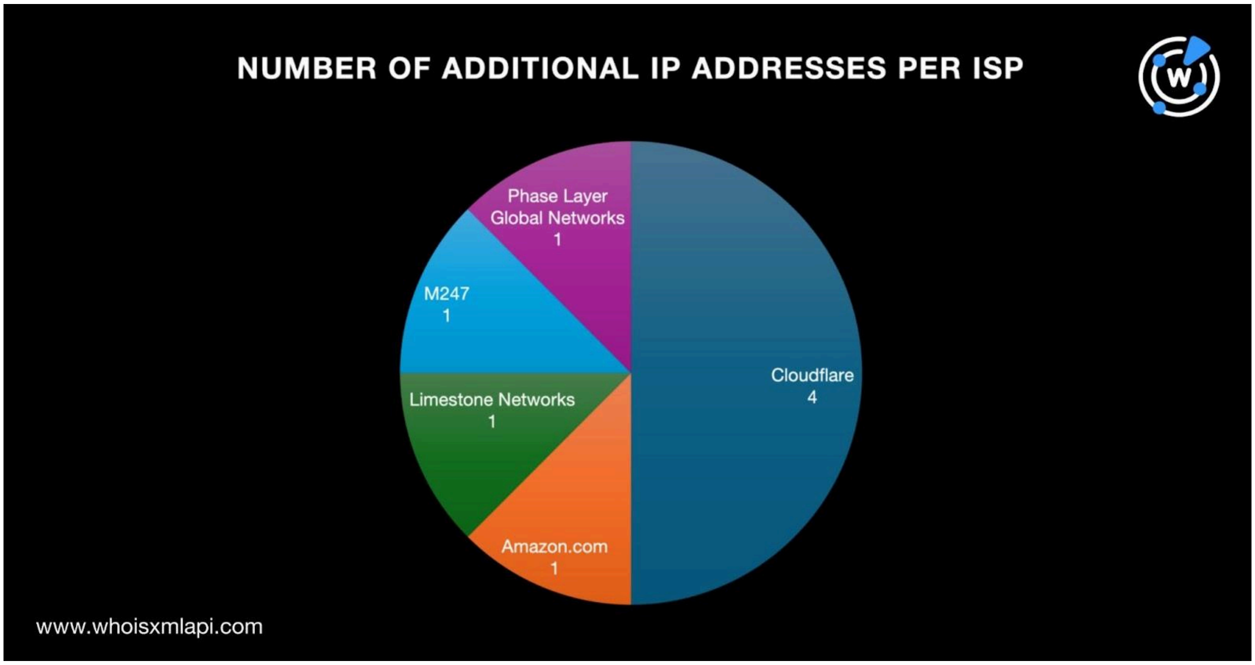
A bulk IP geolocation lookup for the eight additional IP addresses showed that:

- They were spread across four geolocation countries. Four of the additional IP addresses were geolocated in the U.S. akin to the IoC. Two originated in Germany and one each in China and Switzerland.



NUMBER OF ADDITIONAL IP ADDRESSES PER GEOLOCATION COUNTRY

- They were also split among five ISPs led by Cloudflare, which accounted for four of the IP address IoCs. One IP address IoC each fell under the purview of Amazon.com, Limestone Networks, M247, and Phase Layer Global Networks.



NUMBER OF ADDITIONAL IP ADDRESSES PER ISP

Next, we performed reverse IP lookups for a total of nine IP addresses—one identified as an IoC and eight domain IoC resolutions. Three of them were seemingly dedicated and connected to a couple of domains. After removing duplicates, the IoCs, and the registrant- and email-connected domains, however, we did not uncover any IP-connected domain.

To cover all bases, we scoured the DNS for other potentially connected domains, specifically those containing the text strings found among the eight domains tagged as IoCs. We used the **Domains only** and **Starts with** parameters for the text strings **digitalmarketingstart.**, **herominers.**, **mailservicess.**, **omagle-chat-secure.**, **sealingshop.**, **subprocess.**, and **unmineable.** on Domains & Subdomains Discovery. We unearthed 44 string-connected domains after we removed duplicates, the IoCs, and the registrant- and email-connected domains.

—

Our Foxit PDF Reader expansion analysis of the eight domains and one IP address named as IoCs led to the discovery of 108 potentially connected digital properties, specifically 55 registrant-connected domains, one email-connected domain, eight additional IP addresses, and 44 string-connected domains. We also found that eight of the connected artifacts were associated with various threats spanning C&C, generic threats, malware distribution, and phishing.

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 Registrant-Connected Domains

- 6dayclickhotdeals[.]com
- account-approved[.]help
- account-center[.]com
- account-center[.]online
- accounts-manager-protect[.]help
- accountsmanager[.]help
- ads-business[.]help
- adsmanager-support[.]help
- approved-support-ads[.]help
- bot4avbekxosinwnzkl[.]online
- business-account-help[.]xyz
- business-account[.]help
- business-recover-manager[.]help
- contracsupport[.]click

- facebook-helper[.]click
- filo-contact[.]help
- grammasly[.]com
- grammasly[.]xyz
- internetdownloadmanager[.]click
- langtalangoang[.]click

Sample String-Connected Domains

- digitalmarketingstart[.]bond
- digitalmarketingstart[.]lol
- digitalmarketingstart[.]online
- herominers[.]club
- herominers[.]cn
- herominers[.]co
- herominers[.]de
- herominers[.]net
- herominers[.]party
- herominers[.]pl
- herominers[.]ru
- herominers[.]vip
- herominers[.]ws
- mailservicess[.]club
- mailservicess[.]info
- mailservicess[.]nl
- sealingshop[.]com
- subprocess[.]com
- subprocess[.]dance
- subprocess[.]net