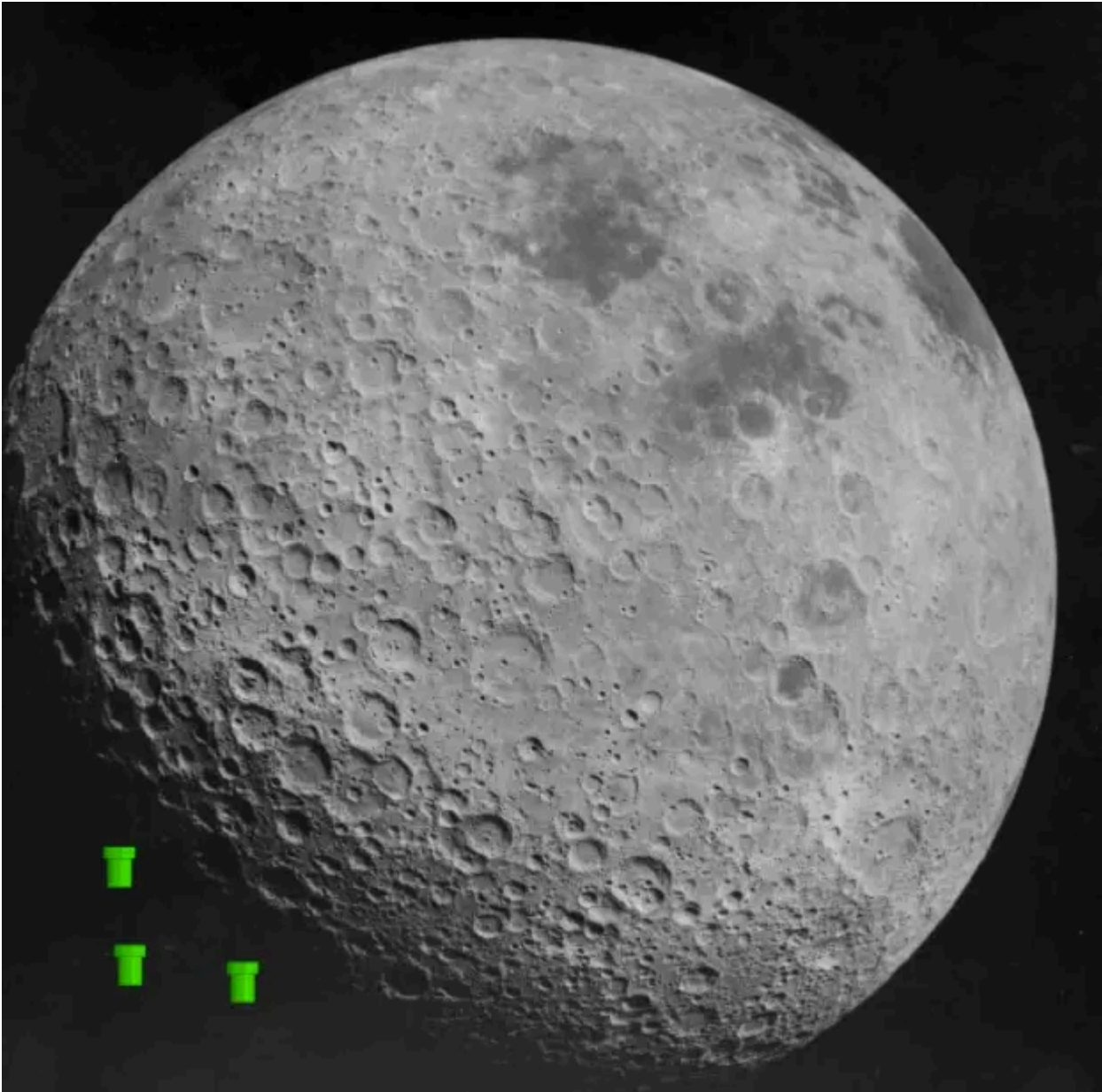


The DarkSide of the Ransomware Pipeline | Splunk

By James Brodsky

Published: 2021-05-11 · Archived: 2026-04-05 19:57:59 UTC



Authors and Contributors: [Mick Baccio](#), [Ryan Kovar](#), [Marcus LaFerrera](#), Michael Natkin, [John Stoner](#), and [Bill Wright](#).

