Cyber Threat Intelligence Network, Inc.
P.O. Box 5042 | Carefree, AZ 85377 | USA
001 (928) 399-0509

OASIS Automation Workshop

Ransomware Use Case: Ryuk

Conti

R. Jane Ginn, MSIA
May 26, 2022
TLP=White

USE CASE TYPE: Big Picture

Introduction

Following is a curated Use Case built to meet the needs of the June 2, 2022, OASIS Automation Workshop for demonstrating interoperability of multiple security standards including:

- OpenC2
- Collaborative Automated Course of Action Operations (CACAO)
- Threat Actor Context (TAC)
- Cyber Threat Intelligence (CTI) [for STIX2.1 & TAXII2.1]
- Common Security Advisory Framework (CSAF)
- Open Security Alliance

This Use Case is a compilation of data from multiple sources about an ongoing threat posed by a sophisticated advanced persistent threat (APT). I have used open-source data for documenting TTPs used by the threat actor(s) as a secondary source and then conducted threat hunts on their ongoing reported malicious infrastructure as a primary source.

For the purposes of this Automation Workshop, I have chosen specific offensive actions taken by the threat actor for illustrative purposes to meet the needs of the participants in the Automation Workshop. I have supplemented historical findings from multiple threat hunt teams with my own findings of ongoing campaigns by the profiled threat actor. For consistency I use the threat actor naming convention used by the US-CERT: Conti.

The following are the key elements of this Use Case:

Elements	Description
Situation	**Conti** — one of the most ruthless and successful Russian ransomware groups — publicly declared during the height of the COVID-19 pandemic that it would refrain from targeting healthcare providers. But new information confirms this pledge was always a lie, and that Conti has launched more than 200 attacks against

	hospitals and other healthcare facilities since first surfacing in 2018 under its earlier name, "**Ryuk**."[i] They used multiple malicious infrastructures including TrickBot, which is likely also linked to BazarLoader malware. From their first appearance until May, 2022 they have continued to develop new functionality and tools, increasing the ease, speed, and profitability of victimization. These threat actors increasingly use loaders as part of their malicious cyber campaigns. Cybercriminals disseminate TrickBot and BazarLoader, and later, Zloader (see below) via phishing campaigns that contain either links to malicious websites that host the malware or attachments with the malware. Loaders start the infection chain by distributing the payload; they deploy and execute the backdoor from the command and control (C2) server and install it on the victim's machine.
Industry	Healthcare
Organization	Example: Alabama-based Springhill Medical Center[ii]
Infrastructure Systems	Facility benign Infrastructure, unknown; Offensive Infrastructure identified in 2022 = Zloader.[iii] See Microsoft and Health-ISAC Complaint[iv] - See also Declaration from Weiss in support of injunctive relief for a botnet takedown[v] - Internet Infrastructure used: DNS (see below)
Attributes	In early 2019, the FBI began to observe new TrickBot modules named Anchor, which cyber actors typically used in attacks targeting high-profile victims—such as large corporations. These attacks often involved data exfiltration from networks and point-of-sale devices. As part of the new Anchor toolset, TrickBot developers created anchor_dns, a tool for sending and receiving data from victim machines using Domain Name System (DNS) tunneling. The anchor_dns is a backdoor that allows victim machines to communicate with C2 servers over DNS to evade typical network defense products and make their malicious communications blend in with legitimate DNS traffic. anchor_dns uses a single-byte XOR cipher to encrypt its communications, which have been observed using key 0xB9. Once decrypted, the string anchor_dns can be found in the DNS request traffic.
Assets	Unknown
Playbooks	CACAO: Notification and Detection Playbooks With Yara Rule[vi]
Security Policies	Unknown

USE CASE TYPE: Mid-Level Scenario & Interoperability Demo

An October 28th, 2020 alert from the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) entitled ***Ransomware Activity Targeting the Healthcare and Public Health Sector Alert (AA20-302A)*** has raised the level of situational awareness regarding a new campaign from the Conti threat actor group and their use of Ryuk ransomware to target health sector entities.[vii] Active since at least 2018, as documented by Checkpoint[viii], it has sometimes piggy-backed on top of previous infections of Emotet or Trickbot.[ix]

