Unlike Its Namesake, Aoqin Dragon Isn't Mythical

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts and IoCs

Executive Report

Aoqin Dragon, like the mythical character it's named after, has recently been unearthed after nearly a decade of flying under the cybersecurity community's radar. Now believed to have been active since 2013, the advanced persistent threat (APT) group has targeted various organizations in the government, education, and telecommunications sectors.

SentinelLabs unveiled indicators of compromise (IoCs)—six IP addresses, 31 domains, and 155 malware hashes—related to the threat on 10 June 2022. We used the 37 web properties identified as IoCs as jump-off points and discovered other findings, including:

- 11 additional IP addresses to which the domain IoCs resolved, one of which turned out to be malicious
- 31 unredacted registrant email addresses from the domain IoCs' historical WHOIS records that revealed connections between a majority of the IoCs (IP addresses and domains alike)
- 22 additional domains that shared some of the domain IoCs' IP hosts, hinting at their dedicated nature, and past and current registrant email addresses

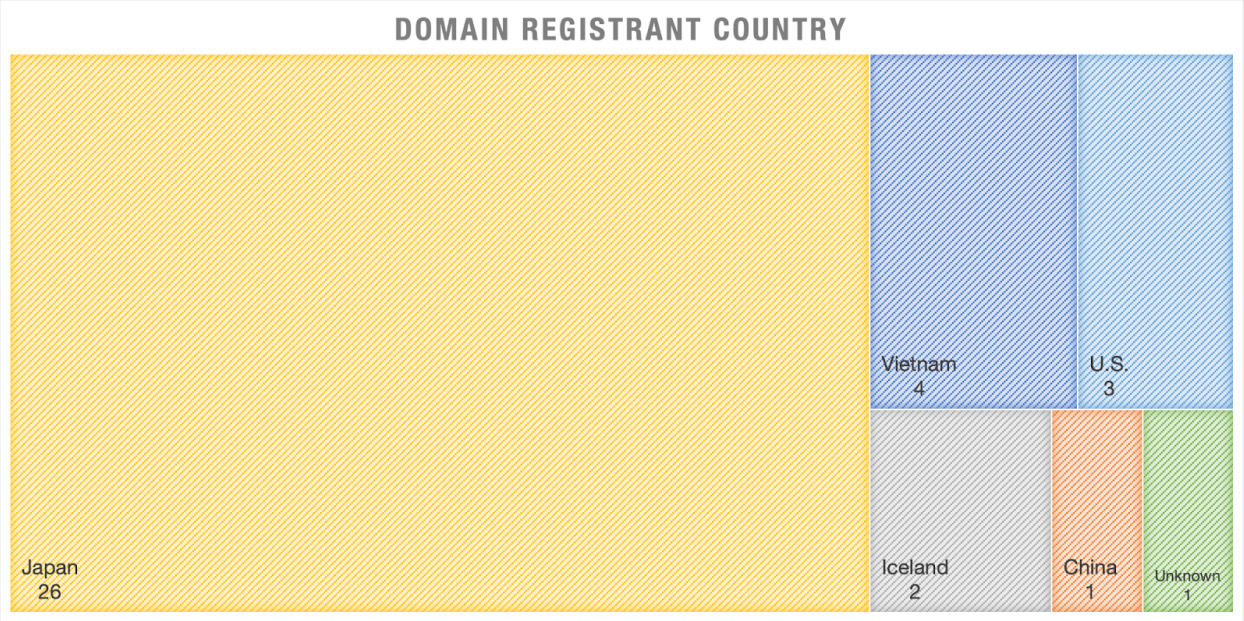
What Aoqin Dragon Has Been Up to Over the Years

Several organizations across the three sectors mentioned above throughout Southeast Asia have succumbed to Aoqin Dragon, which used old vulnerabilities, malicious executable files, and most recently, infected removable drives to get to their targets' networks.

