DomainTools And Digital Archeology: A Look At RotaJakiro

domaintools.com/resources/blog/domaintools-and-digital-archeology-a-look-at-rotajakiro

Background

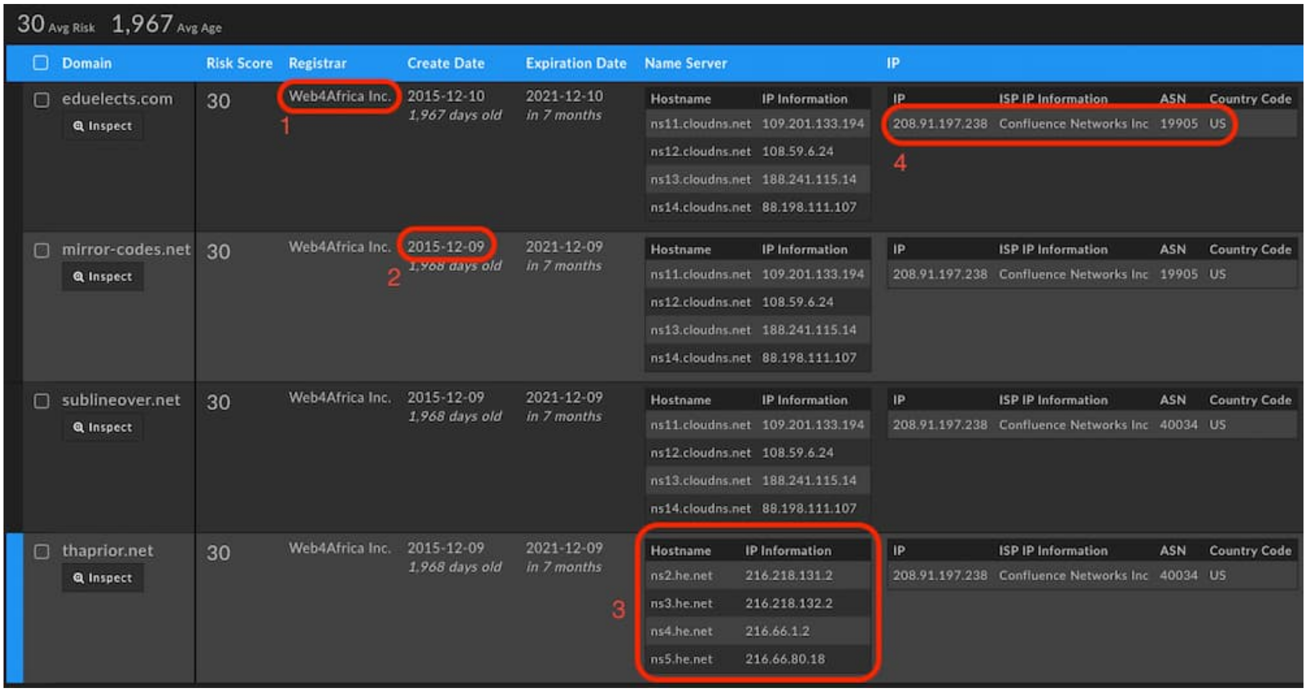
On April 21, 2021, Netlab released an excellent report on a malware sample they dubbed RotaJakiro, a long-lived backdoor targeting 64-bit Linux systems with 0 detections on VirusTotal. This backdoor used a number of techniques to remain unnoticed and the craftiness of the sample piqued the attention of the DomainTools Research Team. Netlab's post ended talking about how analysis of the binary was just the tip of the iceberg in discovering what this sample was about and that is where we feel that DomainTools, with our thorough historical data set of over 20 years of Whois and DNS information, had to take a look. For analysis on the binary itself, we suggest reading their excellent post while we concentrate here on one of our specialties: digital archeology.

Initial Indicators

In this instance, the samples found by Netlab were first added to VirusTotal in 2018. As mentioned, none of them were detected by any of the engines VirusTotal employs. These samples all called out to C2 infrastructure of the following domains:

```
news.thaprior.net
blog.eduelects.com
cdn.mirror-codes.net
status.sublineover.net
```

A quick look in passive DNS shows that these domains only have these subdomains listed and they do not appear to be a part of any Dynamic DNS system so we can assume that the SLDs are owned by the same operator. We'll look more at passive DNS later, but for now we can throw these domains into Iris Investigate to see more about their intrinsic properties.