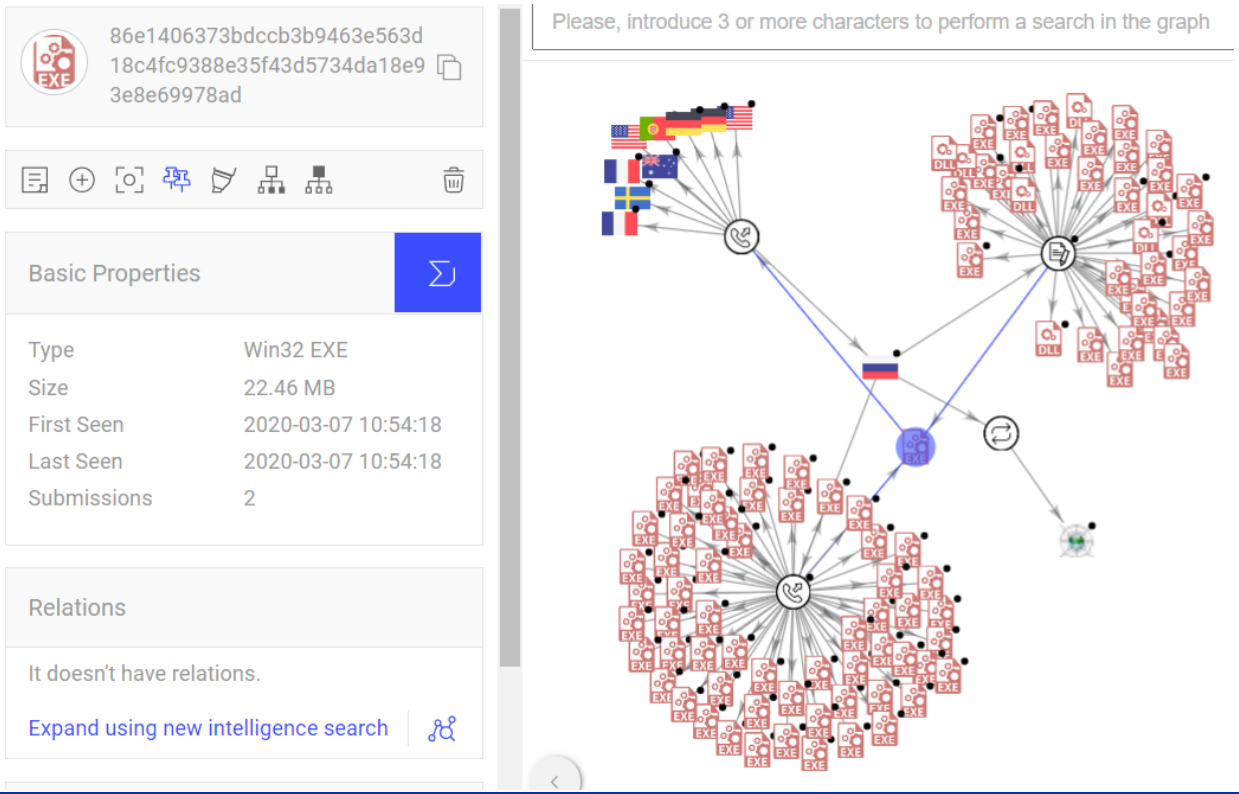
As noted by CISA/FBI/HHS, the most recent campaign appears to be building off of an anchor_dns cyber observable (CO). The key cyber observables called out in their Alert are given below as fanged COs:

- kostunivo[.]com
- chishir[.]com
- mangoclone[.]com
- onixcellent[.]com

- 23[.]95[.]97[.]59
- 51[.]254[.]25[.]115
- 193[.]183[.]98[.]66
- 91[.]217[.]137[.]37
- 87[.]98[.]175[.]85