If you want to quickly find out how to use Splunk to find activity related to the DarkSide Ransomware, skip to the “Detection and Remediation of DarkSide” section. Otherwise, read on for a quick breakdown of what happened to the Colonial Pipeline, how to detect the ransomware, and view MITRE ATT&CK mappings.

Introduction to the Colonial Pipeline Ransomware Attack

It might be more expensive for you to take that Great American Road Trip this summer because filling up the tank of the [Family Truckster](#) may cost you some serious Dogecoin. Let us give you a little bit more color on this:

Late on Friday, May 7th, one of the US's [largest gasoline pipelines was preemptively shut down](#) by operator [Colonial Pipeline](#), because their corporate computer networks were affected by [Ransomware-as-a-Service authored and maintained by the group DarkSide](#). This 5500 mile pipeline transports about 45% of the East Coast's fuel supplies, and at the time of this blog, Colonial Pipeline had not returned to full operation. Now, mind you, ***the ransomware did not directly cause the pipeline to shut down*** - rather, Colonial shut down operations voluntarily out of an abundance of caution. But until they can be sure that the adversary leveraging the DarkSide ransomware for the attack does not have the ability to affect operations, the pipeline will remain dry. Colonial is hoping to get the pipeline back to operation by the end of this week.

Regardless of how all of this plays out, what Splunk customers want to know is how to detect and mitigate DarkSide ransomware, especially if they work in critical infrastructure. In fact, last year [CISA released an alert about ransomware targeting pipeline operators](#) - so we know this is a big deal. And, they just [updated it today with new alert guidance](#) (AA21-131A) specific to DarkSide.

After review, we're happy to find that the behavior of this ransomware isn't particularly novel, and all of the guidance we've shared for years on ransomware detection and mitigation applies. Let's review that guidance, and update it where appropriate.

What You Need to Know

One of the last significant ransomware events was the [Ryuk ransomware](#) at the end of October 2020, however our specialists pointed out that Ryuk wasn't particularly novel in terms of its operation. Our Threat Research team also posted about detecting the [Clon ransomware](#) last month and [recently updated further](#).

Is the DarkSide variant of ransomware more interesting than either of these? No, it isn't! However, there's significant worldwide interest because of the target chosen. We also see these "affiliate" actors [attempt a "double extortion"](#) where not only have they encrypted critical business data, they're also threatening to release it publicly if additional ransom is not paid. DarkSide also contains a killswitch if it detects a Russian language environment. There are also [reports](#) that the ongoing global pandemic has made infections like this easier, because operational staff may be working from home and that may broaden the attack surface. However, this is not new, as remote access for Operational Technology (OT) networks is commonplace and long predates the pandemic.

Splunk & Ransomware: Not Our First Rodeo

As we've stated, this blog ain't the first time we're covering our approach to Ransomware. Feast your eyes on the following corpus of material from days of yore:

- .conf talks and videos
 - [Splunking the Endpoint 2016: Ransomware Edition!](#) and [Video](#)
 - [How Splunk Can Help You Prevent Ransomware From Holding Your Business Hostage](#)

- [Windows Ransomware Detection with Splunk \(1 of 6\) – Vulnerability Detection and Windows Patch Status](#)
- Detections Blogs
 - [Clon Ransomware Detection: Threat Research Release, April 2021](#)
 - [Ryuk and Splunk Detections Splunk Blogs](#)
 - [Detecting Ryuk Using Splunk Attack Range](#)
- Whitepaper
 - [Splunk Security: Detecting Unknown Malware and Ransomware](#)
- Phantom Responses
 - Automate Your Response to WannaCry Ransomware
 - Playbook: Detect, Block, Contain, and Remediate Ransomware
- Machine Learning Method
 - [Detect Ransomware in Your Data with the Machine Learning Cloud Service](#)
- Operationalizing Detections
 - [Operationalize Ransomware Detections Quickly and Easily with Splunk](#)

Also, looking for some fun Ransomware eye-candy to survey the kinds of infections rampant within the US over the past several years? Check out this [interactive map from Statescoop](#).

