Why Domain Seizure Doesn't Necessarily Translate to No More Risks

Table of Contents

Executive Report

In the realm of cybersecurity, seizing domains unfortunately doesn't always mean the end for the threats they pose. Such could be the case for the 18 domains U.S. law enforcement agents recently took offline for their ties to a money mule recruitment operation reported by Bleeping Computer.

We dove deeper into the threat vectors aided by WHOIS, IP, and DNS intelligence and discovered potentially connected artifacts that could still pose risks to Internet users. Our investigation led to the discovery of:

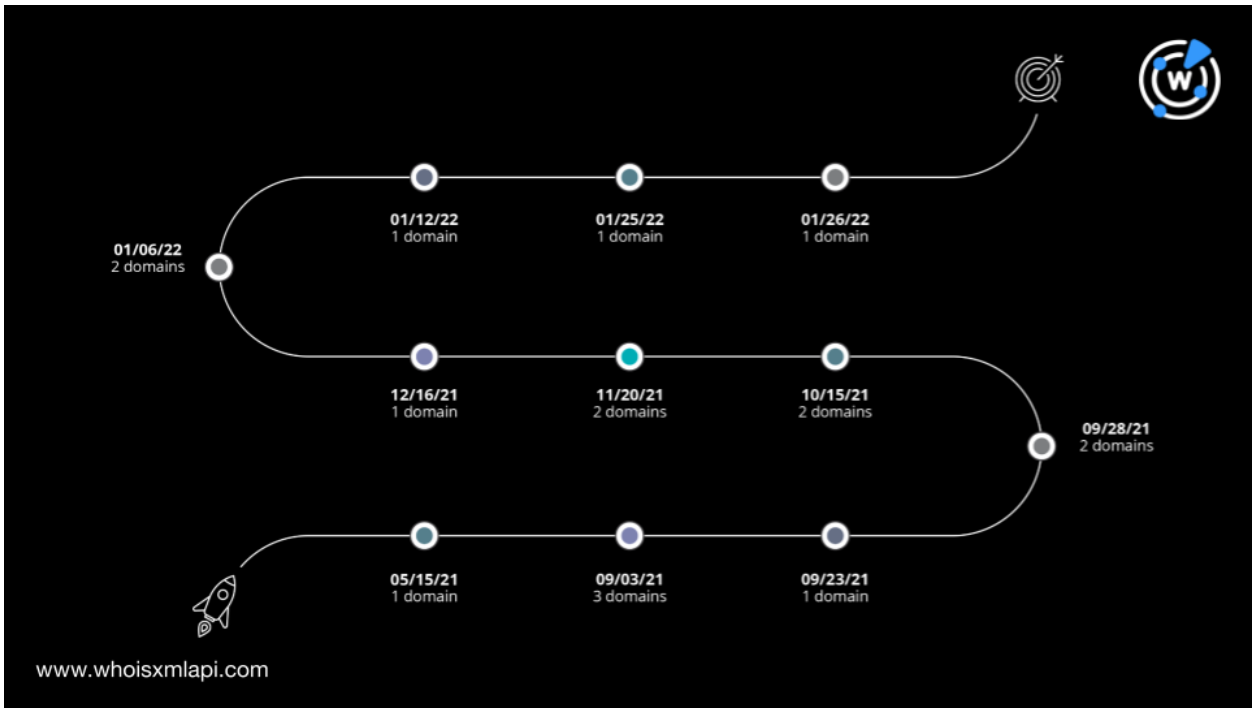
- A single IP address to which all the seized domains resolved to
- 63 additional domains that resolved to the same IP address as the domains identified as indicators of compromise (IoCs)
- 418 more domains that shared unique strings or string combinations found among the seized domains
- Nine unredacted personal registrant email addresses from the historical WHOIS records of 400+ artifacts
- 104 additional domains that shared some of the 400+ artifacts' registrant email addresses, two of which were malicious

Digging into the IoCs' Past

We began our deep dive by subjecting the IoCs to historical WHOIS searches that showed the following:

- All the domains were managed by registrar Eranet International Limited.

