ThreatConnect Research Roundup: Probable Sandworm Infrastructure

threatconnect.com/blog/threatconnect-research-roundup-probable-sandworm-infrastructure

June 12, 2020

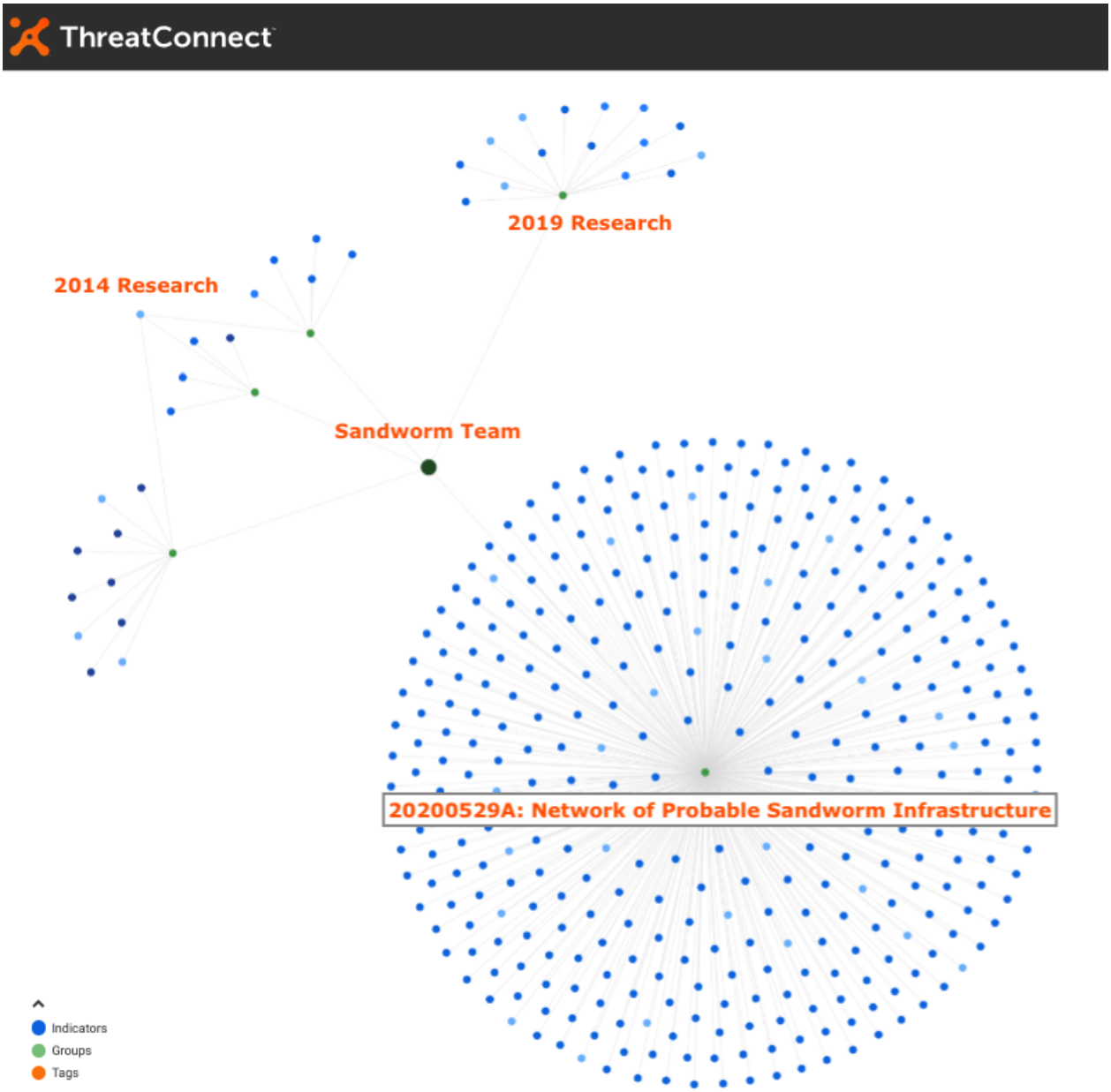
June 12 2020 Edition

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.

