ThreatConnect Research Roundup: Possible Ryuk Infrastructure

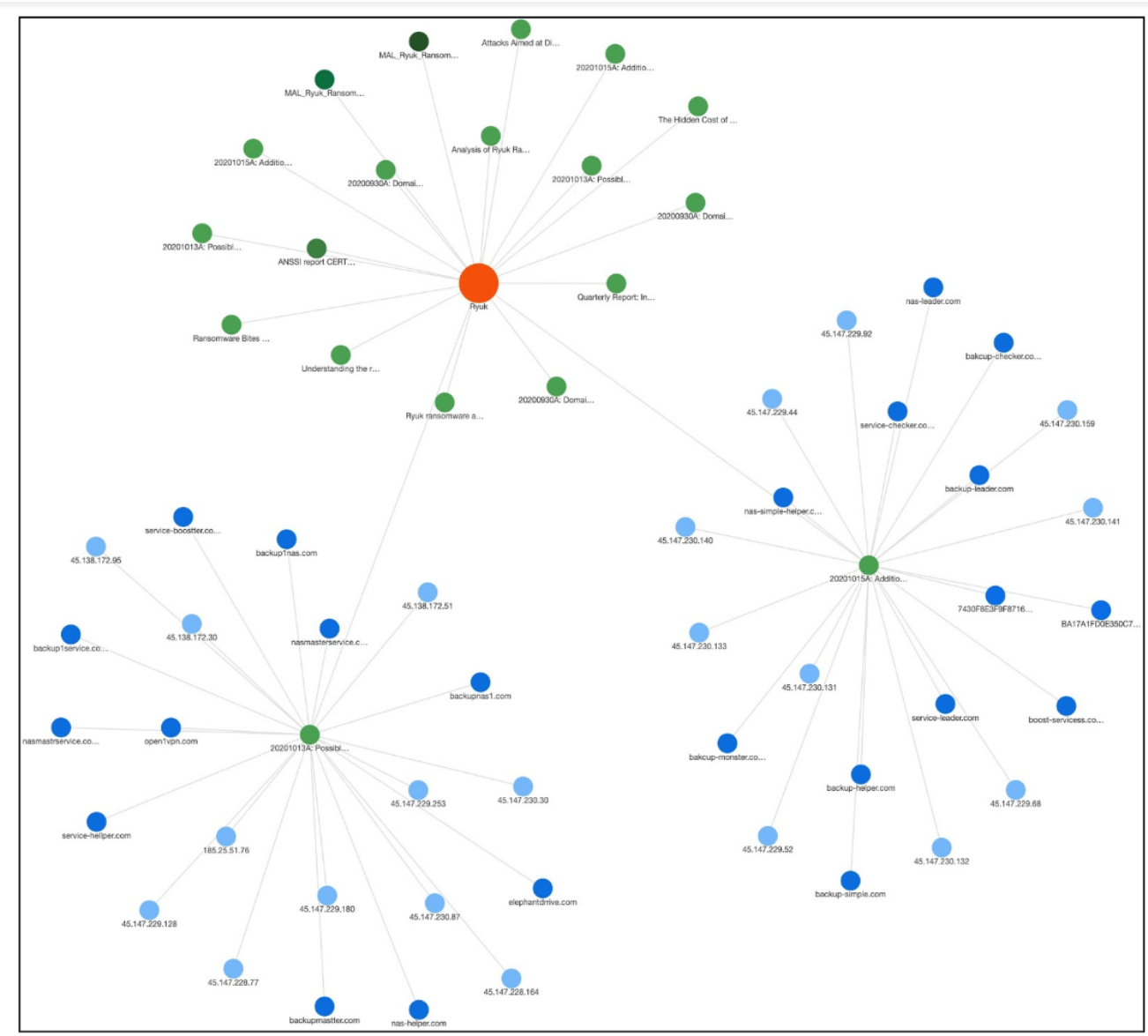
threatconnect.com/blog/threatconnect-research-roundup-possible-ryuk-infrastructure/

October 16, 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.

Roundup Highlight: Possible Ryuk Infrastructure



Screenshot of a “news” site identified in 20201013A: Possible Ryuk Infrastructure, 20201015A: Additional Possible Ryuk Infrastructure

In this Roundup, we highlight Incidents 20201013A: Possible Ryuk Infrastructure and 20201015A: Additional Possible Ryuk Infrastructure.

ThreatConnect Research identified several possible Ryuk domains based on consistencies with infrastructure identified in Incident 20200930A: Domains Registered Through MonoVM Used with Cobalt Strike. Those consistencies include naming similarities, registration through NameCheap, and reuse of the same CIDR blocks for hosting. However, those consistencies are not unique and most of the identified infrastructure is not hosted on ASNs seen in the previous infrastructure, SSL certificates have not been created for most of the domains, and we have no information on Cobalt Strike or Bazar communicating with this infrastructure. Additionally, one of the domains — service-boostter.com — uses a Let’s Encrypt SSL certificate, which differs from the previously identified infrastructure. New SSL certificates or relevant malicious file behavior consistent with the previously identified infrastructure would help increase our confidence in the assessed relationship to Ryuk.