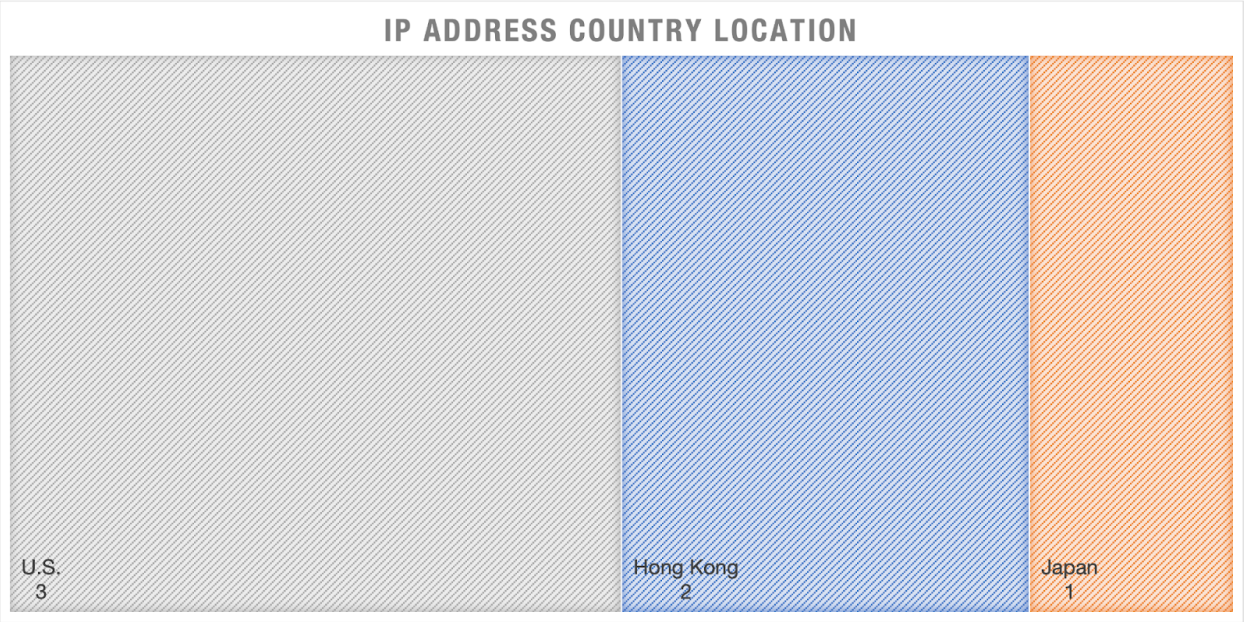
Apart from uncovering other suspicious domains and IP addresses that could have ties to the APT group, our deep dive also established connections between the publicized IoCs and additional artifacts.

What Our Deep Dive Revealed

We began our investigation by subjecting the domain IoCs to a bulk WHOIS lookup, which revealed that a majority of their owners claimed Japan as their registrant country. The rest were distributed across four countries and one didn't indicate its origin.