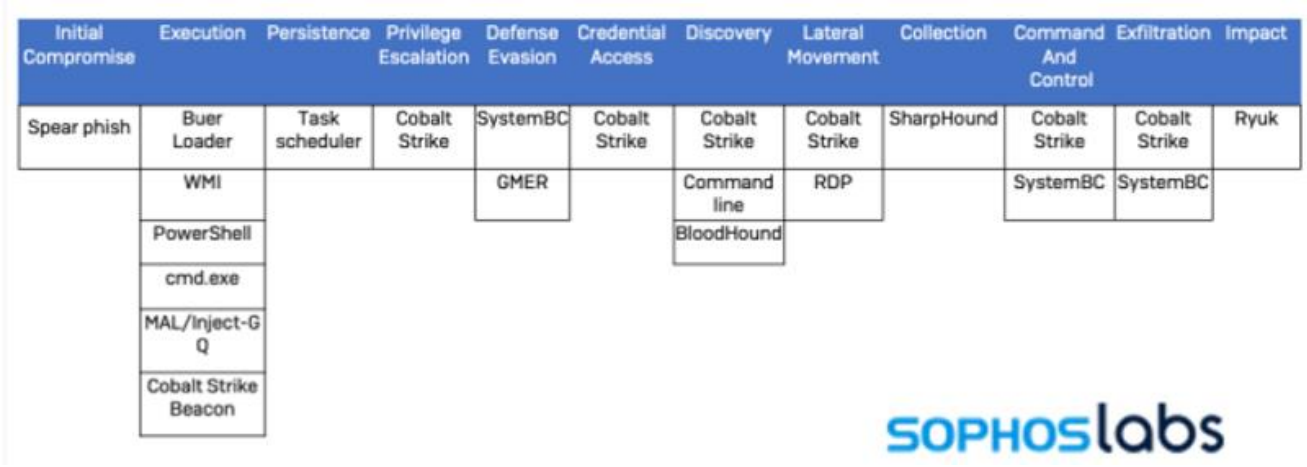
I uploaded each of these COs into VirusTotal and found that the most recent samples they had were from late September to mid-October. The most recent domain was onixcellent[.]com which communicated with 208[.]91.197.91 (British Virgin Islands), 185[.]25.50.213 (Lithuania) and 209[.]99.40.222 (US). I have not drilled down further into the pDNS, WHOIS, or ASN activity associated with these IPv4 addresses yet. However, I suspect there will be fruitful information if I follow that route.

With respect to the IPv4 addresses given on the CISA/FBI/HHS Alert, the crytominer module appears to be dropped from the 91[.]217.137.37 CO, a Russian IPv4 that resolves to: frod[.]subnets.ru. The following screenshot shows the VirusTotal graph of the Referrer Files (top right) and Communicating files (bottom left) along with the IPs (flags) depicted in the graph data model. Note that I have highlighted an .exe file that links the two clusters. The SHA256 for this is: 86e1406373bdccb3b9463e563d18c4fc9388e35f43d5734da18e93e8e69978ad. I have not yet drilled down into this malware component; however, its central connectivity to all three clusters indicates that this is an important executable in the most current Ryuk campaign.

