Analyzing Account Takeover Attacks Leveraging SquarePhish2 and Graphish

Table of Contents

Executive Report

Proofpoint tracked several state-sponsored and financially motivated threat clusters that used SquarePhish2 and Graphish, among other phishing tools, to trick users into granting the actors access to their Microsoft 365 accounts by bypassing the OAuth device code authorization process. Successfully compromising the victims' accounts reportedly led to account takeover, data exfiltration, and other serious consequences. The researchers identified at least 44 IoCs associated with the attacks in their report.

Note that four of the 21 subdomains identified as IoCs can have multiple variations, which could mean a substantially bigger volume. Any number of target organization names can be appended to the subdomain onlinedocuments-[OrganisationName][.]vxhwuulcnfzlfmh[.]live, for example.

After extracting unique domains from the subdomains identified as IoCs, we collated 52 IoCs. Next, we weeded out legitimate domains from the 28 identified as IoCs using Jake AI. Our queries revealed that six of them were legitimate, reducing the number of domains for further analysis to 22. In the end, we analyzed 46 IoCs comprising 21 subdomains (including four with multiple variations), 22 domains, one IP address, and two email addresses.

Using our homegrown tools to investigate the threat, we uncovered these findings:

- Five domains identified as IoCs were deemed likely to turn malicious 65–93 days before being dubbed as such
- 91 email-connected domains
- 23 additional IP addresses, 22 of which turned out to be malicious
- Two IP-connected domains
- 15 string-connected domains

- Two string-connected subdomains

Scrutinizing the Subdomain IoCs

Our quest to unearth more information about the threat began with Jake AI queries for 17 of the 21 subdomains (excluding the four with multiple variations). We discovered that four of them are worth avoiding as they could well be on their way to becoming phishing pages. One such case is illustrated below.

Based on the information I've gathered, `onedrive.gov-zm.workers.dev` **is a highly suspicious domain and should be treated with extreme caution.** It has several characteristics of a phishing site. Here's a breakdown of what I found and why it's a cause for concern:

- **Domain Structure:** The domain is structured to impersonate a legitimate service.
  - `onedrive`: This part of the domain is clearly meant to mimic Microsoft's OneDrive file hosting service.
  - `gov-zm`: This is designed to look like an official government of Zambia domain (`.gov.zm` is the country's official government top-level domain).
  - `workers.dev`: This is a domain provided by Cloudflare for its "Workers" service, which allows developers to run applications on Cloudflare's network. While it's a legitimate service, it can be abused to host malicious sites.
- **DNS Information:** The domain resolves to Cloudflare's IP addresses, which is expected for a `workers.dev` domain. However, this doesn't tell us anything about the legitimacy of the content hosted on it.
- **Threat Intelligence:** My scan of threat intelligence databases did not find any malicious activity associated with this domain. However, this does not mean it's safe. Phishing sites are often new and may not have been reported or flagged yet.
- **Categorization:** The domain could not be categorized, and the website did not respond. This is also common with phishing sites, as they may only be active for short periods or may only serve content to specific users.

Conclusion: High-Risk Phishing Attempt

The combination of a well-known brand name (`onedrive`) with a government-impersonating subdomain (`gov-zm`) on a `workers.dev` domain is a classic phishing tactic. The goal is likely to trick users into believing they are on a legitimate government or Microsoft OneDrive page, and then steal their login credentials or other sensitive information.

I strongly advise against visiting this domain or providing any information to it. If you received a link to this site in an email, it is almost certainly a phishing attempt. You should delete the email and, if possible, report it as phishing to your email provider.

Sample Jake AI query result for the subdomain onedrive[.]gov-zm[.]workers[.]dev

Examining the Email IoCs

We looked closer into the two email addresses identified as IoCs next via Jake AI as well. One of them could be dangerous to interact with due to its association with a phishing campaign.

I have investigated the domain `ksmus.virtoshare.com`, which is associated with the email address you provided. Based on my findings, this domain is **not legitimate and should be treated as highly suspicious.**

Here's a breakdown of the red flags I discovered:

- `clientHold` **Status:** The root domain, `virtoshare.com`, has a `clientHold` status. This is a serious issue, as it's an explicit status set by the domain registrar that deactivates the domain. This action is typically taken due to legal disputes, non-payment, or, most commonly, when the domain has been flagged for malicious or illegal activities.
- **No DNS Resolution:** The DNS lookup for `ksmus.virtoshare.com` failed to find any 'A' records, meaning it doesn't point to a valid IP address. This is consistent with the `clientHold` status and confirms the domain is not active.
- **Recent and Anonymous Registration:** The domain `virtoshare.com` was registered on October 8, 2025, and the owner's information is redacted for privacy.
- **Unreachable Website:** The categorization tool confirmed that the website is offline.
- **No Threats Found (Yet):** While the Threat Intelligence tool did not find any current threats, this is not a guarantee of safety. The `clientHold` status suggests the domain was likely suspended before it could be widely used and blacklisted.

