Research Roundup: Activity on Previously Identified APT33 Domains

threatconnect.com/blog/research-roundup-activity-on-previously-identified-apt33-domains/

September 11, 2020

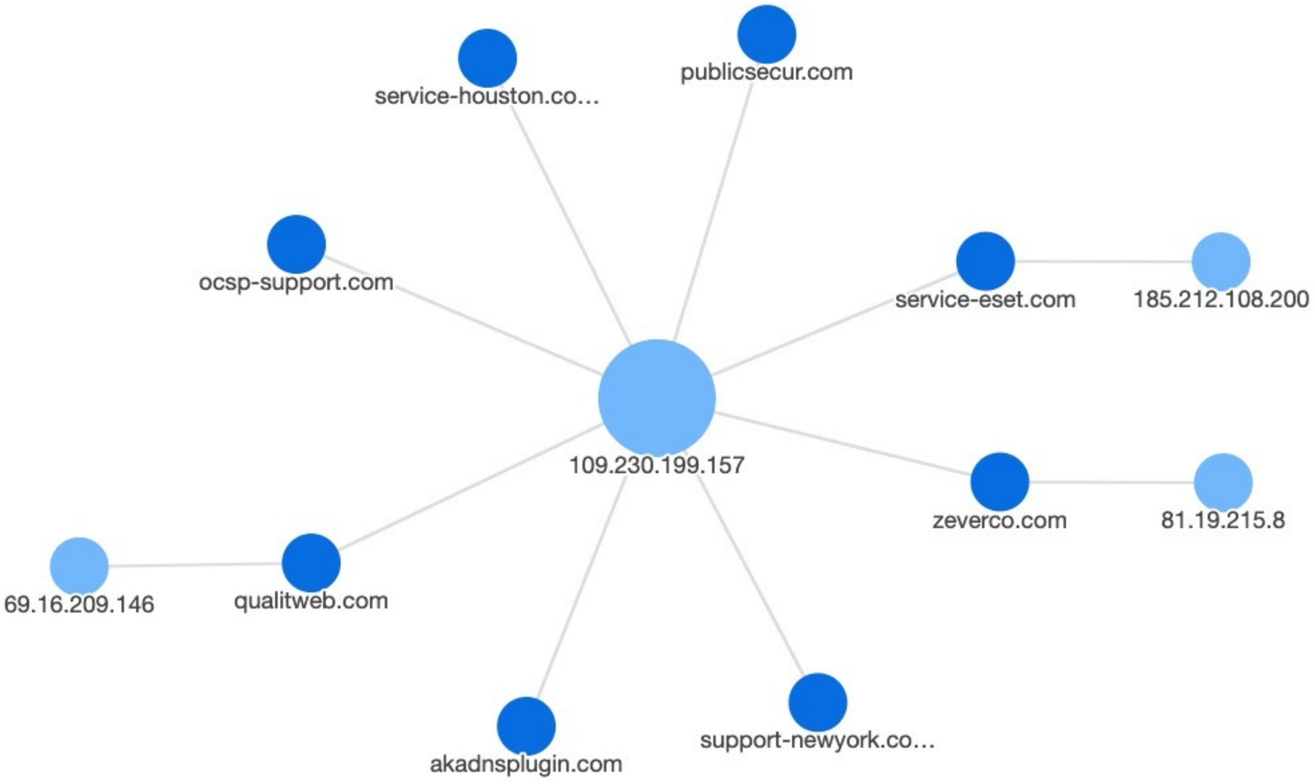
Howdy, and welcome to the ThreatConnect Research Roundup, a collection of recent findings by our Research Team and items from open source publications that have resulted in Observations of related indicators across ThreatConnect's CAL™ (Collective Analytics Layer).

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

In this edition, we cover:

- APT33
- RedDelta PlugX
- Domains Spoofing CDN, News, and File Sharing Sites
- Emotet

Roundup Highlight: Activity on Previously Identified APT33 Domains



20200908A: Previously Identified APT33 Domains Resolving to 109.230.199[.]157

Our highlight in this Roundup in Incident 20200908A: Previously Identified APT33 Domains Resolving to 109.230.199[.]157. A number of APT33 domains previously identified in a TrendMicro report on obfuscated command and control infrastructure — zeverco[.]com (oliverleftley@inbox[.]com), service-eset[.]com (wata.nakatsu@mail[.]com), simsoshop[.]com (tsuda2016@mail[.]com), and qualitweb[.]com (tsuyukisogawa@inbox[.]lv) — began resolving to 109.230.199[.]157 starting in late July 2020. At this time, we do not know if this IP address is a sinkhole or parking IP used for previous malicious infrastructure. Further, we don't know the extent to which the aforementioned domains are still under APT33's control. If 109.230.199[.]157 is a sinkhole or not under APT33's control, then the following additional infrastructure is not necessarily associated with APT33 and may be associated with a different actor.

Several additional domains not previously associated with APT33 or other actors' activity also began resolving to this IP in the last two months. The identified domains (and their registrants when known) include the following:

publicsecur[.]com

akadnsplugin[.]com (joshua.toon1978@mail[.]com)

service-houston[.]com

support-newyork[.]com

ocsp-support[.]com (warren.jones2626@mail[.]com)

Given our uncertainty on whether the previous domains and 109.230.199[.]157 IP address are under APT33's control, we do not know if these domains are also associated with APT33. Regardless, they merit further scrutiny as some of them were registered through suspicious resellers like THCservers that various state and criminal actors have used to procure infrastructure.