- The oldest domain—main-sgl[.]com—was created on 21 May 2021. Meanwhile, the newest one—dash-spt[.]com—was created on 26 January 2022. That made all of them between 10 and 14 months old, possibly newly registered at the time they figured in money mule recruitment campaigns.



- It's also interesting to note that while most of the domains (12 out of 13) were recorded as registered in the U.S., one—zim-dash[.]com—indicated Russia as its registrant country. The 12 U.S.-based web properties, however, differed in terms of state. But what piqued our interest more was that only four of them indicated three identifiable U.S. states—MD for Maryland, NY for New York, and AL for Alabama. The remaining eight indicated what seemed to be nonexistent state abbreviations.

A Look at the IoCs' Current Status

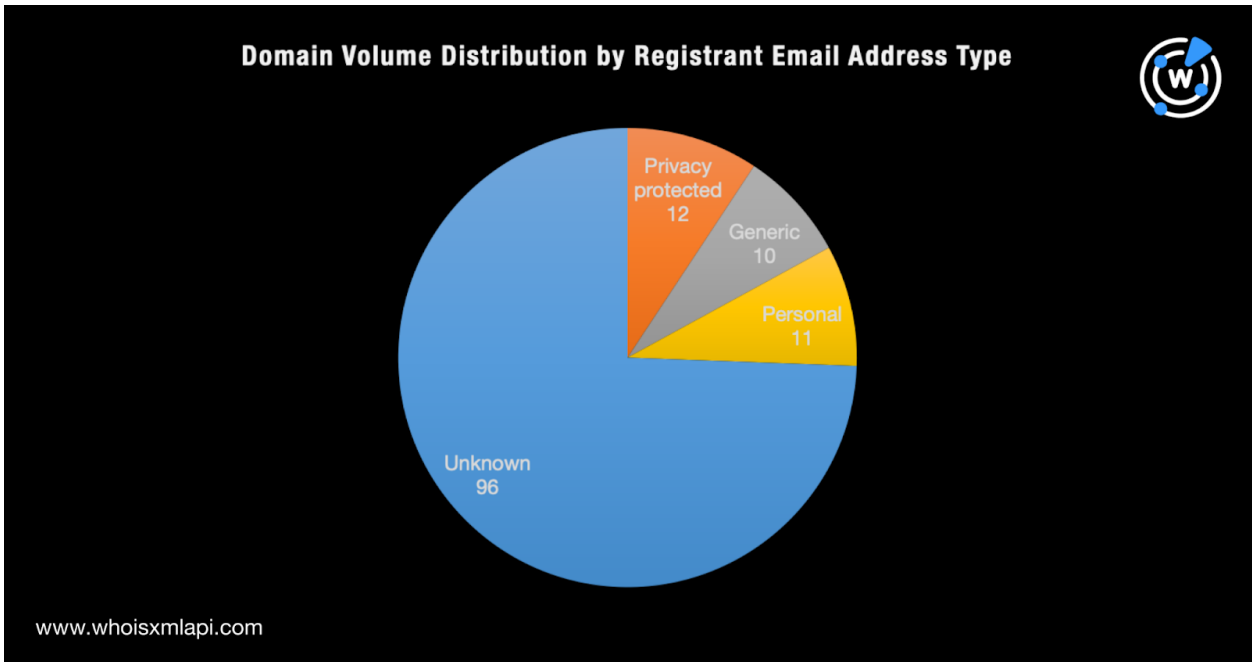
DNS lookups for the domains tagged as IoCs revealed that they all pointed to the same shared IP address 66[.]212[.]148[.]117. Geographically located in the U.S. and while considered nonmalicious to date, the host did point to 63 potentially connected domains.

A bulk WHOIS lookup for the 60+ domains showed that more than half (38 to be exact) were likely owned by legitimate businesses. The remaining web properties' registrant details, specifically email addresses, were left blank.