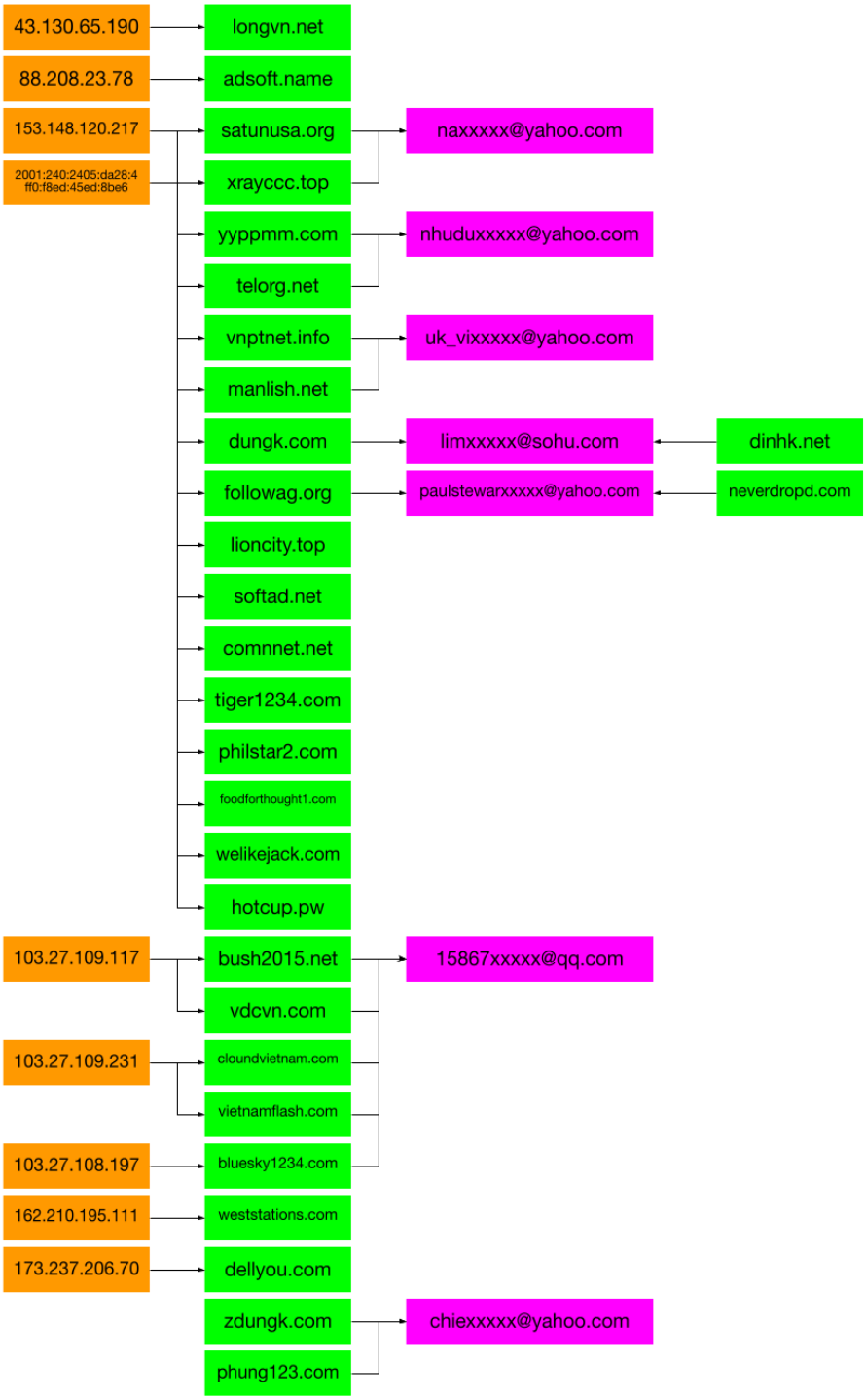
We also ran the IP address IoCs through a bulk IP geolocation lookup, which told us most of them originated from the U.S., Hong Kong, and Japan. One of the IP addresses—45[.]77[.]11[.]148—is currently tagged "malicious" by various malware engines based on a Threat Intelligence Platform (TIP) check.



In an effort to uncover possibly hidden connections, we looked at the domain IoCs' historical WHOIS records and uncovered 31 registrant email addresses. Using these as reverse WHOIS search terms led to the discovery of 22 additional domains.

While only one of the web properties turned out to be malicious, mapping the domains, IP addresses, and registrant email addresses identified as IoCs and potentially connected artifacts with one another showed interesting results, such as:

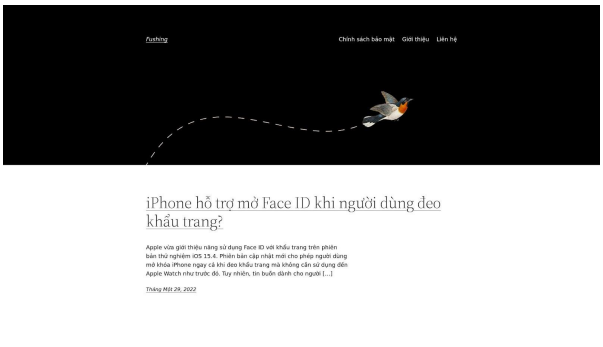
- A total of 16 of the domains shared a single IPv4 address—153[.]148[.]120[.]217. They also shared a single IPv6 address—2001[:]240[:]2405[:]da28[:]4ff0[:]f8ed[:]45ed[:]8be6.
- Satunusa[.]org and xrayccc[.]top shared a registrant email address; so did yyppmm[.]com and telorg[.]net and vnptnet[.]info and manlish[.]net
- Bush2015[.]net and vdcvn[.]com shared the IP address 103[.]27[.]109[.]117. Cloundvietnam[.]com and vietnamflash[.]com shared the host 103[.]27[.]109[.]231. Bluesky1234[.]com resolved to 103[.]27[.]108[.]197. And these five domains shared a registrant email address.
- Finally, zdungk[.]com and phung123[.]com shared a common registrant email address.