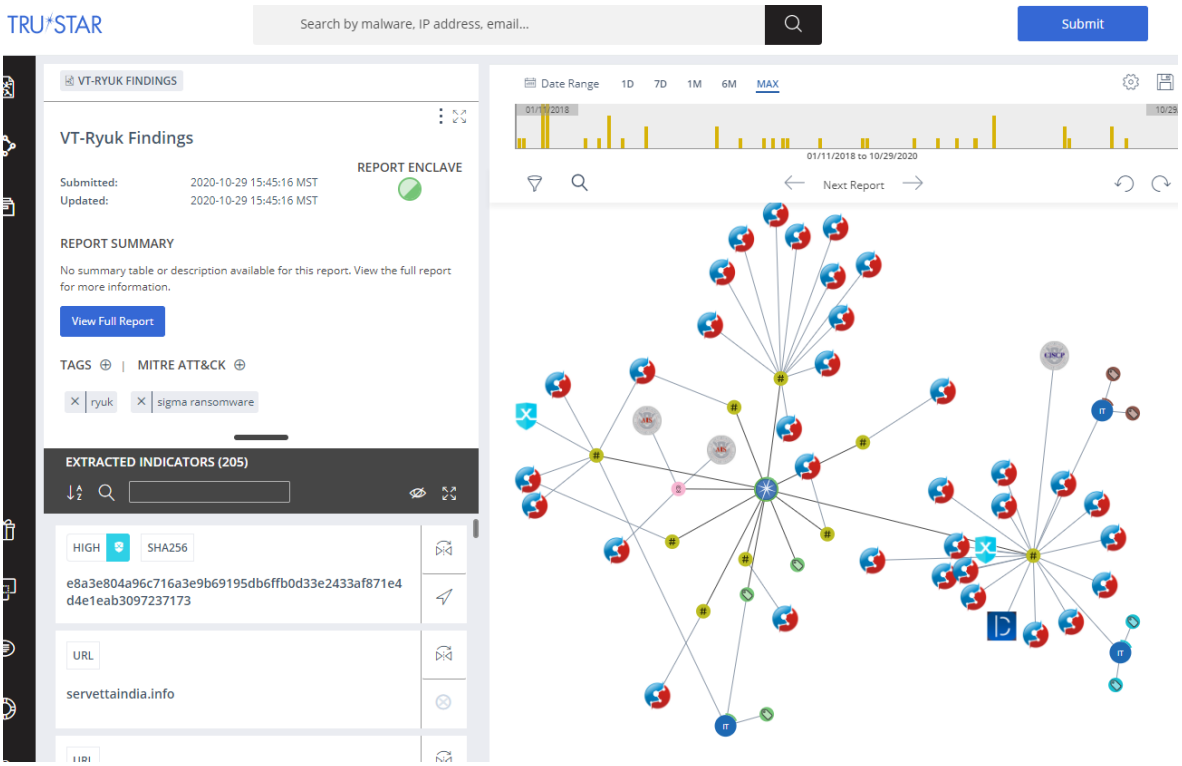


I also pursued another track in my brief hunt on these COs; and I believe this is one that will also give us some actionable COs on the most recent campaign. Fourteen days prior to the CISA/FBI/HHS Alert Sophos provided a detailed walk-through of a new Ryuk campaign they had analyzed.[x] They show how the threat actors used a Buer loader host in the Netherlands (104[.]248.83.13) and a Cobalt Strike C&C server in the US that resolved to 'mn[.]fastbloodhunter.com.

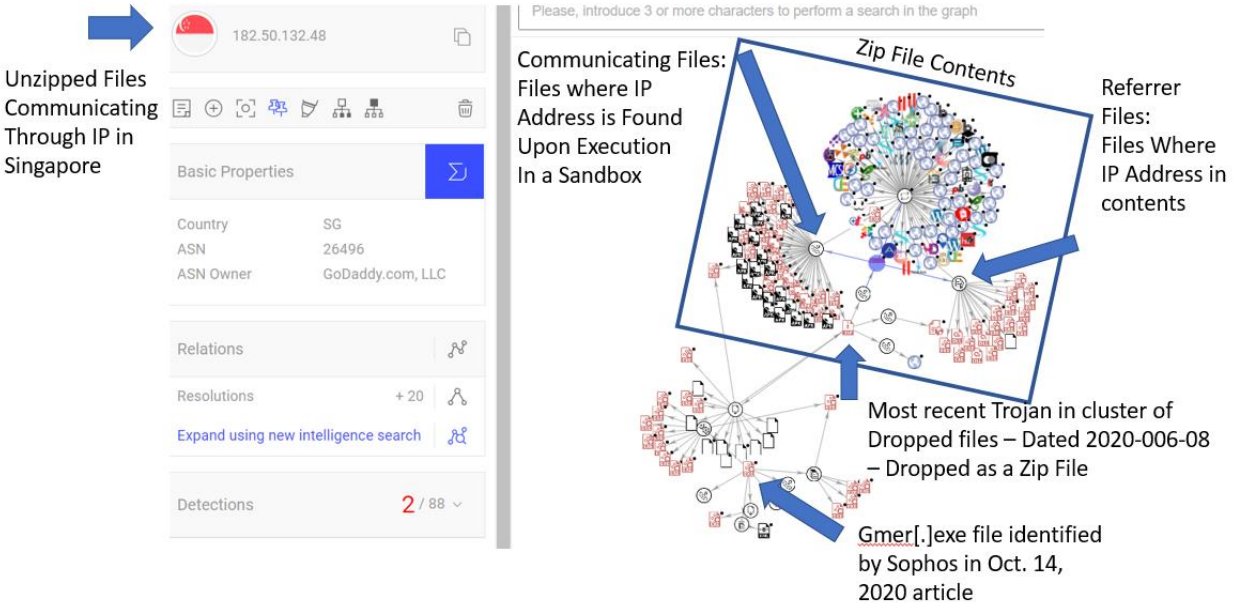
After a walk-through of the steps in the attack the author describes a rootkit detector tool called gmer[.]com. The various TTPs are summarized by ATT&CK Tactic on the illustration below. This gmer[.]com CO is included in the list of COs they released at their GitHub site.[xi]



I uploaded select COs from that GitHub list to the TRUSTAR TIP and found some correlations with earlier campaigns by the same threat actor group. The following graph also shows Hybrid Analysis, IBM X-Force Exchange, AIS and CISCP enrichments of the data going back to 2018.