A closer look at the IoCs also let us identify 11 unique strings or string combinations that appeared among them, namely:

- amari + dash
- control + scorpio
- costa + account
- dashboard + zim
- dash + egreen
- dash + orient
- dash + satori
- dash + spt
- main + sgl
- navois + account
- zim + dash

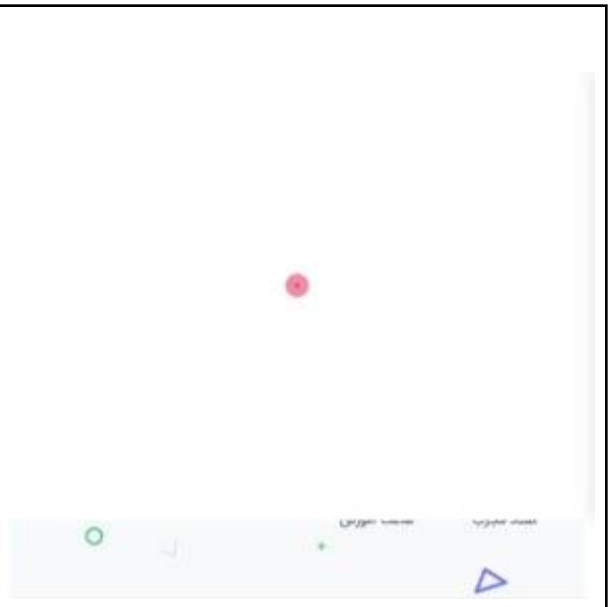
Using these as Domains & Subdomains Discovery search terms led to the discovery of another 418 possibly connected artifacts. While they were all deemed safe to access at the time of this writing, a bulk WHOIS lookup revealed that 12 were privacy protected, 10 used generic email addresses (e.g., info@company[.]TLD and sales@company[.]TLD), 11 used personal email addresses (i.e., mostly Gmail addresses), and the remaining 96 were left blank. Here's a graphical representation of the web properties' breakdown.



Subjecting nine unredacted personal registrant email addresses to historical reverse WHOIS searches allowed us to uncover 104 more domains. Of these, two—cmms[.]ir and mechanichome[.]com—turned out to be malicious according to various malware engines.

Screenshot lookups for these two dangerous web properties showed one hosted a computerized maintenance management system provider's website while the other appeared to be a mechanic's site. They could have been made to look like they belong to legitimate service providers but serve as malware hosts instead or may have been compromised.

Screenshot of cmms[.]ir



Screenshot of mechanichome[.]com

Since these two websites were live at the time of this writing, we decided to get some deeper context using website contacts lookup to gather their meta titles and descriptions, all of which were written in Persian. For mechanichome[.]com, we were also able to get company names, an email address, and a phone number.

—

Our IoC expansion exercise allowed us to uncover one IP address, 585 domains, and nine unredacted registrant email addresses that could have ties to the threat actors behind the seized domains. And with the help of exhaustive WHOIS, IP, and DNS data, we found two new malicious domains that could be considered IoCs.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

IoCs Identified by Bleeping Computer

- amari-dash[.]com
- control-scorpio[.]com
- costa-account[.]com
- dash-amari[.]com
- dashboard-zim[.]com
- dash-egreen[.]com
- dash-orient[.]com
- dash-satori[.]com
- dash-spt[.]com
- egreen-dash[.]com
- main-sgl[.]com
- navois-account[.]com
- orient-dash[.]com
- satori-dash[.]com
- scorpio-control[.]com
- spt-dash[.]com
- zim-dash[.]com

Sample Domains That Shared the IoCs' IP Host

- 1lib[.]ae
- 1lib[.]me
- alexandria[.]bigcity[.]com
- b-ok[.]as
- b-ok[.]lat
- backpage-insider[.]com
- backpage[.]be
- backpage[.]co[.]uk
- backpage[.]com
- backpage[.]cz
- backpage[.]gr
- backpage[.]ie
- backpage[.]it
- backpage[.]lt
- backpage[.]mx
- backpage[.]net
- backpage[.]pl
- backpage[.]pt
- backpage[.]si
- backpage[.]us

