# ThreatConnect Research Roundup: Possible APT33 Infrastructure

threatconnect.com/blog/threatconnect-research-roundup-possible-apt33-infrastructure/

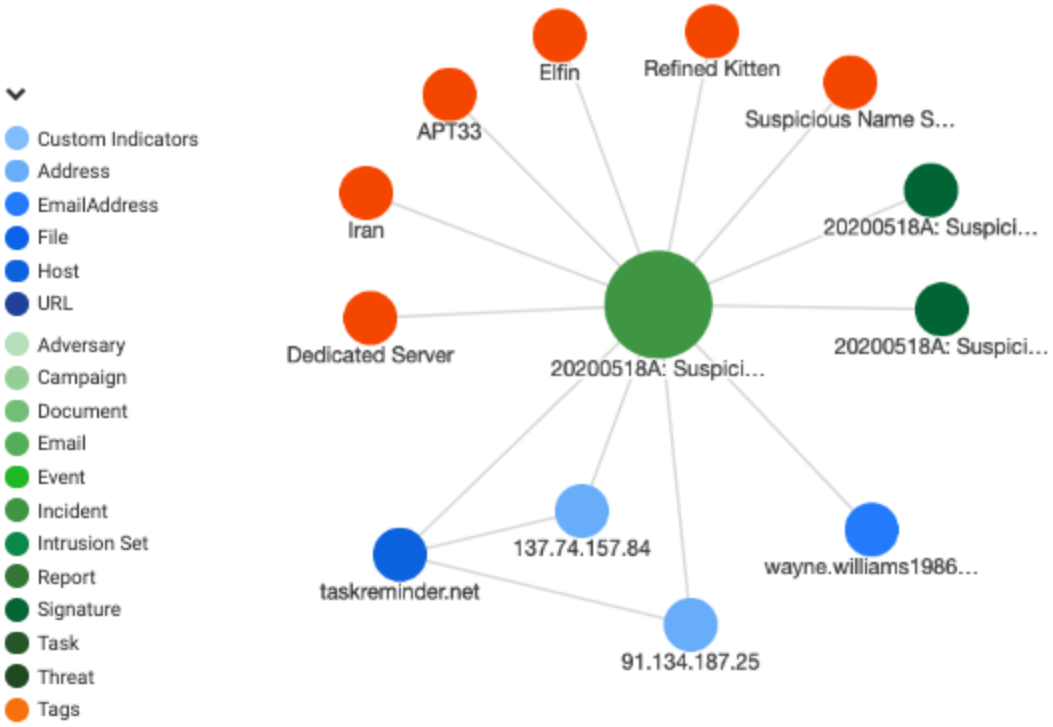
May 21, 2020

### May 21 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.

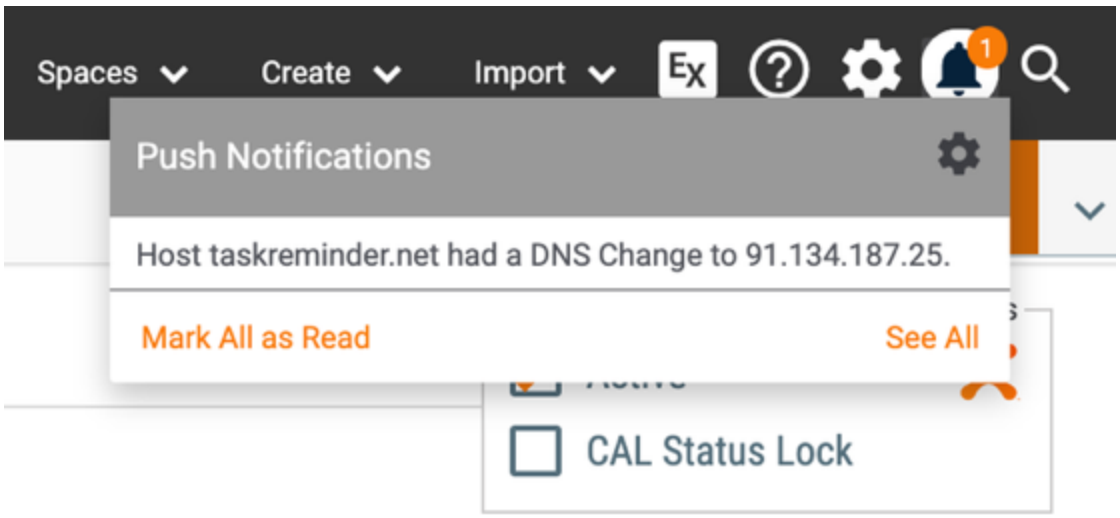
### Roundup Highlight: Possible APT33 Infrastructure