Conclusion: Do Not Trust This Domain or Email Address

The `clientHold` status is a definitive indicator that `virtoshare.com` and its subdomains are not legitimate. The email address `no-reply.[redacted]@ksmus.virtoshare.com` is associated with a domain that has been suspended for a violation of the registrar's policies.

I strongly advise against interacting with any emails from this address or visiting any links associated with it. It is almost certainly part of a phishing campaign or other malicious activity.

Jake AI query result for an email address identified as an IoC

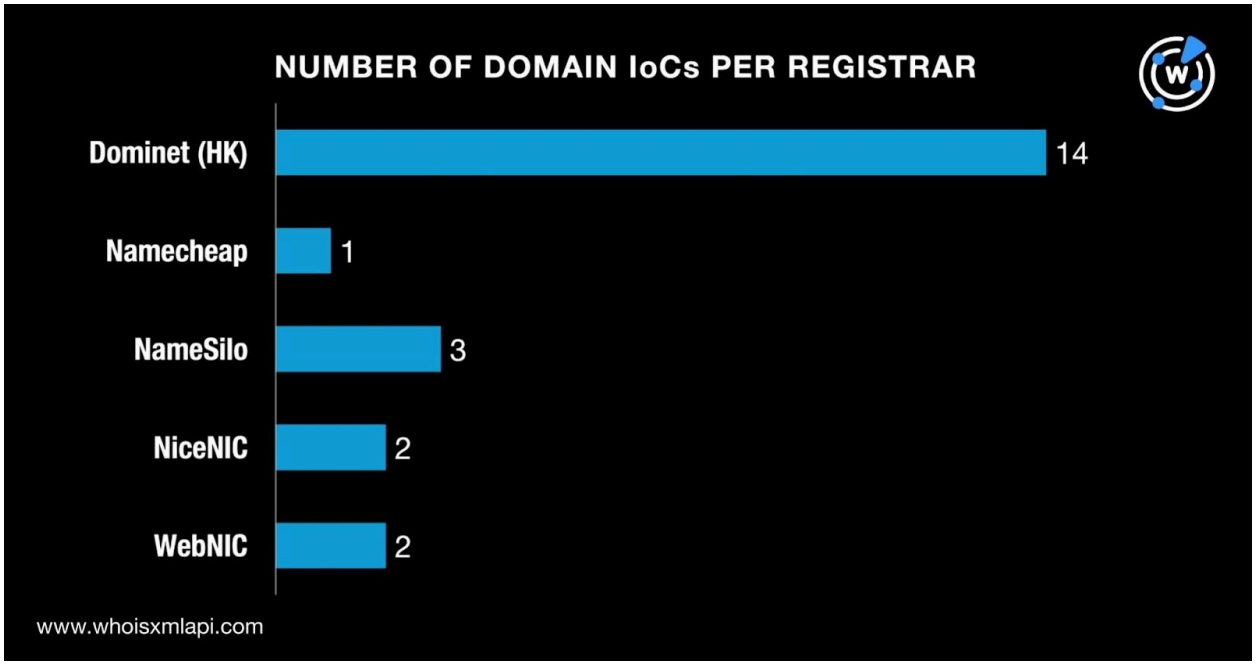
Dissecting the Domain IoCs

First off, we queried the 22 domains identified as IoCs on the First Watch Malicious Domains Data Feed and found out that five of them were deemed likely to turn malicious 65–93 days before they were reported as such on 18 December 2025.