GMER is frequently used by ransomware actors to find and shut down hidden processes, and to shut down antivirus software protecting the server. This proved to be a useful route of investigation for surfacing more of the malicious infrastructure currently in use by the FIN6 group. The following figure is a screenshot of the VirusTotal graph that I developed along with annotations describing the clusters in the image.



As you can see, I've pointed out the gmer[.]com executable node at the bottom of the image. I've also identified the node that represents a Zip file Trojan that, when expanded, shows clusters of Referrer files and Communicating files. Finally, note that this most recent gmer[.]com Rootkit ZIP file communicates through an IPv4 in Singapore.

This memo provides a quick summary of what I was able to surface in my hunts over the past couple of days. Importantly, I wanted to provide the various COs embedded above.

Cyber Observables from Oct. 29, 2020 Investigation of Ryuk Activity

gmer[.]exe
e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173,

Zip File
***7ddce2ee73dced0ec94d3eddd1af75d9aee245bdb11a50766408861f353a0a40,

cf0eace21fbf2e8f2fbe46e269ef32dcf3ae8a23aa70e7ad13add568fbf3c450,
24506048b4ca6c50ea35509e0da1e86876d34c4c30ec24856b7124b1712a4e54,
2cf8b69a47be583b8eb949797b15f5fef50342b735e6480910f79c4711c5120e,
96cf0fb2f0f70140c6bea138c06ebe312b9697776755a430f2c479f31570fccb,
bae1d5580fc2f015a1b4c1102e4b7e10bcd4f5cc83dc81385086ca7676abd220,
cabb42fc30e734b4c5a6de98c8f0d3c4787914d5a578534ba1e851a2fb453bfb,
ec2a64422dfba448cad78e468e97d99866c3d11ad8dd673dbbbfaddc0d36abb3,
18bb9729de5562f46c2a334f3a655b65fc9f7f3e9343d01d08e8c87a6c1a6148,
4eb8e439dbea03f9da2c344d4002c5c4df9700c68a53878f18c6f1cfa287e08c,
5af880227953474794226d796a594ba70f15c78b80103a7c670b1fa17e4f6b88,
633b3e17f0c7688ac27cbd3a013ab0fc452a916752fa13e4ce67bf9c6ca6c9d0,

