ThreatConnect Research Roundup: Ryuk and Domains Spoofing ESET and Microsoft

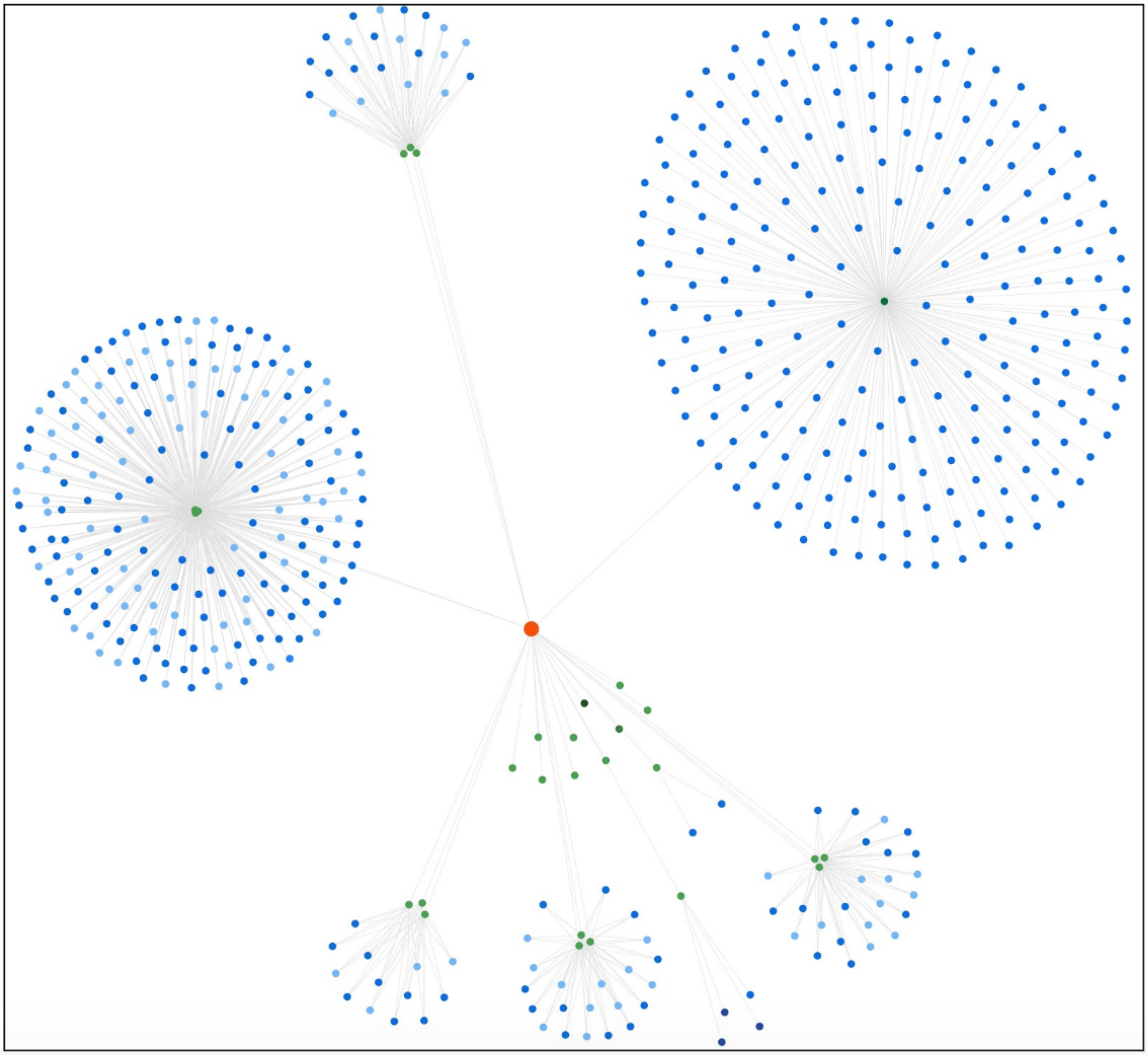
threatconnect.com/blog/threatconnect-research-roundup-ryuk-and-domains-spoofing-eset-and-microsoft/