Sample Domains That Shared Unique Strings or String Combinations Seen among the IoCs

- dashamari[.]com
- dashsamari[.]com
- dashannamarie[.]com
- samarindashop[.]com
- dashdatamarine[.]com
- priodashuwamari[.]com
- anamariaanddashel[.]com
- samarindashipping[.]com
- samarindadashboard[.]com
- kudashudamarijuana[.]com

- vendashipercasamaringa[.]com[.]br
- scorpioncontrol[.]co
- scorpioncontrol[.]vg
- scorpiocontrol[.]com
- scorpioncontrol[.]icu
- scorpioncontrol[.]top
- scorpion-control[.]co
- scorpioncontrol[.]net
- scorpioncontrol[.]org
- scorpionscontrol[.]xn--mxtq1m
- scorpioncontrols[.]us
- scorpioncontrol[.]red
- scorpioncontrol[.]pro
- scorpioncontrol[.]com
- scorpioncontrols[.]ca
- scorpioncontrol[.]xyz
- scorpioncontrol[.]blue
- scorpioncontrol[.]info
- scorpioncontrols[.]com
- scorpioncontrol[.]live
- scorpioncontrol[.]club
- scorpioncontrol[.]casa
- scorpioncontrol[.]space
- scorpioncontrolaz[.]com
- txscorpioncontrol[.]com
- scorpion-controls[.]com
- nvscorpioncontrol[.]com
- azscorpioncontrol[.]com
- scorpioncontrolaz[.]pro
- gotscorpioncontrol[.]com
- getscorpioncontrol[.]com
- scorpioncontroller[.]com
- scorpionpestcontrol[.]ws
- tjsscorpioncontrol[.]com
- proscorpioncontrol[.]com
- scorpionpestcontrol[.]in
- scorpioncontrol101[.]com
- mesascorpioncontrol[.]com
- bestscorpioncontrol[.]com
- scorpionpetscontrol[.]com

Sample Personal Registrant Email Addresses

- mahdimXXXXX@gmail[.]com
- vadim[.]cXXXXX@gmail[.]com
- ShagXXXXX@gmail[.]com
- MKONTODXXXXX@GMAIL[.]COM
- PRIYAXXXXX@YAHOO[.]COM

Sample Domains That Shared Some of the Artifacts' Registrant Email Addresses

- cmms[.]ir
- mtpa[.]ir
- kzis[.]ir
- electrofermion[.]ir
- mkms[.]ir
- jalaliart[.]com
- bpmn[.]ir
- mechanichome[.]com
- costaccounting[.]ir
- rozhmaan[.]ir
- thecouragetochange[.]ir
- xana[.]ir
- jalalicarpet[.]ir
- kavazak[.]ir
- hoopak[.]ir
- idef[.]ir
- bpmtalk[.]ir
- coq[.]ir

- sciencetalk[.]ir
- irantpm[.]ir
- amozeshvatest[.]ir
- oee[.]ir
- colearning[.]ir
- shellmanfood[.]ir
- shelmanfood[.]ir
- gooyamedia[.]ir
- rozhmaan[.]com
- eanbar[.]ir
- rezghehalal[.]ir
- seoism[.]ir
- i-halal[.]ir
- halaltec[.]ir
- golrizanteb[.]ir
- wpgoup[.]ir
- parnianpolymer[.]com
- karnegar[.]com
- gooyamedia[.]com
- bpmtalks[.]com
- bpmtalk[.]com
- avijehdoor[.]com
- acupressure[.]ir
- klavye-music[.]com
- rahbordcmc[.]ir
- kikhoobe[.]com
- bihooshi[.]com
- ankengineering-intl[.]com
- khayatimehr[.]com
- hamilawyers[.]com
- rahbordcmc[.]com
- pmcmms[.]com