7718c946c43c3c2a75944c97acfc78bc23bb8ec605aa1e8549967d2095c46b68,
7c6875e0adf6ea50f296cf1e4bec01d0a9165299f824ca887757f9bf6bb7e31d,
8ba1c35da497dc1ac7f08e5ab4b5aeb2a0678acedf7f974b270c43afd63df978,
b019ad35625aee7490b146e999ab996f3af6820921d17126fbedeac902b5c767,
f03a6337cb8767c0a2ff7256b00274c085ff5b1d47aa7b7c48d69aba685f1b0f,
18c909a2b8c5e16821d6ef908f56881aa0ecceeaccb5fa1e54995935fcfd12f7,
2f380f4a3d05a8d90c2106f50da75064e9ce57a598599dc5404f8f69a0223aa9,
3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef,
4d800d7512c252589878405426c4c954e7f38a483b2feb741618c5d0df4b0bcb,
6194c34da4e6c565f58e5e62e9a7152347188da471dd8d200a1977e8d4cb7351,
7f5f447fe870449a8245e7abc19b9f4071095e02813d5f42c622add56da15b8b,
82f453db400e72fae9c701510c18e986bded3b76370a25ed1327929573251f3c,
ac2f019c8d9cb6feaf82eba4b2290c8c15f9e0477b731291535ea5ea615ab1c2,
b1097d78e9db7cf372ad2233639fdd9bf1d63e33ed3d10ffded847f703732804,
b14c68ca4ff8ef45dec4d692a04754e7f31ae92af9e26f249cdbf0e54d5d625b,
c13fef0a56ad907c325b240bb0cf4876b261fad974089627b7bff63072bf6bd8,
d2f6a2f6b7396fc0d4221cc11e4e3de76631a8c92f20d93f56198d4fe4ee8b46,
d65165279105ca6773180500688df4bdc69a2c7b771752f0a46ef120b7fd8ec3,
http://omerez.com/repository/eternalblues-version.txt,
omerez.com,
182.50.132.48,
3c7b8b75f3ba23c81e737b0871ae64e6621332a33ac5322d9a85048d20bd929a,
00958d0e795c0304d4ecf612aaae4ae0bea32ccb88f7096d988582a5f3634a1a,
3a574df0f77fc258a03b82069338d690ca47f2daeafad0c7598bcbd8268ed8b2,
04c8f06864c6adbf47e6379c0d9ca179f2fc484ba5395868facab229cd501ac5,
271b3b12cb749ed4532dc1b137b76a9bce0a8c1e86149247a3bbe104125adcd7,
54800ac26c2eb67e8a01dee730fe68b8119c7a1568d5317b75abe300c14cb2d9,
c81d17da2521b02908ed200159bec514c974eb2bd2249d792539d559a3a21034,
7740bb566e2dfaf0d4753a00f123b4be256c4d8a34ea7c6e789c41cbc4740acc,
d6e161932c6ec4e886f007513243ef4b403a8035fab7c9dcdbae539b06a3ee7a,
247bb136a1e862dd7c6ad9d3114da2728e99c7872fbd766f9479db681d73b81d,
20b0cba57d774006ff7d7b48abc5443420653f43818e31f8971c1251fe1805dd,
207ff671ca444a60ae10e3f2b9dde3d2a8842daccf3595bd588c0ceea207b8de,
bcb36516ee90a689736dfcc3ca5d4847649694758aa2e75f288df1233708a603,
a156688c7d9e20f5c65652be925eec23e1c14aeb35934c561173a5c25a82dee5,
0b07aa5e6488d295ada8f11b93288174a39d042cd0fe9a5e0b74877a72301890,
595a438a041f4aeba756a6316a1fc242d05e016950782e9e93e17755eed95ea6,
17411f3315c49e74769db01abbfee3983ad9e2430b728acf8b7e358c4a98e9f3,
a4bd47f4a4cf6f0b157afc41295f0c1655e9d6f47a33f5a69b7eaf5695d38075,
db0e272f6837cb1d9345bcaa6905c68bb6073fd51e58b6fe9050db8a1943558d,
be911d193412f0db6a48fe863abd228d9e311feab863a4079ffa07fc917d7481,
f5e01cc64ee5a5d8872d780c8c30ae64db97cb757e1fcef2b14c5fcb9b70c0f6,
0cc8ad791dc4061ce1f492d651ed2a9baeed02413c5940240bf47bb023f509ef,
524042c542c5090b6e7a02ee57ce8ff3a5952a11e7d6f8e5425374e0897e33dc,
997dd694132e87a162aa008b46898bc9c09378ca0d9188127578ab949fee1273,
5e8c54f9982f8075a8d17c3a4ff015a0a6c48306e863d912e9a9b7bea564f03e,
4c382c1f4e28c17ac262bc95ddd9aa69b6018e791c8aa1fb9d90e1887c37d66b,
14614a064a7c17d82231fab33c189657f266c58993c6ed74d93be43862863784,
599dbfb01517a3fbceb9ef9a99c37ca20b22acc8dea935e0680b0845bc2edaac,
1e6fc5078edd00a8ecedcbd2e2054a769610bfacce81b22f1285a7e14dbeacb0,
2befe9731da1cfe3890408ad66929a890d51f279e6e85590006de9e940277ba0,