October 26, 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: Ryuk



Ryuk Tag in ThreatConnect Common Community

In this Roundup, we highlight Incident 20201023A: 20201023A: Ryuk Infrastructure Registered on 10/20/20. ThreatConnect Research identified several probable Ryuk domains based on consistencies with infrastructure identified in Incident 20200930A: Domains Registered Through MonoVM Used with Cobalt Strike and other recent incidents. Those consistencies include naming similarities, registration through NameCheap, and reuse of the same CIDR blocks for hosting. However, those consistencies are not unique and SSL certificates have not been created for most of the domains, nor do we have any information on Cobalt Strike or Bazar communicating with this 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 include the following:

The identified infrastructure includes the following:

viewdrivers[.]com (prev. 188.116.36[.]155, 45.153.240[.]222)

service1updater[.]com (prev. 185.117.75[.]193, 45.153.240[.]178)

godofservice[.]com (prev. 194.36.188[.]154, 45.153.240[.]246)

driverdwl[.]com (prev. 194.36.188[.]45, 45.153.240[.]220)

driver1updater[.]com (45.153.240[.]157)

driver1master[.]com (45.153.240[.]194)

checktodrivers[.]com (45.153.240[.]240)

boost-yourservice[.]com (45.153.240[.]138)

backup1master[.]com (45.153.240[.]136)

backup1helper[.]com (prev. 45.153.240[.]133, 45.153.241[.]1)

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)

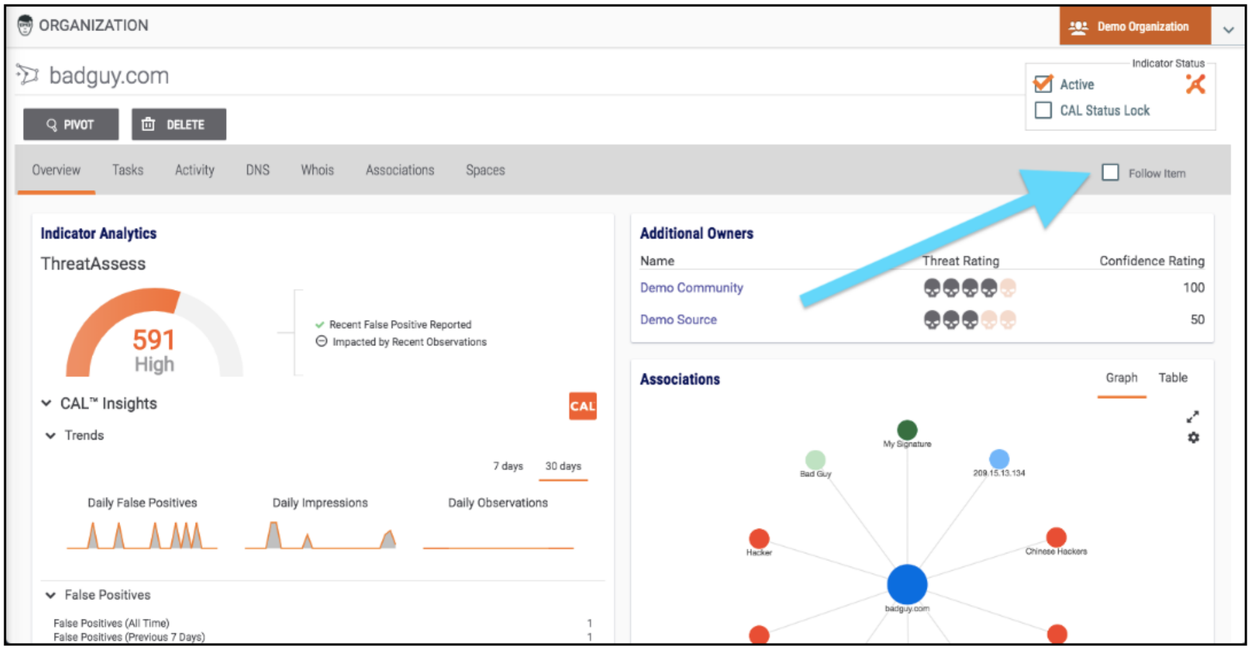
service-leader[.]com (45.147.230[.]159)