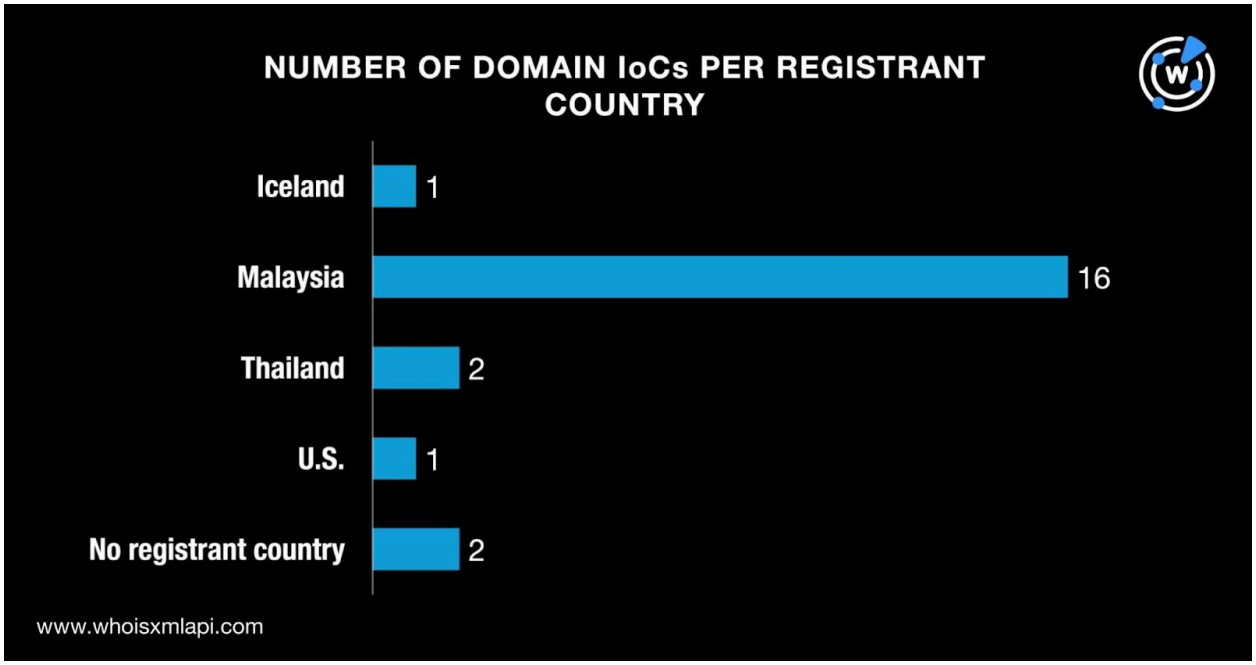
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS BEFORE REPORT DATE
blitzcapital[.]net	09/16/25	93
bluecubecapital[.]com	09/17/25	92
vxhwuulcnfzlfmh[.]live	10/06/25	73

WHOIS API queries for the 22 domains identified as IoCs revealed that:

- All of them were created in 2025, specifically between 15 September and 1 December 2025.
- A majority of them, 14 to be exact, were administered by Dominet (HK). The remaining eight domains were managed by four other registrars—three by NameSilo, two each by NiceNIC and WebNIC, and one by Namecheap.



- While two of them did not have registrant countries on record, the remaining 20 were registered in four countries—16 in Malaysia, two in Thailand, and one each in Iceland and the U.S.



DNS Chronicle API queries for the 22 domains identified as IoCs showed that 21 of them had historical domain-to-IP resolutions. All in all, the 21 domains posted 823 resolutions over time. The domain bluecubecapital[.]com recorded the oldest first resolution date—5 February 2017.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
bluecubecapital[.]com	261	02/05/17	12/25/25
blitzcapital[.]net	172	04/28/17	06/02/25
magnavite[.]com	101	06/03/17	08/09/19
virtoshare[.]com	56	11/10/17	10/10/25
vaultally[.]com	136	11/15/19	01/03/21

Investigating the IP IoC

An IP Geolocation API query for the sole IP address identified as an IoC showed that while it did not have an ISP on record, it was geolocated in the Netherlands.

Hunting for New Artifacts

After obtaining more information about the IoCs connected to SquarePhish2 and Graphish, we searched for other possibly connected artifacts. We started our hunt with WHOIS History API

queries for the 22 domains identified as IoCs. We learned that nine of them had 35 unique email addresses in their historical WHOIS records. Further scrutiny revealed that three of them were public email addresses.

Next, we queried the three public email addresses on Reverse WHOIS API and discovered that while none of them appeared in current WHOIS records, all of them were present in historical WHOIS records. Our search, in fact, turned up 91 unique email-connected domains after those already identified as IoCs were filtered out.

We then queried the 22 domains identified as IoCs on DNS Lookup API and found out that 14 of them actively resolved to 23 unique IP addresses after the sole IoC was filtered out.

Threat Intelligence API queries for the 23 additional IP addresses revealed that 22 of them have already been weaponized for various attacks.