21cc36e60e661613f0c05e73b9496bf2d456931686b0693112842d91d7e64e78,
1d04a5a31e98ae0605e1267530ae6e3e59e975df96b577505a776ceb2ed6a3e8,
7a08f7010402e2813830c77be1e992f6193f5c1ea97b76fbe706c2090ba66cb3,
b34370d60446f6b175d1f0ca16aed47e54a3c1963b39aeccbce67ac1a9d04813,
ad996f4093080fde022c9b24450df0c8a287e3d8b527d4cef3f76f5b33f6a936,
d1f4936c3f8f97abe59ecbdeb089e53292d19bf39d10dabf676a18398e0893de,
8b2ef5d528770232165163e17c2c538a929f4d6bb44b1051fb06f8f80d11c3be,
f553368310af84d39dd55ad5ffd6b64f0144518c4c34c70d5234974c258a4ebf,
2702799cfa623998eaa0d960e6ce0460cd7ddba3305cec96710abc5093f04ef0,
590f11420933977807668cce81b8b3015d8c55a9f27831eda13a5578f54a245b,
491d0cae1f774d112d4920821b6f766be9459aa4479d5cb2310aff554ce8020b,
28c351d2f1f3798d96ab0d1b232c1812b9ac1bb5c6ff2e093b9afe56ad242f02,
40cec48b1eded584d670da4b211311ce67a6b5d1f2bfe3574cc84c5362b27c55,
d66af770a078600c08395fd1c9ba7f97fa5a534687bf8be6b6f1acebbbaaff7f,
f0f34605752e244a4abcc699ef2c4a3cf49d935c3d1718c32244ff8cec1752b6,
5242276f4bb35990d8f96c41030165750a14d58d3ff132938380998727cb29f3,
6c285d79cc6f6f31163dbc335accf5b1633059ab9a888c0a40bc51cac2c9045e,
09c85ada47bbc10bbcc02a137e309ea1866aa34f5a130062865b623985f48231,
a378fc6620d12b038191a2693bff5307ec969cda6facb0a82de201a7b9b57c4e,
4fc58091dd64e468c6f573838234b3657455a95d3c24fcda71067abf326458f4,
9afc6b16f1b5ba2d0e6092894c77eb71248e4b69e60eaeeebda6e152dbe79f90,
f8958af81f979cc0c2fbd6c42e79d8131c912306a9fc3bb3d94a2034e8c5d1dd,
f2c199b1e8bba1d65e6aeb70ad5817b7e343ce70a91f85b56190a720ed078504,
8438ee8e96375e3ebe4aa383f11d225330ca344fda8e4a88341a715e37d3cdd2,
1276332088baa25ff541e93b2a66a6f92fb6b80ea9cf55d7b420114e47ca3412,
f487d62d2c4335c3be813ade443ef9148cccfdfab77b18cce2fffac18b7607ef,
91f443549ee2f309305332079b6c5a5ac9395dee6c6dd12f400a4463e512c6d5,
01a29b1dd1d9f00bd91ffaa048cedb4a58e4a4d06f7a41603052236a157fe4b0,
eb73d143b74d45c6a90e15db4785fc6ca3456b91ba21426b2c545c2378dbb67d,
73108e2916d3d942a7dcb3aedde46553d14cf583fddb0455a50f79388c9cb8d7,
6e5357eb64b3e8f6e07dbc436e36d15b972d8f79bec731344d64cf63091b9762,
9554555f9df327781f0a746d1aa85a8492bb985db263f7682fd04657d18b4685,
210882dcbcda9a0afd0bd5c44bc782d14fd81cec41f876162987ab7fe2ddf043,
24dd1c7791398ffef31f61911f2cec6099e1baf09ab16d2f49b5401e919d93be,
0ea9f3fc1b7ca4be10894dd10d7be8ccce25357f6d482fe2e7c700739ca97e54,
b0cb49c2b3d1eccec438f8114ec04b42af221b0b6821d0bcbeeb2fc78ca71b75,
3dd3ed2116d68b295a6237b1c3e2ed12fec532700905d40759e42a54f2f6982f,
7a96f1b89060382a9e3a8bf4bc6ff4bc9e4c3530a5fad77990507bc9f130627c,
2c6455272ec7a802daecb26aa3b032357bda67edc023da27cb86cfe2fa8e1caf,
fba98b6d7175b309ce05dd3b14fddbc29f85f6b9a343c5a1641b907b78b62619,
e87c04b079bbe5bfd70f45d653eeef6bde4199f3487287bf0a008eea0bcd961a,

[i] https://attack.mitre.org/software/S0446/
[ii] https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges
[iii] https://krebsonsecurity.com/2022/04/contis-ransomware-toll-on-the-healthcare-industry/
[iv] https://noticeofpleadings.com/Zloader/
[v] https://noticeofpleadings.com/zloader/files/Application%20for%20TRO/TRO%2008%20-%20Weiss%20Decl%20with%20Ex%201%20ISO%20TRO%20and%20PI.pdf
[vi] https://www.cisa.gov/uscert/ncas/alerts/aa20-302a
[vii] https://us-cert.cisa.gov/ncas/alerts/aa20-302a
[viii] https://research.checkpoint.com/2018/ryuk-ransomware-targeted-campaign-break/
[ix] https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
[x] https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/
[xi] https://github.com/sophoslabs/IoCs/blob/master/Ransomware-Ryuk.csv