The identified infrastructure includes the following:

service-hellper[.]com (45.138.172[.]95)

open1vpn[.]com (45.147.229[.]253)

nasmastrservice[.]com (45.147.230[.]87)

nasmasterservice[.]com (45.147.229[.]128)

nas-helper[.]com (45.147.228[.]164)

elephantdrrive[.]com (45.147.229[.]180)

backupnas1[.]com (45.147.230[.]30)

backupmastter[.]com (45.147.228[.]77)

backup1service[.]com (45.138.172[.]51)

backup1nas[.]com (45.138.172[.]30)

service-boostter[.]com (185.25.51[.]76)

We identified several additional possible Ryuk domains based on consistencies with Incident 20200930A. At least two of the domains were also identified in behavioral information for Cobalt Strike executables, similar to those in the aforementioned Incident. The domains’ consistencies include naming similarities, registration through NameCheap, and reuse of the same CIDR blocks for hosting. It should be noted that those consistencies are not unique

and most of the identified infrastructure is not hosted on ASNs seen in the previous infrastructure and SSL certificates have not been created for most of the domains. New SSL certificates or relevant malicious file behavior consistent with the previously identified infrastructure would help increase our confidence in the assessed relationship to Ryuk.

The identified infrastructure and files includes the following:

backup-helper[.]com (45.147.229[.]44)

backup-leader[.]com (45.147.229[.]52, Cobalt Strike 4544b478b2029ec38eb4bda111741a10f0684e38f1b29ce092b93df882d11f9e)

backup-simple[.]com (45.147.229[.]68)

bakcup-checker[.]com (45.147.229[.]92)

bakcup-monster[.]com (45.147.230[.]131, Cobalt Strike 2376a8da650c124b3d916765f82929b4109f20bc4f211a39a4d1cd4391780d1f)

boost-servicess[.]com (45.147.230[.]132)

nas-leader[.]com (45.147.230[.]133)

nas-simple-helper[.]com (45.147.230[.]140)

service-checker[.]com (45.147.230[.]141)

service-leader[.]com (45.147.230[.]159)

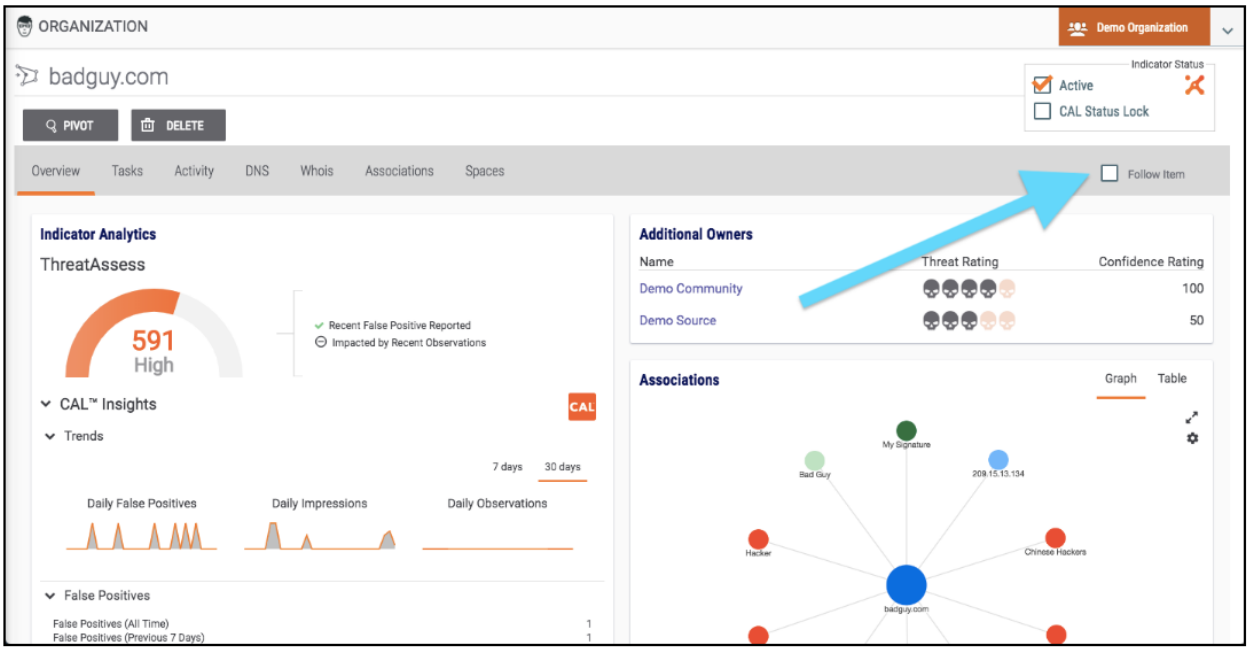
ThreatConnect Research Team Intelligence: Items recently created or updated in the ThreatConnect Common Community by our Research Team.

> 20201011A: File Matching YARA Rule Associated to Mustang Panda PlugX
> ThreatConnect Research identified a Mustang Panda PlugX binary and extracted Command and Control locations from the embedded configuration.

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 2020/10/14 as of 08:15EDT or 12:15UTC (Source: https://paste.cryptolaemus.com/emotet/2020/10/14/emotet-C2-Deltas-1215-0815_10-14-20.html)
- Daily Emotet IoCs and Notes for 10/14/20 (Source: https://paste.cryptolaemus.com/emotet/2020/10/14/emotet-malware-IoCs_10-14-20.html)

- Threat Roundup for October 2 to October 9 (Source: https://blog.talosintelligence.com/2020/10/threat-roundup-1002-1009.html)
- Emotet C2 Deltas from 2020/10/12 as of 17:45EDT or 21:45UTC (Source: https://paste.cryptolaemus.com/emotet/2020/10/12/emotet-C2-Deltas-2145-1745_10-12-20.html)



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