ADDITIONAL IP	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
104[.]21[.]46[.]218	Malware distribution Phishing Generic threat Suspicious activity	10/27/24 06/11/23 01/18/25 03/26/25	12/29/25 12/08/25 12/07/25 10/07/25
172[.]67[.]142[.]223	Malware distribution Phishing Generic threat Suspicious activity	10/27/24 06/11/23 01/18/25 03/26/25	12/29/25 12/08/25 12/07/25 10/07/25
172[.]67[.]175[.]171	Phishing Malware distribution Generic threat Suspicious activity	09/01/23 11/11/24 07/16/25 04/07/23	12/30/25 12/29/25 12/22/25 11/21/25
104[.]21[.]22[.]9	Phishing Generic threat Malware distribution	05/07/23 04/29/25 06/30/23	11/03/25 10/03/25 10/01/25
104[.]21[.]24[.]177	Phishing Malware distribution Generic threat	06/12/23 08/11/25 04/05/23	12/29/25 12/22/25 10/13/25

We now had 24 IP addresses—the sole IP address identified as an IoC and 23 additional—on hand. Reverse IP API queries for them showed that only one could be a dedicated host. Our

search also led to the discovery of two unique IP-connected domains after those identified as IoCs and email-connected domains were filtered out.

Next, we extracted 22 unique text strings from the 22 domains identified as IoCs. Domains & Subdomains Discovery searches for them revealed that four appeared at the start of domains that were not part of the IoC list. These were:

- **blitzcapital.**
- **bluecubecapital.**
- **confidentfiles.**
- **renewauth.**

The results also allowed us to collate 15 unique string-connected domains after those already identified as IoCs and the email- and IP-connected domains were filtered out.

We also looked for subdomains that started with the text string **onlinedocuments-** akin to the four subdomains with several possible variations and uncovered two unique string-connected subdomains after those already identified as IoCs were filtered out.

—

In sum, our in-depth investigation of the account takeover attacks that leveraged SquarePhish2 and Graphish revealed that five domains identified as IoCs were deemed likely to turn malicious 65–93 days before being dubbed as such. Finally, we unearthed 133 new artifacts, comprising 91 email-connected domains, 23 additional IP addresses, two IP-connected domains, 15 string-connected domains, and two string-connected subdomains. It is also worth noting that 22 of these newly found connected artifacts have already been weaponized for various 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

- 5555972[.]com
- 888666866[.]com
- 88866860[.]com
- accelaris[.]com
- accelmetrics[.]com
- accelstack[.]com
- bolthost[.]com
- bovvi[.]com
- brookfund[.]com
- cardipping[.]com
- cloakchip[.]com
- crowdbio[.]com
- dealright[.]com
- deluxebloom[.]com
- dollardeck[.]com
- electronic-game[.]com
- everbarter[.]com
- expedidor[.]com
- faircupid[.]com
- fetchtalent[.]com
- fileraft[.]com
- globe-conspiracies[.]com
- gymforest[.]com
- hellosentry[.]com
- hirekarma[.]com
- honestkush[.]com
- jobgenics[.]com
- jobgenix[.]com
- kushsome[.]com
- lendsky[.]com
- logicwhale[.]com
- mediaparrot[.]com
- nebulahosts[.]com
- nerdtribe[.]com
- outfreight[.]com
- paysurge[.]com
- peakgains[.]com
- picninja[.]com
- qourtesy[.]com
- realition[.]com
- recruitville[.]com
- renslo[.]com
- sagecrew[.]com
- scoutfirm[.]com
- sentryful[.]com
- tenhaus[.]com
- tevoro[.]com
- thegeko[.]net
- uchirp[.]com
- upgevity[.]com
- veganmile[.]com
- wealtheden[.]com
- wearbyte[.]com
- wethrivewell[.]com
- xxzer0modzxx[.]net
- yumcast[.]com
- zapmetrics[.]com
- zencreed[.]com

Sample Additional IP Addresses

- 104[.]21[.]22[.]9
- 104[.]21[.]24[.]177
- 104[.]21[.]27[.]223
- 147[.]28[.]229[.]127
- 172[.]67[.]135[.]7
- 172[.]67[.]142[.]198
- 172[.]67[.]142[.]223

Sample IP-Connected Domain

- aevistascapital[.]com

Sample String-Connected Domains

- blitzcapital[.]co
- blitzcapital[.]com
- blitzcapital[.]com[.]au
- bluecubecapital[.]co[.]uk
- bluecubecapital[.]uk
- bluecubecapital[.]xyz
- confidentfiles[.]top
- renewauth[.]es
- renewauth[.]net

Sample String-Connected Subdomain

- onlinedocuments-com[.]mail[.]protection[.]outlook[.]com