30 Avg Risk 1,967 Avg Age

□ Domain	Risk Score	Registrar	Create Date	Expiration Date	Name Server	IP
□ eduelects.com Inspect	30	Web4Africa Inc.	2015-12-10 *1,967 days old*	2021-12-10 *in 7 months*	Hostname IP Information ns11.cloudns.net 109.201.133.194 ns12.cloudns.net 108.59.6.24 ns13.cloudns.net 188.241.115.14 ns14.cloudns.net 88.198.111.107	IP ISP IP Information ASN Country Code 208.91.197.238 Confluence Networks Inc 19905 US
□ mirror-codes.net Inspect	30	Web4Africa Inc.	2015-12-09 *1,968 days old*	2021-12-09 *in 7 months*	Hostname IP Information ns11.cloudns.net 109.201.133.194 ns12.cloudns.net 108.59.6.24 ns13.cloudns.net 188.241.115.14 ns14.cloudns.net 88.198.111.107	IP ISP IP Information ASN Country Code 208.91.197.238 Confluence Networks Inc 19905 US
□ sublineover.net Inspect	30	Web4Africa Inc.	2015-12-09 *1,968 days old*	2021-12-09 *in 7 months*	Hostname IP Information ns11.cloudns.net 109.201.133.194 ns12.cloudns.net 108.59.6.24 ns13.cloudns.net 188.241.115.14 ns14.cloudns.net 88.198.111.107	IP ISP IP Information ASN Country Code 208.91.197.238 Confluence Networks Inc 40034 US
□ thaprior.net Inspect	30	Web4Africa Inc.	2015-12-09 *1,968 days old*	2021-12-09 *in 7 months*	Hostname IP Information ns2.he.net 216.218.131.2 ns3.he.net 216.218.132.2 ns4.he.net 216.66.1.2 ns5.he.net 216.66.80.18	IP ISP IP Information ASN Country Code 208.91.197.238 Confluence Networks Inc 40034 US

First is the use of the Web4Africa registrar. This registrar has just a little over 18,000 domains associated with it so the frequency of registration is rather low. Second, we see the registration dates are about the same for all of the domains being from December 9th and 10th of 2015. This aligns with the research from the Netlab report and may indicate that there are actually older samples to be found in the wild. Third, we see that all have the same nameservers except for one domain. Outliers are always useful as they often link to additional connections elsewhere in the broader domain name data set. Lastly, the use of the Confluence Networks IP for their apex A record which is only slightly valuable. This is a parking page IP address and makes sense as the operator of this backdoor used subdomains that all had A records to a specific IP address for C2.

Summary of Additional Information and What it Tells Us

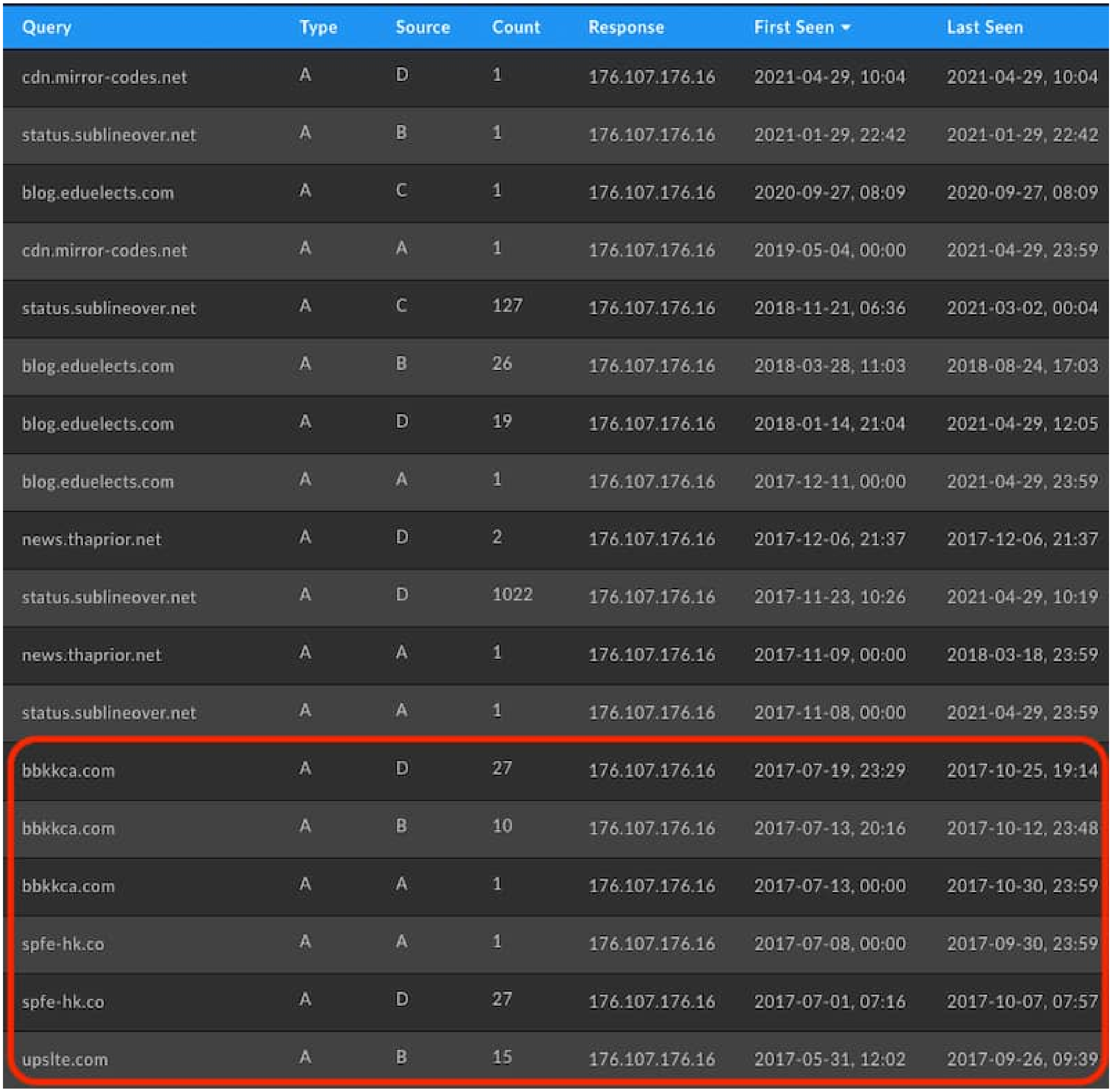
Web4Africa Registrar	Low volume registrar.

Grouped Create Date	Grouped create date plus low volume registrar means we can hunt on the same day for additional registrations.
Outlier Nameserver	Outliers often lead to additional infrastructure as they have been treated special for a reason.
Parking Page IP For Apex Domain	Good to point out simply because it can be a rabbit hole.

Diving Deeper Than Domains

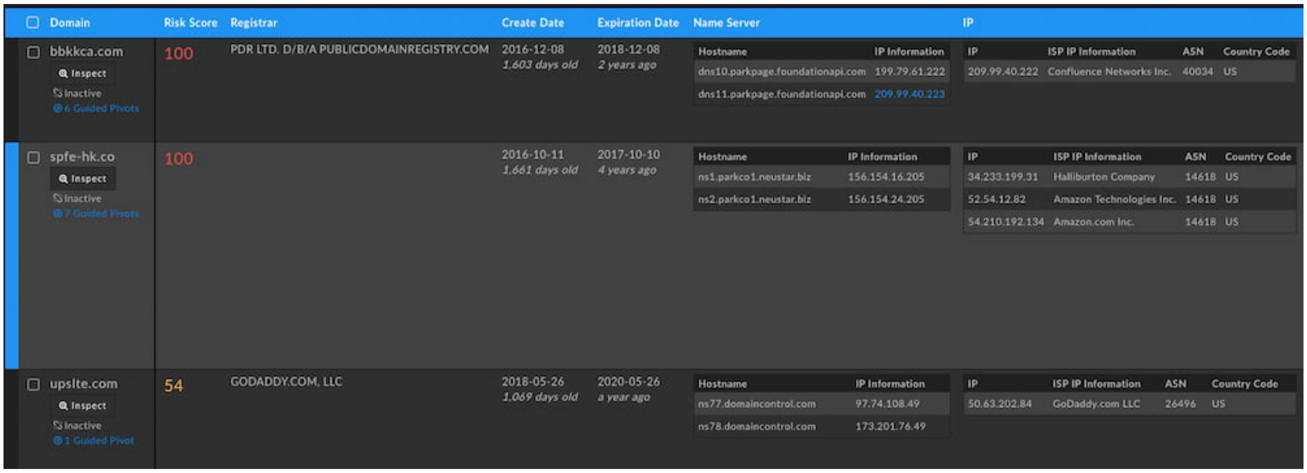
The first step from here is we look at Whois history. In this case, privacy protection has been in place since the domains were first registered in 2015. Most importantly we can tell that because the domain has never been allowed to expire,these weren’t domains that were dropped and re-registered. This lets us know that **the same person has owned these domains since 2015**. That is an important distinction to make as adversaries are increasingly aware that getting a drop catch domain is a nice way to immediately “age” a domain so it goes undetected as many machine learning algorithms rely heavily on registration date to determine malicious intent. We have certainly found that an overwhelming number of attacks come from newly registered domains in our analysis.

Since Whois history provides minimal additional points to pivot on, we can then turn to passive DNS. This data set of passively collected query and response pairs from recursive resolvers around the Internet shows a first and last seen entry for any pair along with a count. This can help determine both breadth of use as well as when something first began and was last seen operating. In the case of the IP address used for all four of the subdomains that were C2 infrastructure, we get the following list that shows activity as early as November 08, 2017 and as recently as April 29, 2021 which is the time of this writing. In addition to that we get three new domains pointing to the exact same IP address just a few months prior in 2017.



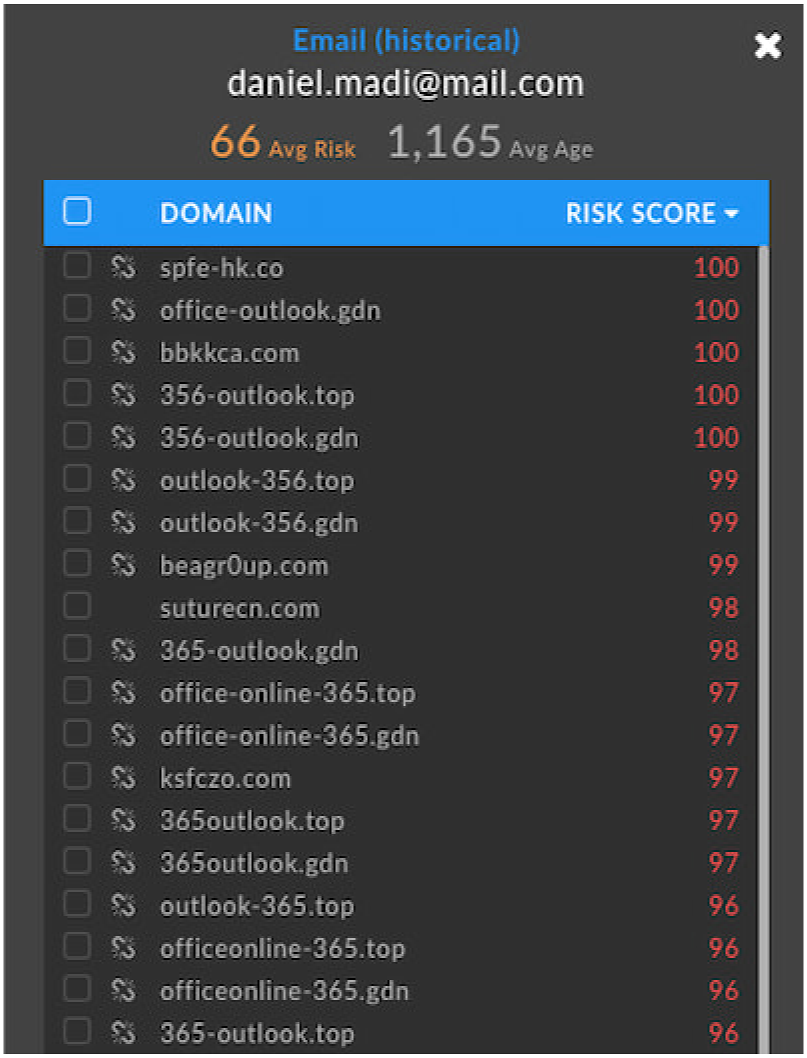
Query	Type	Source	Count	Response	First Seen ▾	Last Seen
cdn.mirror-codes.net	A	D	1	176.107.176.16	2021-04-29, 10:04	2021-04-29, 10:04
status.sublineover.net	A	B	1	176.107.176.16	2021-01-29, 22:42	2021-01-29, 22:42
blog.eduelects.com	A	C	1	176.107.176.16	2020-09-27, 08:09	2020-09-27, 08:09
cdn.mirror-codes.net	A	A	1	176.107.176.16	2019-05-04, 00:00	2021-04-29, 23:59
status.sublineover.net	A	C	127	176.107.176.16	2018-11-21, 06:36	2021-03-02, 00:04
blog.eduelects.com	A	B	26	176.107.176.16	2018-03-28, 11:03	2018-08-24, 17:03
blog.eduelects.com	A	D	19	176.107.176.16	2018-01-14, 21:04	2021-04-29, 12:05
blog.eduelects.com	A	A	1	176.107.176.16	2017-12-11, 00:00	2021-04-29, 23:59
news.thaprior.net	A	D	2	176.107.176.16	2017-12-06, 21:37	2017-12-06, 21:37
status.sublineover.net	A	D	1022	176.107.176.16	2017-11-23, 10:26	2021-04-29, 10:19
news.thaprior.net	A	A	1	176.107.176.16	2017-11-09, 00:00	2018-03-18, 23:59
status.sublineover.net	A	A	1	176.107.176.16	2017-11-08, 00:00	2021-04-29, 23:59
bbkkca.com	A	D	27	176.107.176.16	2017-07-19, 23:29	2017-10-25, 19:14
bbkkca.com	A	B	10	176.107.176.16	2017-07-13, 20:16	2017-10-12, 23:48
bbkkca.com	A	A	1	176.107.176.16	2017-07-13, 00:00	2017-10-30, 23:59
spfe-hk.co	A	A	1	176.107.176.16	2017-07-08, 00:00	2017-09-30, 23:59
spfe-hk.co	A	D	27	176.107.176.16	2017-07-01, 07:16	2017-10-07, 07:57
upslte.com	A	B	15	176.107.176.16	2017-05-31, 12:02	2017-09-26, 09:39