In this edition, we cover:

Roundup Highlight: Probable Sandworm Infrastructure



Sandworm Related Intelligence in ThreatConnect

Our highlight in this Roundup is Incident 20200529A: Network of Probable Sandworm Infrastructure. Sandworm, also known as Sandworm Team, Quedagh, and VOODOO BEAR, is a Russian threat actor group that has historically targeted energy, industrial, government, and media organizations in Ukraine.

ThreatConnect Research, in conjunction with industry colleagues, identified a network of probable Sandworm infrastructure dating back to at least 2018. NSA released a report on Sandworm activity on May 29 2020 that identified the domain hostapp.be (IPs: 95.216.13[.]196, 103.94.157[.]5). This domain was registered on December 24 2018 through Njalla. In reviewing historical registrations, we were only able to identify seven other domains that were registered on that date through Njalla. While we were unable to directly associate any of these domains to hostapp.be due to its lack of a creation timestamp, three of the other domains — fbapp[.]top, fbapp[.]info, fbapp[.]link — appeared notable and possibly related.

We reviewed the hosting history, subdomains, and co-locations for these additional domains and to-date have identified a network of 30 domains, 17 IPs, and hundreds of subdomains that we assess probably are related with largely historic Sandworm activity. Further indicative of the probable association to Sandworm, some of the identified domains, such as hostapp[.]art and hostapp[.]link, share strings with the domain identified in NSA's report.

In reviewing subdomains for the identified domains, many subdomains strings were reused across the domains. Many Twitter, Google, and Facebook-related subdomains were identified. The following notable subdomain strings were also identified and possibly are indicative of operational targets, themes, or affected countries:

passport.abv.bg.*
passport.above.bg.*
mail.bg.*
accounts.ukr.net.*
mail.adm.khv.ru.*

It's important to note that while the identified infrastructure is largely historic, at least two domains — userarea[.]click (46.4.10[.]58) and userarea[.]eu (185.226.67[.]190) — and/or their subdomains were actively resolving in May 2020. At this time, we do not have any additional insight into how or against whom this infrastructure has been operationalized.

Update 5/31/20

ThreatConnect Research identified another set of domains and IPs that are a part of this network of probable Sandworm infrastructure. The following domains were registered through Njalla at essentially the same time as userarea[.]click and userarea[.]eu and are currently hosted on dedicated servers:

userarea[.]top (194.117.236[.]33)
userarea[.]in (5.255.90[.]243)

Three other domains were registered through Njalla about two and a half hours later:

myaccount[.]click (185.76.68[.]70)
myaccount[.]one (92.62.139[.]114)
webcache[.]one (195.211.197[.]25)

Notably, four of these IP addresses were identified by GreyNoise as exploiting the Exim vulnerability CVE-2019-10149.

