Ryuk and Splunk Detections

splunk.com/en_us/blog/security/ryuk-and-splunk-detections.html

October 30, 2020

By Ryan Kovar October 30, 2020

Several weeks ago, my good friend Katie Nickels (Director of Intelligence at Red Canary extraordinaire) and I were chatting about Ransomware. She was super interested and passionate about some new uses of a ransomware variant named “Ryuk” (first detected in 2018 and named after a manga/anime character) [1]. I was, to be honest, much less interested. It turns out, as usual, Katie was right; this was a big deal (although as you will see, I’m right too… still dull stuff!).

On October 29th CISA (Cybersecurity and Infrastructure Agency) posted Alert AA-20-302 (since updated) discussing Ryuk as an “imminent cybercrime threat to U.S. hospitals and healthcare providers.” If you’ve been paying attention to the ransomware world for the last couple of months, there was a declared “ceasefire” as ransomware operators proclaimed that they would not target hospitals during COVID. This announcement was, perhaps not surprisingly, not accurate. Over the last couple of months, Ryuk has been ravaging public institutions like hospitals and city governments, causing delays in surgeries and possibly causing actual deaths [2] [3]. Suppose you are interested in the attribution of the Ryuk operators or a deep dive into the malware? In that case, I recommend you read some of the

great blogs/postings from Mandiant or Red Canary on the subject. Otherwise, buckle up for discussion on some resources to help detect and even possibly remediate Ryuk using Splunk!

Quick Breakdown of the Ryuk Kill Chain

Although Ryuk is getting the headlines, what I find most interesting about Ryuk is that it is actually the final step of a multi-staged attack. Historically Ryuk was delivered with a spearphishing attack using a weaponized Microsoft Word document to drop Emotet or Trickbot trojans. The malware would be installed and used to survey a network, steal creds, move laterally, and gain footholds on critical servers like domain controllers to modify GPO settings. All of this amounts to a type of reconnaissance to find the most vital "crown jewels" of the company that are ripe for ransom. The most recent behavior has shown actors sending google documents with embedded links asking the user to click on the URL, which then delivers a newish-trojan named Bazar or even Cobalt Strike. Then, using Bazar's capabilities, the actors perform the same reconnaissance and establishment of footholds. The outcome of either of these initial vectors is the use of Ryuk ransomware to encrypt files and demand a payout via "*RyukReadMe.txt*" (which was the genesis of the Ryuk name).

So what's new, fascinating, or different about **Ryuk** versus other ransomware? To be honest... not much. It's just typical Spearphishing with a 2-year-old (albeit updated) variant of ransomware (if you are interested, my colleague Rod Soto from the Splunk Threat Research team also released a blog, Detecting Ryuk Using Splunk Attack Range, showing how to use the Splunk Attack Range to simulate and detect Ryuk). The reason it's hitting the news is that they are targeting healthcare facilities amid a global pandemic. Suppose I had to pick one thing out of the mix of Ryuk/Bazar/Trickbot TTPs to stay awake about? I'd probably point out that the ransomware uses the initial trojan vector to ensure that the ransomware is deployed on the most critical parts of an organization's network rather than just "encrypt and pray." Some reports have shown a 56-minute delta between initial infection and ransomware encryption activity. THAT "human touch" has been what has made it so maddeningly effective and dangerous.

Detection of Ryuk

Usually, this blog post section is filled with fun TTPs pulled from the zero-day or possibly a breakdown of a new malware variant. But, after reviewing the last six years of content that Splunk has created, I am proud to say that we already have you covered. **On top of the corpus of general ransomware detection information listed below, it is essential to note that the Splunk Threat Research team has released detections to Ryuk, Trickbot and Bazar to both Splunk Security Essentials (SSE) and Splunk Enterprise Security Content Update (ESCU) in release 3.0.9**. In my list of detections below, you will notice that I did not break out IOCs. As David Bianco has pyramidized in the past, IOCs are ephemeral and change often! I recommend working with a threat intel provider for any low-level IOCs

like hashes or IPs. Throw them into a Lookup table or ES threat intel framework, and off you go! If you don't have a threat intel provider, start skimming Twitter for some tremendous open-source lists.

Splunk Security Essentials

In case you are unaware (or living under a rock for the last two years), Splunk Security Essentials is one of the key places to get Splunk's security content. When you boot up the app, navigate to "security content," and search for Ransomware, you get a plethora of content!

On top of that, I took the MITRE ATT&CK Techniques from the CISA alert and selected the SSE detection content that mapped to them. It turns out we have over 45 searches to detect Ryuk and trojans like Bazar, Trickbot, or Emotet.

I bet you would love to get this information, wouldn't you… Well, you can either download this 825 page PDF OR copy the JSON blob here of this bookmarked content and upload it into your updated SSE local instance. As always, try in dev before prod! Also, some of these searches may need to be modified to detect Ryuk with greater confidence. Refer to the CISA alert or the excellent work from Red Canary if you want more atomic TTPs of the malware for integration into your signatures.

Historical Corpus

Now, of course, this is not the only content that Splunk has created around Ransomware. In addition, take a peek at Rod Soto's blog for some examples of where our Security Research team is developing explicit Ryuk content.

James Brodsky (our security Ransomware SC magazine author)
- Splunking the Endpoint: "Hands on!" Ransomware Edition | Recording (.conf2016 presentation)
- How Splunk Can Help You Prevent Ransomware From Holding Your Business Hostage (Blog)
- Windows Ransomware Detection with Splunk (1 of 6) – Vulnerability Detection and Windows Patch Status (YouTube Video Series)

Whitepaper
- Splunk Security: Detecting Unknown Malware and Ransomware

Splunk Phantom Resources
- Automate Your Response to WannaCry Ransomware (Blog)
- Playbook: Detect, Block, Contain, and Remediate Ransomware (Blog)

Other Ransomware Blogs to Check Out
- Detect Ransomware in Your Data with the Machine Learning Cloud Service
- Operationalize Ransomware Detections Quickly and Easily with Splunk

As always, Happy Hunting and good luck :-)

P.S. If you are much of a MITRE ATT&CK junkie as I am, take a peek at this great Bzar/ Cabolt Strike/ Ryuk ATTACK navigator that Red Canary created!

Also a big shout out to Katie Nickels for reminding me that Ransomware is still kind of a big deal. ;-)

---

[1] https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-shinigamis-revenge-long-tail-ryuk-malware

[2] https://twitter.com/search?q=%23Ryuk&src=typeahead_click

[3] https://www.washingtonpost.com/national-security/hospitals-being-hit-in-coordinated-targeted-ransomware-attack-from-russian-speaking-criminals/2020/10/28/e6e48c38-196e-11eb-befb-8864259bd2d8_story.html

Posted by

Ryan Kovar

NY. AZ. Navy. SOCA. KBMG. DARPA. Splunk.