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

- 20201021A: Additional Probable Ryuk Infrastructure ThreatConnect Research identified several probable Ryuk domains based on consistencies with infrastructure identified in Incident 20200930A: Domains Registered Through MonoVM Used with Cobalt Strike and other recent incidents.
- 20201019A: Additional Ryuk Infrastructure ThreatConnect Research identified several most likely Ryuk domains registered on October 14 and 15 2020 based on consistencies with infrastructure identified in Incident 20200930A: Domains Registered Through MonoVM Used with Cobalt Strike and other recent Ryuk Incidents.
- 20201019B: Suspicious Microsoft and ESET Spoofing Domains Hosted at 45.147.231[.]188 ThreatConnect Research identified two suspicious domains that spoof Microsoft and ESET respectively. One domain was registered through NameCheap on June 26 2019, while the other was registered through NameCheap on October 15 2020. Both domains began resolving to a probable dedicated server in mid October 2020.

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).

- Daily Emotet IoCs and Notes for 10/22/20 (Source: https://paste.cryptolaemus.com/emotet/2020/10/22/emotet-malware-IoCs_10-22-20.html)
- Emotet C2 Deltas from 2020/10/21 as of 13:00EDT or 17:00UTC (Source: https://paste.cryptolaemus.com/emotet/2020/10/21/emotet-C2-Deltas-1700-1300_10-21-20.html)
- Daily Emotet IoCs and Notes for 10/20/20 (Source: https://paste.cryptolaemus.com/emotet/2020/10/20/emotet-malware-IoCs_10-20-20.html)
- Emotet C2 Deltas from 2020/10/21 as of 06:10EDT or 10:10UTC (Source: https://paste.cryptolaemus.com/emotet/2020/10/21/emotet-C2-Deltas-1010-0610_10-21-20.html)
- Emotet C2 Deltas from 2020/10/20 as of 10:10EDT or 14:10UTC (Source: https://paste.cryptolaemus.com/emotet/2020/10/20/emotet-C2-Deltas-1410-1010_10-20-20.html)
- Daily Emotet IoCs and Notes for 10/19/20 (Source: https://paste.cryptolaemus.com/emotet/2020/10/19/emotet-malware-IoCs_10-19-20.html)
- Two New IoT Vulnerabilities Identified with Mirai Payloads (Source: https://unit42.paloaltonetworks.com/iot-vulnerabilities-mirai-payloads/)
- Threat Roundup for October 9 to October 16 (Source: https://blog.talosintelligence.com/2020/10/threat-roundup-1009-1016.html)
- Emotet C2 Deltas from 2020/10/15 as of 11:50EDT or 15:50UTC (Source: https://paste.cryptolaemus.com/emotet/2020/10/15/emotet-C2-Deltas-1550-1150_10-15-20.html)
- Emotet C2 Deltas from 2020/10/16 as of 11:05EDT or 15:05UTC (Source: https://paste.cryptolaemus.com/emotet/2020/10/16/emotet-C2-Deltas-1505-1105_10-16-20.html)
- “We’re Grateful For The Trust!” (Source: https://cofense.com/were-grateful-for-the-trust-devious-link-inside-pdf-attachment-leads-to-compromised-credentials/)
- Daily Emotet IoCs and Notes for 10/15/20 (Source: https://paste.cryptolaemus.com/emotet/2020/10/15/emotet-malware-IoCs_10-15-20.html)



Indicator Status

☑ Active

☐ CAL Status Lock

☐ Follow Item

✓ Recent False Positive Reported

⊖ Impacted by Recent Observations

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

False Positives (All Time) 1

False Positives (Previous 7 Days) 1

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