HC3: Alert

August 24, 2021 TLP: White Report: 202108241000

Indicators of Compromise Associated with OnePercent Group Ransomware

Executive Summary

The FBI shared indicators of compromise (IOCs) associated with the ransomware threat actors the OnePercent Group. The OnePercent Group uses IceID-infected phishing email attachments to install ColbaltStrike and other malware on their victims' computers. The "OnePercent Group actors' extortion tactics always begin with a warning and progress from a partial leak of data to a full leak of all the victim's exfiltrated data" if their ransom is not paid.

Because the OnePercent Group uses the rclone program, the FBI recommends "organizations be aware" of the hashes associated with rclone that are included in their alert. "Rclone is a command line program to manage files on cloud storage."

Report

FBI – Flash Alert (CU-000149-MW) Indicators of Compromise Associated with OnePercent Group Ransomware
https://www.ic3.gov/Media/News/2021/210823.pdf

Impact to HPH Sector

While HC3 is not aware of any Healthcare and Public Health (HPH) Sector entities target by the OnePercent Group, IceID and ColbaltStrike malware has affected the HPH Sector in the past. Sector entities targeted by ransomware could have some or all of their data leaked if a ransom is not paid and experience disruptions to services provided to their patients and customers.

References

CISA - Additional Resources Related to the Prevention and Mitigation of Ransomware
https://www.stopransomware.gov

Rclone - About rclone
https://rclone.org/

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback