# ThreatConnect Research Roundup: Suspected Naikon DGA Domains

threatconnect.com/blog/tag/naikon/

ThreatConnect Research Team

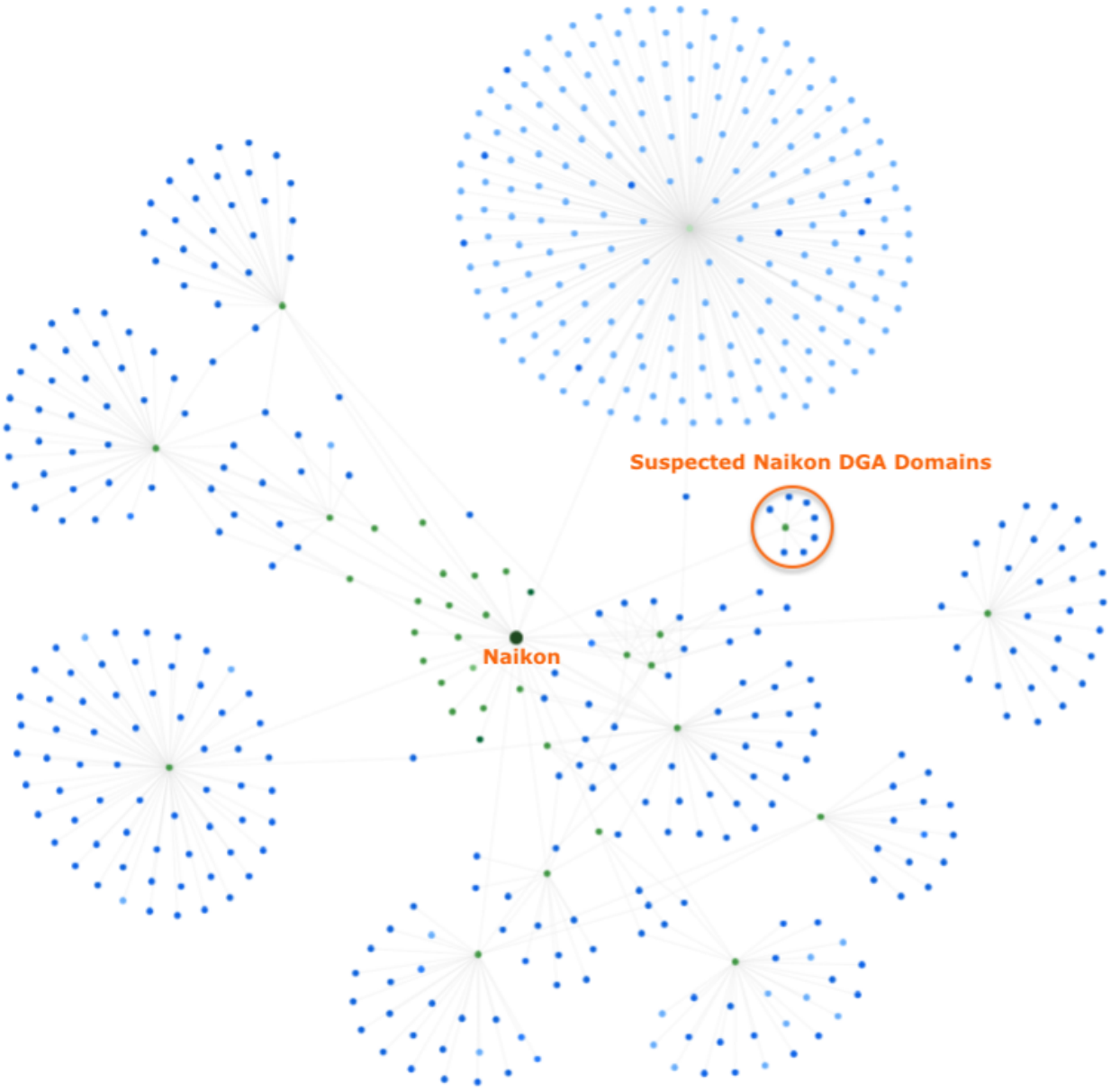

**May 28 2020 Edition**

Howdy, and welcome to the ThreatConnect Research Roundup, a collection of recent findings by our Research Team and items from open source publications that have resulted in Observations of related indicators across ThreatConnect's CAL™ (Collective Analytics

Layer).

Note: Viewing the pages linked in this blog post requires a ThreatConnect account.

**Roundup Highlight: Suspected Naikon DGA Domains**




*Naikon related intelligence in ThreatConnect Common Community*

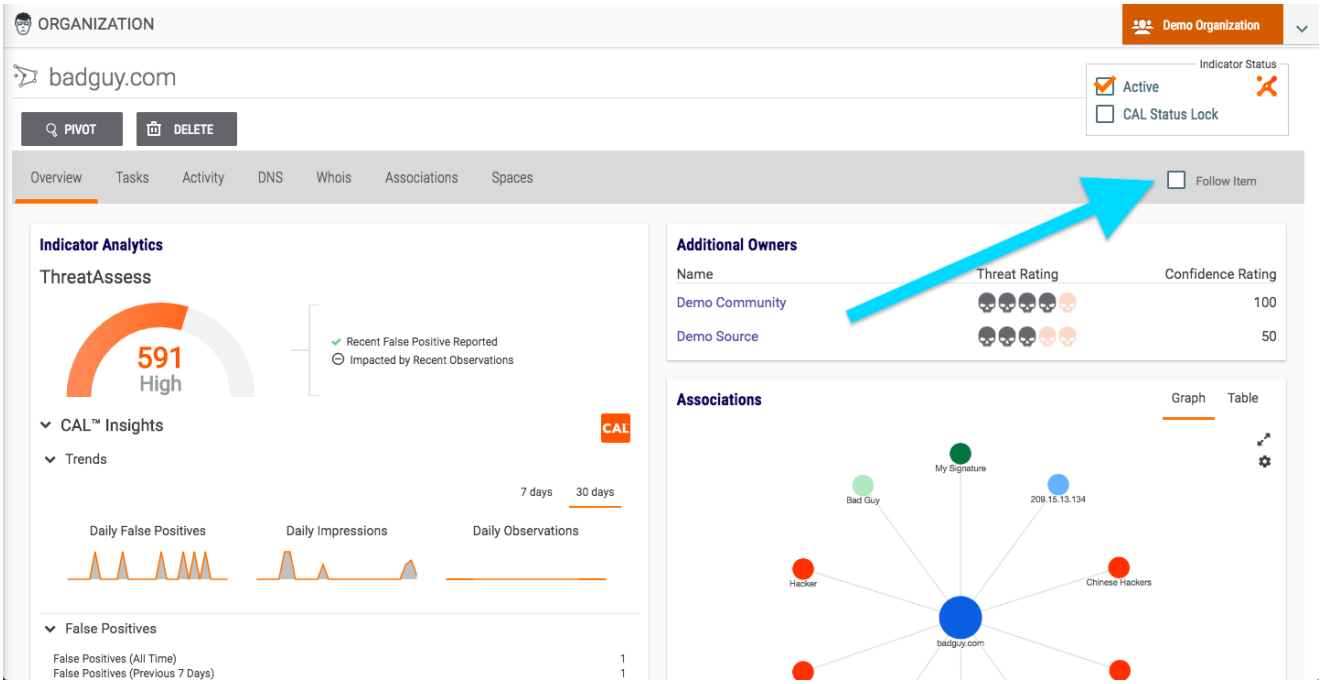
Our highlight in this week's Roundup is Incident 20200519B: Suspected Naikon DGAs. After reviewing research published by Check Point and Kaspersky, our team identified additional suspected Naikon DGA domains consistent with registration and hosting data of previously identified Naikon domains:

- dwjmannje[.]com (shared IP with previously identified forcejoyt[.]com)
- ujghr63revf[.]org (shared IP with previously identified rrgwmmwgk[.]com)
- 76rythb5435[.]org (shared IP with previously identified rrgwmmwgk[.]com)
- 46vev33g81[.]org (shared registration data with ujghr63revf[.]org and 76rythb5435[.]org)

Additional domains identified based on registration and hosting consistencies:

- etnwtmrkh[.]com
- nrtfmwhim[.]com
- wahatmrjn[.]com

We don't have any information on the extent to which, if any, these domains have been used maliciously. However, given the commonalities identified, these domains merit scrutiny as possible Naikon DGA domains.




To receive ThreatConnect notifications about any of the above, remember to check the "Follow Item" box on that item's Details page.

**ThreatConnect Research Team Intelligence:**

These are items recently created or updated in the ThreatConnect Common Community by our Research Team. They include threat actor profiles, malware families, campaigns, signatures, and incidents based on our research and threat hunting activities.

- 20200526B: Possible APT34 Domain lebworld[.]us ThreatConnect Research identified the possible APT34 / Helix Kitten / OilRig domain lebworld[.]us, which has registration and hosting consistencies with previously identified APT34 infrastructure. This domain was registered through MonoVM on May 18 2020 using jame@protonmail[.]com, and is hosted on a probable dedicated server at 23.19.227[.]117. We don't have any information on the extent to which, if any, this infrastructure has been used maliciously. It's important to note that the identified registration and hosting consistencies are not enough to definitively attribute this infrastructure to APT34.
- 20200526A: Server Support Domains Registered Through ITitch ThreatConnect Research identified two domains — login-server[.]support and domain-server[.]support — that were registered through ITitch within about a minute of each other on May 22 2020 and most likely were registered by the same actor. Start of authority (SOA) records show the login-server[.]support domain was registered using trabant@cock[.]li. This domain is currently hosted on a probable dedicated server at 102.152[.]107 and, per urlscan.io, redirects to CNBC's legitimate website.

SOA records show domain-server[.]support was registered using jirajira@cock[.]li. This domain is hosted on a probable dedicated server at 185.10.68[.]163, has switched to using its own name server, and hosts a mail-in-a-box server.

At this time we don't have any information indicating the extent to which these domains have been used maliciously.

**Technical Blogs and Reports Incidents with Active and Observed Indicators:**

The ThreatConnect Technical Blogs and Reports Source is a curated collection of open source blogs and reports that are automatically aggregated and parsed for Indicators on a daily basis. Incidents listed here are associated to one or more Indicators with an Active status and at least one global Observation across the ThreatConnect community. These analytics are provided by ThreatConnect's CAL™ (Collective Analytics Layer).

- Cyber-Criminal espionage Operation insists on Italian Manufacturing (Source: https://yoroi.company/research/cyber-criminal-espionage-operation-insists-on-italian-manufacturing/)
- Update on JavaScript Skimmer Enhancements (Source: https://www.zscaler.com/blogs/research/update-javascript-skimmer-enhancements)
- Emotet C2 and RSA Key Update – 05/25/2020 14:15 (Source: https://paste.cryptolaemus.com/emotet/2020/05/25/emotet-c2-rsa-update-05-25-20-1.html)