As regular readers of our blogs will expect, we normally fill this section with TTPs pulled from the zero-day or possibly a breakdown of a new malware variant. But, after reviewing the last six seven years of content that Splunk has created, we are again proud to say we already have you covered. In the list of detections below, you will notice that we 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.

The fine folks at CyberReason have a [detailed walkthrough](#) of how DarkSide behaves after the initial foothold. From a Splunk detection perspective, here are some things we suggest collecting:

- [Process execution logs](#), from our favorite Windows Security 4688 events, or [Sysmon EventCode 1](#), or any commercial EDR, are, as always, key to detection of the parent/child process relationships involved in actions on intent and lateral movement as well as the [deletion of Volume Shadow Copies](#).
- [PowerShell Script Block Logging](#) is also critical, so that you can detect certain modules like WebClient.DownloadFile being used where you don't expect, as well as the use of encoded PowerShell.
- [Windows System events](#), so that you can detect Scheduled Tasks being created and enabled (4698, 4700).

And as always, **unusual network connections** from servers and endpoints (can be accomplished via firewall, proxy, [Sysmon EventCode 3](#), or EDR logs) and [DNS query logging](#) will be helpful.

Splunk Security Essentials

In case you are unaware (or living under a rock for the last two years), [Splunk Security Essentials](#) is the place to get Splunk's security content. And since our last-go round with Ryuk, we've updated [Splunk Security Essentials](#) and made it a fully-supported Splunk product (but it's still free!). When you boot up the app, navigate to "Security Content Library," and search for Ransomware, you get a plethora of content!

 Splunk Security Essentials - Ransomware content

Splunk Enterprise Security and ESCU

Know Thyself

While we have spent some time explaining this attack and effort needs to be put toward investigating this, it is also important to note that the basics are important. Basic asset management, hopefully via your asset and identity framework, will tell you where your vulnerable systems reside. Running regular vulnerability scans that integrate into Splunk will display which systems are vulnerable and can help you prioritize your patching schedule and better focus your detection efforts.

 Splunk Enterprise Security and ESCU

Threat Intelligence Framework

If you are using [Splunk Enterprise Security \(ES\)](#), many organizations are posting IOCs that can be ingested easily into the threat intelligence framework. Perhaps you aren't sure how to do that? No worries, we published some guidance and a how-to on integrating lists of [IOCs into the Enterprise Security threat intelligence framework](#). We won't be publishing a list of IOCs along with this blog as they are quite ephemeral, but use of the Threat Intelligence Framework (or standard lookups within Splunk) will allow you to easily perform IOC matching.

Enterprise Security Content Updates (ESCU)

For folks using ESCU, our Splunk Threat Research team will release a new Splunk Analytic Story called Darkside Ransomware by the end of this week containing detections for this threat. Saying that, check out the MITRE ATT&CK table below. If you have ESCU running today, you already have some great coverage!

MITRE ATT&CK

Reviewing one of the first blog posts on DarkSide Ransomware from [Digital Shadows](#) in September 2020, we extracted their MITRE ATT&CK tactics and then linked to Splunk Content to help you hunt for that information. Be aware; these searches are provided as a way to accelerate your hunting. We recommend you configure them via the Splunk Security Essentials App. You may need to modify them to work in your environment! Many of these searches are optimized for use with the [tstats](#) command.

Finally, as more information becomes available, we will update these searches if more ATT&CK TTPs become known.

Conclusion

We know that such a publicly visible example of the impact of Ransomware can stoke visceral fear, but we've got your back. Hopefully, these searches, blogs, videos, conference papers, and whitepapers will provide you the ability to have more visibility into your environment and any malicious activity that you might be experiencing. If they don't work perfectly, think of them as "SplunkSpiration" :-). As soon as we have more information, we will update this blog and, as we talked about earlier, be on the lookout for some more detailed info about DarkSide and an Analytic Story delivered via ESCU from our Splunk Threat Research team.

Source: https://www.splunk.com/en_us/blog/security/the-darkside-of-the-ransomware-pipeline.html