43.130.65.190
longvn.net
88.208.23.78
adsoft.name
153.148.120.217
satunusa.org
naxxxxx@yahoo.com
2001:240:2405:da28:4ff0:f8ed:45ed:8be6
xrayccc.top
yyppmm.com
nhuduxxxxx@yahoo.com
telorg.net
vnptnet.info
uk_vixxxxx@yahoo.com
manlish.net
dungk.com
limxxxxx@sohu.com
dinhk.net
followag.org
paulstewarxxxxx@yahoo.com
neverdropd.com
lioncity.top
softad.net
comnnet.net
tiger1234.com
philstar2.com
foodforthought1.com
welikejack.com
hotcup.pw
103.27.109.117
bush2015.net
15867xxxxx@qq.com
vdcvn.com
103.27.109.231
cloundvietnam.com
vietnamflash.com
103.27.108.197
bluesky1234.com
162.210.195.111
weststations.com
173.237.206.70
dellyou.com
zdungk.com
chiexxxxx@yahoo.com
phung123.com

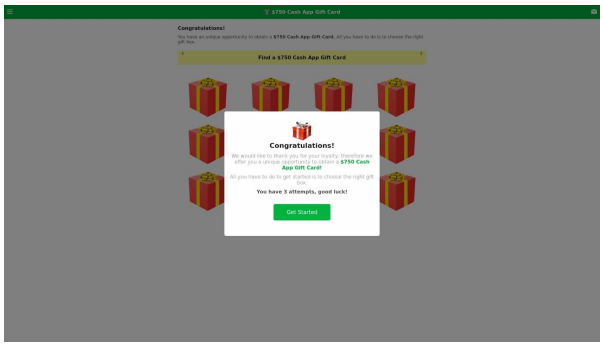
These relationships and others that have yet to be uncovered could be part of a single infrastructure—that which belongs or is closely connected to the Aoqin Dragon APT group.

—

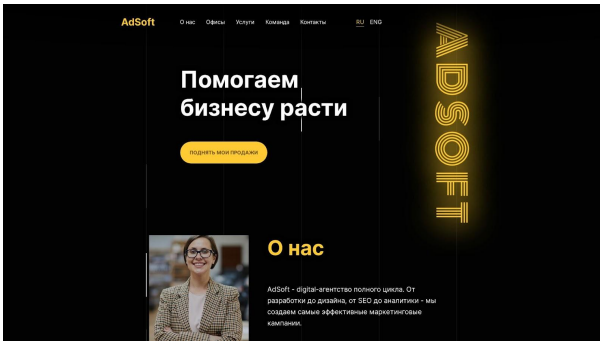
Using domain, IP, DNS, and threat intelligence tools allowed us to unravel important findings that could lead law enforcement agents one step closer to catching the threat actors behind Aoqin Dragon. Users, meanwhile, should remain wary of accessing identified domain IoCs—fushing[.]org, weststations[.]com, adsoft[.]name, phung123[.]com, and dinhk[.]net—as these continue to host live content based on our screenshot lookup results.