While this is interesting, it's important not to jump to conclusions and tie this directly to the other domains. For one, the IP is tied to a Ukraine and Netherlands based VPS provider called DeltaHost. A VPS provider rents out servers and with that IP addresses. This IP could simply have been recycled that month when the operator behind RotaJakiro decided to become active. Secondly, there are no subdomain patterns that match the naming convention of the domains prior. Given that this IP has only ever hosted the confirmed RotaJakiro C2 domains and these new domains, though, it behooves any analyst to take a closer look.



□ Domain	Risk Score	Registrar	Create Date	Expiration Date	Name Server	IP
□ bbkkca.com Inspect Inactive 6 Guided Pivots	100	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	2016-12-08 *1,603 days old*	2018-12-08 *2 years ago*	Hostname / IP Information dns10.parkpage.foundationapi.com 199.79.61.222 dns11.parkpage.foundationapi.com 209.99.40.223	IP / ISP IP Information / ASN / Country Code 209.99.40.222 Confluence Networks Inc. 40034 US
□ spfe-hk.co Inspect Inactive 7 Guided Pivots	100		2016-10-11 *1,661 days old*	2017-10-10 *4 years ago*	Hostname / IP Information ns1.parkco1.neustar.biz 156.154.16.205 ns2.parkco1.neustar.biz 156.154.24.205	IP / ISP IP Information / ASN / Country Code 34.233.199.31 Halliburton Company 14618 US 52.54.12.82 Amazon Technologies Inc. 14618 US 54.210.192.134 Amazon.com Inc. 14618 US
□ upslte.com Inspect Inactive 1 Guided Pivot	54	GODADDY.COM, LLC	2018-05-26 *1,069 days old*	2020-05-26 *a year ago*	Hostname / IP Information ns77.domaincontrol.com 97.74.108.49 ns78.domaincontrol.com 173.201.76.49	IP / ISP IP Information / ASN / Country Code 50.63.202.84 GoDaddy.com LLC 26496 US