Also of note, the ocsp-support[.]com domain may be associated with two other domains — prefmsedge[.]com (warren.jones6363@inbox[.]lv) and tracking-protection[.]net (warrenjones39458@protonmail[.]com) — based on the reuse of the "Warren Jones" strings in the email address. Unlike ocsp-support[.]com, these domains were registered through AminServe.

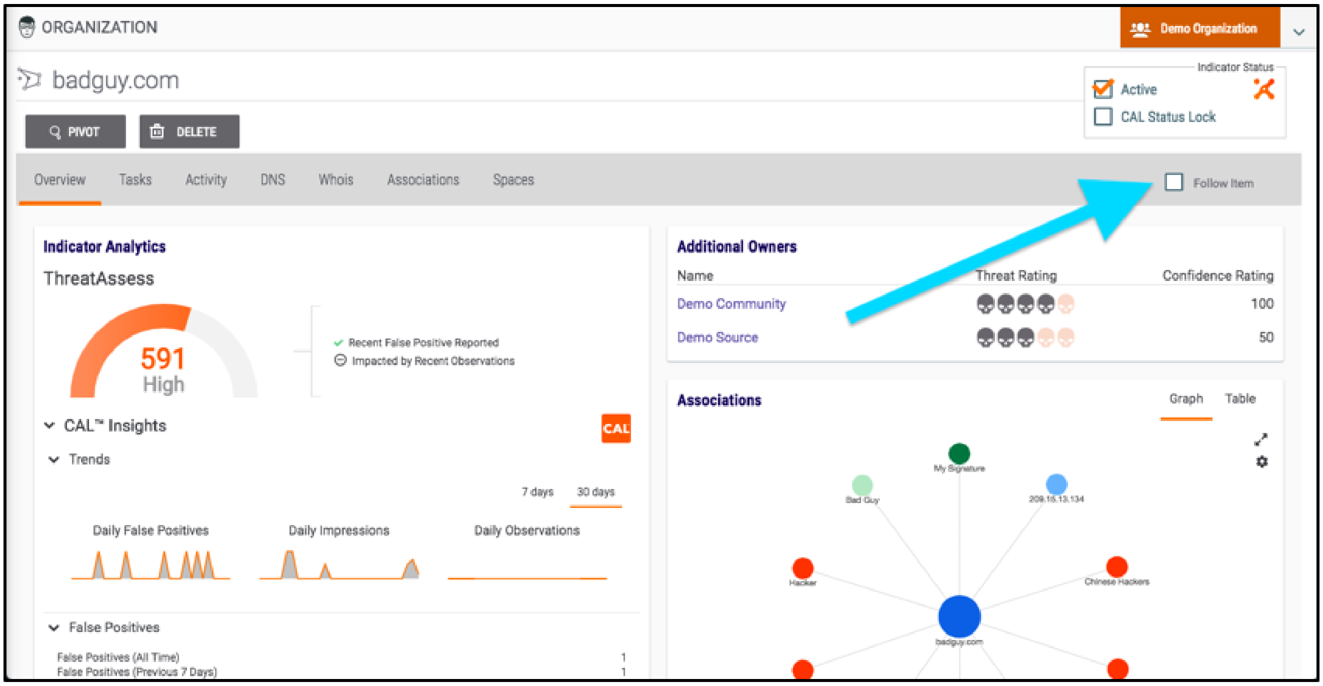
ThreatConnect Research Team Intelligence: Items recently created or updated in the ThreatConnect Common Community by our Research Team.

- 20200908B: File Matching YARA Rule Associated to RedDelta PlugX ThreatConnect Research identified a RedDelta PlugX binary and extracted Command and Control locations from the embedded configuration.

- 20200909A: CDN and News-spoofing Probable Phishing Domains Hosted at 185.228.83[.]110 ThreatConnect Research identified a set of suspicious domains hosted on a probable dedicated server that spoof various content delivery networks (CDNs), news organizations, and file sharing sites. At least one of the domains was identified in phishing activity spoofing an Italian organization. Additional associated domains were identified based on SSL certificate reuse.

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).

- Emotet C2 Deltas from 2020/09/09 as of 8:00EDT or 12:00UTC (Source: https://paste.cryptolaemus.com/emotet/2020/09/09/emotet-C2-Deltas-0800-1200_09-09-20.html)
- Threat Roundup for August 28 to September 4 (Source: https://blog.talosintelligence.com/2020/09/threat-roundup-0828-0904.html)



badguy.com

Indicator Status
☑ Active
□ CAL Status Lock

□ Follow Item

Indicator Analytics

ThreatAssess

591
High

✓ Recent False Positive Reported
⊖ Impacted by Recent Observations

CAL™ Insights

Trends

False Positives

False Positives (All Time)	1
False Positives (Previous 7 Days)	1

Additional Owners

Name	Threat Rating	Confidence Rating
Demo Community	●●●●○	100
Demo Source	●●●○○	50

Associations

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