Update 6/3/20

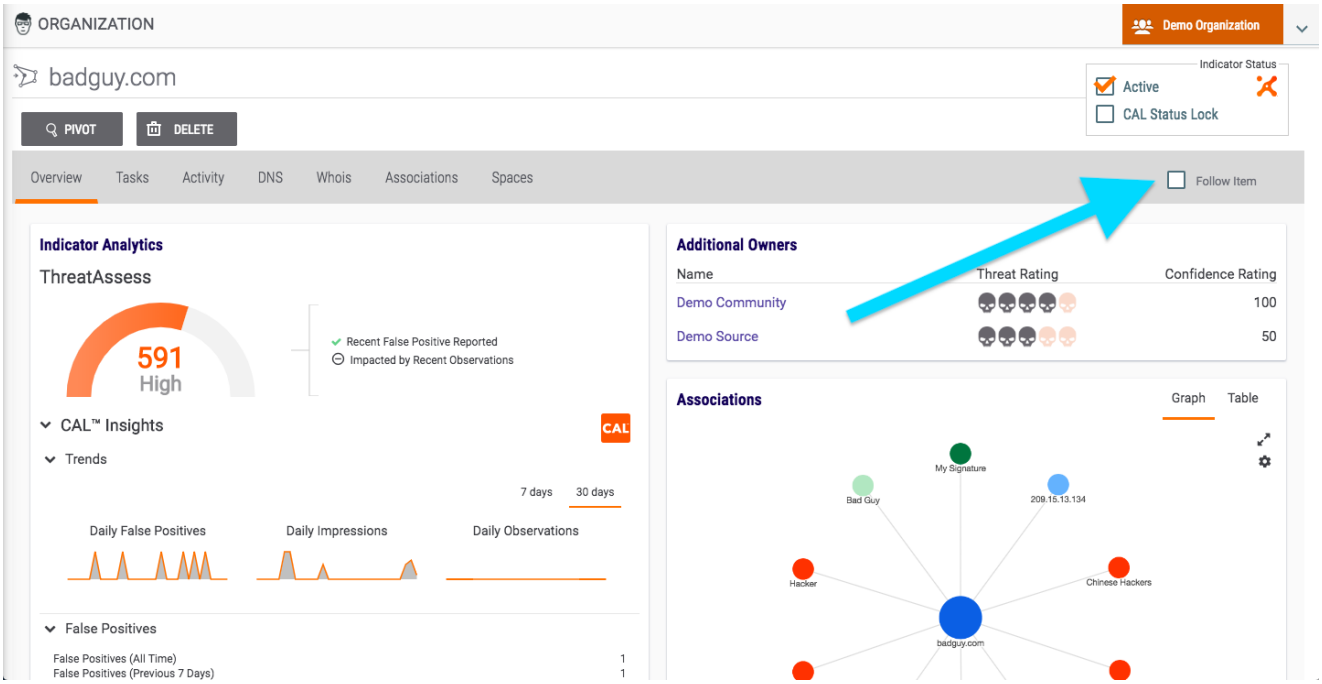
Two other domains — userzone[.]one and userzone[.]eu — are associated with this network of infrastructure. These domains were registered through Njalla on November 13 2019, the same day as those in the previous update. These domains and/or their subdomains have been hosted on a dedicated server at 141.101.196[.]50.

ThreatConnect Research Team Intelligence: Items recently created or updated in the ThreatConnect Common Community by our Research Team.

> 20200604B: Additional Entertainment Industry Spoofed Infrastructure ThreatConnect Research identified additional domains and subdomains that spoof organizations in or related to the entertainment industry. For more information, please see this Incident in the ThreatConnect Common Community.
>
> 20200529B: Suspected Kimsuky Implant ThreatConnect Research identified suspected Kimsuky malware. For more information, please see this Incident in the ThreatConnect Common Community.

Technical Blogs and Reports Incidents with Active and Observed Indicators: Incidents 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).

- In-depth analysis of the new Team9 malware family (Source: https://blog.fox-it.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/)
- Analysis of an attempted attack against Intel 471 (Source: https://blog.intel471.com/2020/03/25/analysis-of-an-attempted-attack-against-intel-471/)
- 2019 tax season phishing scams (Source: https://www.zscaler.com/blogs/research/2019-tax-season-phishing-scams)
- Emotet C2 and RSA Key Update – 06/08/2020 16:10 (Source: https://paste.cryptolaemus.com/emotet/2020/06/08/emotet-c2-rsa-update-06-08-20-1.html)
- Avaddon (Source: https://id-ransomware.blogspot.com/2020/06/avaddon-ransomware.html)
- Threat Roundup for May 29 to June 5 (Source: https://blog.talosintelligence.com/2020/06/threat-roundup-0529-0605.html)
- Emotet C2 and RSA Key Update – 06/04/2020 19:10 (Source: https://paste.cryptolaemus.com/emotet/2020/06/04/emotet-c2-rsa-update-06-04-20-1.html)



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