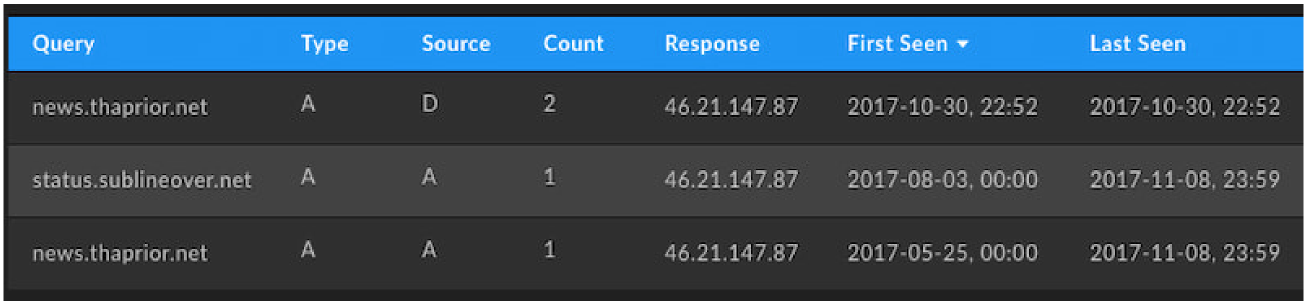
Unfortunately, these three additional domains do not provide anything that can definitively tie them to the other domains. They lack any overlapping times in passive DNS records and their registration patterns are different. One oddity however is their Risk Score of 100. The DomainTools Risk Score is informed by a number of things, but a score of 100 is indicative of a domain being included on a blocklist for a previous report of known badness. Looking at historical Whois for these domains we see them with a registrant email of daniel.madi@mail[.]com who is tied to 88 Office 365 based phishing domains.



Email (historical)
daniel.madi@mail.com
66 Avg Risk 1,165 Avg Age

□ DOMAIN	RISK SCORE ▾
□ spfe-hk.co	100
□ office-outlook.gdn	100
□ bbkkca.com	100
□ 356-outlook.top	100
□ 356-outlook.gdn	100
□ outlook-356.top	99
□ outlook-356.gdn	99
□ beagr0up.com	99
□ suturecn.com	98
□ 365-outlook.gdn	98
□ office-online-365.top	97
□ office-online-365.gdn	97
□ ksfczo.com	97
□ 365outlook.top	97
□ 365outlook.gdn	97
□ outlook-365.top	96
□ officeonline-365.top	96
□ officeonline-365.gdn	96
□ 365-outlook.top	96

Given the complexity and stealth of the RotaJakiro backdoor it seems unlikely that such a noisy phishing campaign would be so easily tied to such a quiet operation. If we were to tie these together it would be with **extremely low** confidence. We feel as researchers that it is much more likely that DeltaHost recycled this VPS IP address shortly after the blocklisting of these domains and it was coincidentally used in other criminal activity and that the IP address was picked up by the RotaJakiro operators. In support of this, passive DNS records show that one of these older domains was suspended just before the C2 domains for RotaJakiro began operating on that IP address. Passive DNS also shows the RotaJakiro C2 domains existing on other IP addresses prior to moving to DeltaHost. Both of these facts support the theory that these are separate.