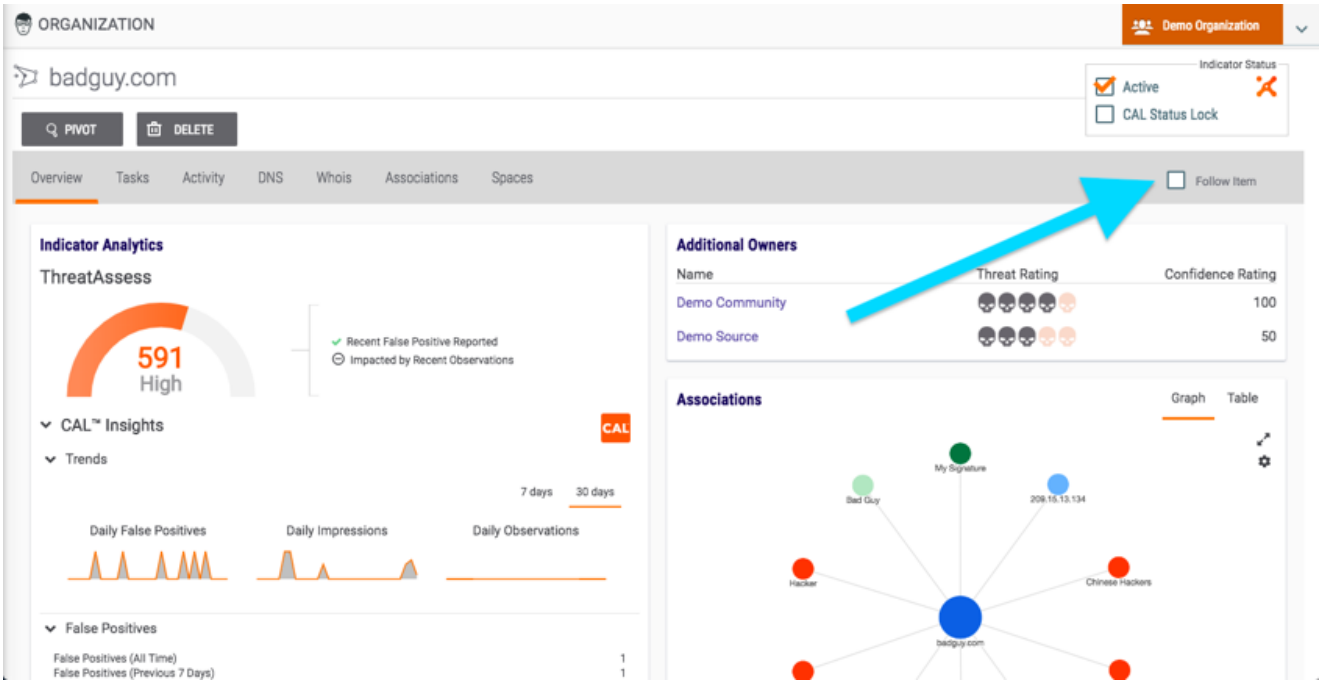

Our highlight in this Roundup is Incident 20200518A: Suspicious Realhosters Name Server Domain taskreminder[.]net, which identifies network infrastructure possibly related to APT33. The domain taskreminder[.]net was registered on May 14 2020 using wayne.williams1986@protonmail[.]com and uses a ns1.realhosters.com name server. As of May 18 2020, this domain is hosted on a probable dedicated server at OVH IP 137.74.157[.]84.

While not definitive in terms of attribution, it's worth noting that some APT33 related infrastructure like times-sync[.]com has previously used the same name server and OVH IP space for hosting. For example, the 137.74.157[.]84 IP was identified in a December 2019 Trend Micro report on APT33 obfuscated botnets. Previously identified infrastructure was documented in 20200106A: Suspicious Realhosters Name Server Domains.

We don't have any information on the extent to which, if any, this domain has been used maliciously. However, given the minimal use of the ns1.realhosters.com name server and APT33's potential reuse of it, any domains using it merit scrutiny as possible APT33 domains.




*Update 5/21/20: The taskreminder[.]net domain is now hosted on a probable dedicated server at OVH IP 91.134.187[.]25. To receive ThreatConnect notifications about updates to Host DNS changes, 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. This week, we highlight new infrastructure registered using previously observed APT33 techniques, suspicious domains spoofing Poste Italiane, and an update to previously reported domains using “msupdate” strings.

- 20200514A: Poste Italiane Spoofed Domains Registered through Reg[.]ru
  ThreatConnect Research identified a series of domains spoofing Poste Italiane that have been registered through Reg.ru since late April 2020 and are hosted on probable dedicated servers. While we have not identified activity leveraging these domains, given the domain name strings, they probably have been used in credential harvesting efforts.
- 20200511A: Suspicious “msupdate” Domains Registered Through Njalla
  ThreatConnect Research identified three “msupdate” themed domains that were registered at essentially the same time through Njalla on May 9 2020. As of May 11 2020, the domains have not been hosted. The identified domains include the following:
  - afr-msupdate.com
  - asia-msupdate.com
  - de-msupdate.com

*Update 5/13/20*: *The aforementioned domains are now hosted on a probable dedicated server at OVH IP 158.69.30.194. Additionally, the domains are also now using their own name servers.*

**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).

- COMpfun authors spoof visa application with HTTP status-based Trojan (Source: https://securelist.com/compfun-http-status-based-trojan/96874)
- Threat Roundup for May 8 to May 15 (Source: https://blog.talosintelligence.com/2020/05/threat-roundup-0508-0515.html)