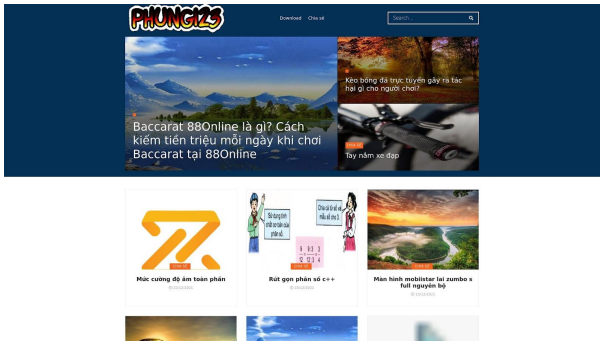
Screenshot of fushing[.]org



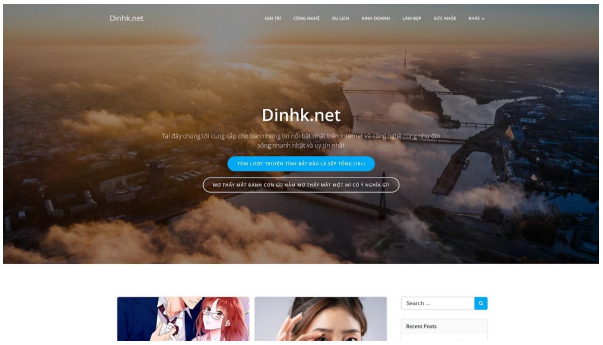
Screenshot of weststations[.]com



Screenshot of adsoft[.]name



Screenshot of phung123[.]com



Screenshot of dinhk[.]net

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

Unpublicized IP Address Resolutions of the Domain IoCs

- 153[.]148[.]120[.]217
- 103[.]27[.]109[.]117
- 212[.]32[.]237[.]101
- 103[.]27[.]109[.]231
- 103[.]27[.]108[.]197
- 88[.]208[.]23[.]78
- 43[.]130[.]65[.]190
- 173[.]237[.]206[.]70
- 157[.]245[.]58[.]209
- 2001[:]240[:]2405[:]da28[:]4ff0[:]f8ed[:]45ed[:]8be6
- 162[.]210[.]195[.]111

Unpublicized Domains That Shared the Domain IoCs' Unredacted Registrant Email Addresses

- my-miki[.]com
- kurashino-gorilla[.]com
- awaji11toko[.]com
- max-tradings[.]net
- shizuka-am[.]com
- nttgaika[.]com
- superwashvietnam[.]com
- dungcucobacbip[.]com
- tuoigi[.]com
- langlangdor[.]com
- trungtambaohanhtulanhsharp[.]com
- liugems[.]com
- rausachgiasi[.]com
- luyenthikhoihv[.]com
- tocdepvn[.]com
- nokiasaigon[.]com
- naihuou[.]com
- dichvu3g[.]com
- autochesslegends[.]com
- tieungaodailuc[.]com

- nhatkiemdoantinh[.]com
- btnrocket[.]com

Registrant Email Addresses Shared by the Domain IoCs

Note that portions of each email address were redacted for privacy-related reasons.

- azaxxx[.]xx@yandex[.]com
- uk_vixxxxx@yahoo[.]com
- katxxxxx@topcast[.]jp
- chiexxxxx@yahoo[.]com
- xxxxx@onamae[.]com
- 15867xxxxx@qq[.]com
- liminxxxxx@163[.]com
- YuMing@YinSixxxxx[.]AliYun[.]com
- ha[.]muxxxxx@yandex[.]com
- 18319xxxxx@163[.]com
- hulxxxxx@163[.]com
- sxxxxx@126[.]com
- nhuduxxxxx@yahoo[.]com
- blueeyxxxxx@yahoo[.]com
- xxxxx@yahoo[.]com
- maskxxxxx@yahoo[.]com
- 18278xxxxx@qq[.]com
- skdhxxxxx@163[.]com
- blueeyes_66xxxxx@yahoo[.]com
- paulstewarxxxxx@yahoo[.]com
- zhaojinyuxxxxx@163[.]com
- dangkyhoc[.]vixxxxx@gmail[.]com
- naxxxxx@yahoo[.]com
- xxxxxi@ais-brain[.]jp
- adbcbmfxxxxx@gmail[.]com
- limxxxxx@sohu[.]com
- bushucxxxxx@hotmail[.]com
- limxxxxx@sohu[.]com
- phongfxxxxx@gmail[.]com
- dljmicdxxxxx@idp[.]email
- 133788xxxxx@189[.]cn