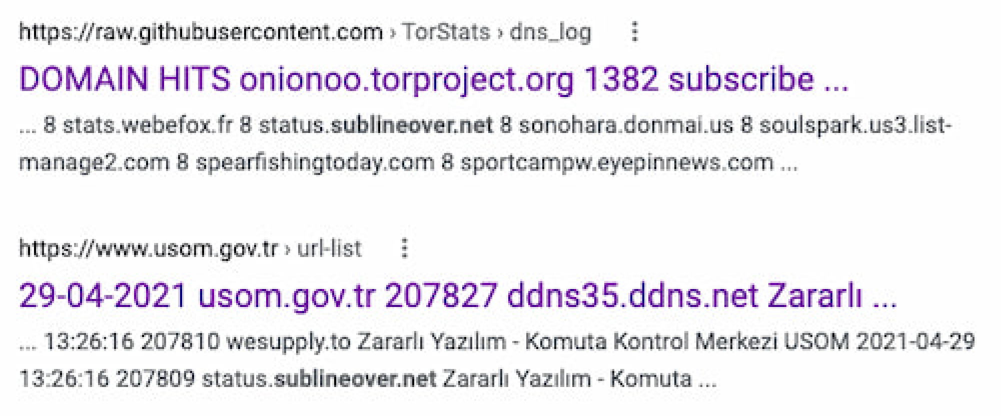


Query	Type	Source	Count	Response	First Seen ▾	Last Seen
news.thaprior.net	A	D	2	46.21.147.87	2017-10-30, 22:52	2017-10-30, 22:52
status.sublineover.net	A	A	1	46.21.147.87	2017-08-03, 00:00	2017-11-08, 23:59
news.thaprior.net	A	A	1	46.21.147.87	2017-05-25, 00:00	2017-11-08, 23:59

This IP now belongs to Hivelocity, a small cloud provider that has only owned the IP address since 2019 according to the create date on the IP Whois record for their subnet. According to historical IP Whois information, Hivelocity acquired this range from Swiftway after acquiring the company which had server locations in the Netherlands. The IP shown, 46.21.147[.]87 is still geolocated in the Netherlands.

Unfortunately, we also cannot find any connections between the C2s mentioned in Avast's Torii botnet report from 2018 and the domains in the RotaJakiro report. Netlab did mention similarities between RotaJakiro and the Torii botnet in their operation. If there had been a tie between those domains even and the daniel.madi@mail[.]com domains we could increase our confidence in them belonging to the same operator.

Sometimes when reaching a dead end on infrastructure databases the best thing for us as analysts to do is turn to traditional search engines. Throwing in the initial C2 domains we discovered and a few interesting hits came up. The first is a link to a 2016 repository of Tor DNS logs that show to us that this domain has at least been accessed since 2016. The second is from a Turkish government website and is a URL list in XML format. The domains are mentioned as appearing on April 29, 2021, same as the time of this writing, from the Zararlı Yazılım Komuta Kontrol Merkezi which is Turkish for Malware Command Control Center, likely having been an ingestion of the original Netlab report.



https://raw.githubusercontent.com › TorStats › dns_log

DOMAIN HITS onionoo.torproject.org 1382 subscribe ...

... 8 stats.webefox.fr 8 status.**sublineover.net** 8 sonohara.donmai.us 8 soulspark.us3.list-manage2.com 8 spearfishingtoday.com 8 sportcampw.eyepinnews.com ...

https://www.usom.gov.tr › url-list

29-04-2021 usom.gov.tr 207827 ddns35.ddns.net Zararlı ...

... 13:26:16 207810 wesupply.to Zararlı Yazılım - Komuta Kontrol Merkezi USOM 2021-04-29 13:26:16 207809 status.**sublineover.net** Zararlı Yazılım - Komuta ...

Summary of Additional Information and What It Tells Us

C2 Domains Never Lapsed	Same registrant has owned these domains since their initial registration in 2015.
IP On DeltaHost VPS Provider	VPS providers share resources amongst clients so unless we can overlap some records we cannot confirm that a single IP ties two events together.
IP Used In Other Maliciousness	The VPS IP was used, but never overlapped, with another set of malicious domains doing Office 365 phishing with entirely different registration patterns and levels of noise.
C2s Previously Used A Different IP	During the time where there could have been overlap with other maliciousness, the C2s used an IP on a different VPS provider in the Netherlands.
No Infrastructure Tie To Match Code Ties	The Torii Botnet mentioned by Netlab does not have any infrastructure ties to RotaJakiro.
Domain Resolving In 2016	Although resolving as early as 2016, we cannot confirm that it resolved to the same IP as the DeltaHost IP.

Conclusion

Although we were unable to tie the Netlab report on RotaJakiro to another operator, we have produced a good amount of evidence and potential conclusions for further analysis. We've been able to confirm timelines from the Netlab report as well as mark key oddities for further avenues of investigation. We were also able to identify additional IP addresses which had been previously used by the C2 domains and would lower the threshold of confidence for tying this to previous maliciousness. When all else brought us to a dead end we were able to expand upon our original timeline thanks to good old fashioned OSINT using classic search engines. Whenever coming across reports like this we hope that customers can find DomainTools useful in the practice of digital archeology.