

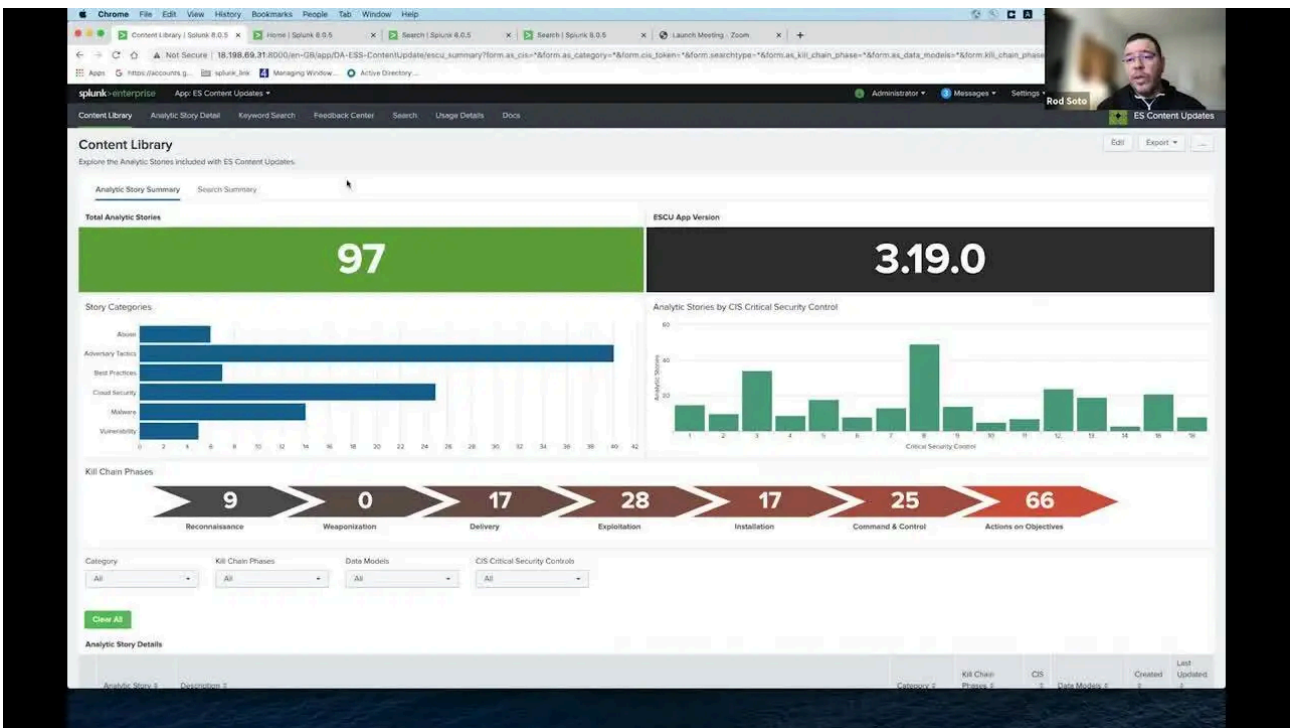
Clop Ransomware Detection: Threat Research Release, April 2021 | Splunk

By Splunk Threat Research Team

Published: 2021-05-03 · Archived: 2026-04-06 01:37:19 UTC

Splunk is committed to using inclusive and unbiased language. This blog post might contain terminology that we no longer use. For more information on our updated terminology and our stance on biased language, please visit [our blog post](#). We appreciate your understanding as we work towards making our community more inclusive for everyone.

[Clop Ransomware](#) has been active since 2019 and has been mostly associated with financially-driven criminal groups. However, lately this ransomware payload has been observed in campaigns against universities and other institutions in the education vertical. Most recently, Clop Ransomware has been used in a cyberattack that demanded one of the highest ransom amounts in recorded history ([\\$20 million](#)), and one of the particular items associated with the actors behind the Clop Ransomware is blackmailing their victims through threatening to publish sensitive information exfiltrated from victims' networks. Within this past month in April, we saw that [Clop Ransomware-related threats](#) were persistent throughout the distinct variants used by several groups of organized criminals and decided to focus our research efforts on Clop Ransomware detections. We hope that these detections will help organizations detect abnormal behavior faster before it becomes detrimental. Watch this video to learn more.



Detection Searches for Clop Ransomware

As we state in our blog, "[Detecting Clop Ransomware](#)," the actors behind this crimeware send the malicious payloads via different methods, such as phishing emails, then proceed to spread ransomware payload post-exploitation by pivoting to exposed or related vulnerable systems. Although the actual developers of this crimeware have not been identified yet, they have been tied to several [financially-driven](#) threat actors. They are also known for leveraging public available vulnerabilities as [entry and post-exploitation vectors](#).

The most common method behind this crimeware is as follows: once they have infiltrated their targets, they then present instructions on how to pay ransom and communicate further threats of exposure by publishing the sensitive information they obtained on a publicly accessible website.

Source [*](#)

Although this may appear as a new modality, in reality ransomware is usually the cherry on top of the cake, as malicious actors usually dwell, exfiltrate and qualify exfiltrated data, which eventually lands on dark web public forums, dark markets or private crime intelligence brokers where qualified financial, business and kompromat information is then priced and sold to the highest bidder.

We used our [attack range](#) tool to demonstrate and research how this malware payload infects and spreads once executed. A number of new searches has been created to address this threat:

Please see our blog "[Detecting Clop Ransomware](#)" for specific information about the events and SPL code involved in these detections. We also provide information about a Splunk Phantom playbook that can be used to defend against this threat.

Why Should You Care?

Having the paid ransom amounts in recorded history ([\\$20 million](#)) and the fact that the Clop Ransomware actors are extremely opportunistic makes this a specially worrisome actor. The actors behind this crimeware are constantly looking for vulnerable targets, and once they are able to infiltrate victims, they are driven by obtaining sensitive information which most likely will end up sold in a dark market.

Ransomware campaigns involving this payload will continue, as this group continuously targets different verticals it is important to prepare and understand the workings of these malicious payloads and prepare your environment in order to defend and be resilient against a ransomware attack. You can use our pre-packaged detections to help your organization stay safe against these types of attacks.

For a full list of security content, check out the release notes on [Splunk Docs](#):

- [3.18.0](#) (Clop Story)
- [3.19.0](#)

Learn More

You can find the latest content about security analytic stories on [GitHub](#) and in [Splunkbase](#). All of these detections are also now available via push update in [Splunk Security Essentials](#).

Feedback

Any feedback or requests? Feel free to submitput in an i Issue on Github and we'll follow up. You can also join us on the [Slack](#) channel **#security-research**. Follow [these](#) instructions If you need an invitation to our Splunk user groups on Slack.

Source: https://www.splunk.com/en_us/blog/security/clop-ransomware-detection-threat-research-release-april-2021.html