FINISHED INTELLIGENCE REPORTS

FBI Releases Indicators of Compromise Associated with OnePercent Group Ransomware

TLP:WHITE

Aug 24, 2021

The US Federal Bureau of Investigation (FBI) has learned of a cyber-criminal group who self-identifies as the “OnePercent Group” and who have used Cobalt Strike to perpetuate ransomware attacks against US companies since November 2020.

OnePercent Group actors compromise victims through a phishing email in which an attachment is opened by the user. The attachment’s macros infect the system with the IcedID banking trojan.

IcedID downloads additional software to include Cobalt Strike. Cobalt Strike moves laterally in the network, primarily with PowerShell remoting.

Please see the attached **FBI Flash** for additional insight and IOCs.

The FBI FLASH alert does not provide detailed information on OnePercent Group's past attacks or the encryptor used, making it hard to attribute them as an affiliate of a specific Ransomware-as-a-service.

However, the agency did link OnePercent Group to the notorious REvil (Sodinokibi) ransomware gang, whose data leak site they have used to leak and auction their victims' stolen files.

"If the ransom is not paid in full after the "one percent leak," OnePercent Group actors threaten to sell the stolen data to the Sodinokibi Group to publish at an auction," the FBI said.

Reference(s)	Bleeping Computer
Report Source(s)	FBI

Release Date
Aug 24, 2021

Sources
BleepingComputer: FBI: OnePercent Group Ransomware Targeted US Orgs Since Nov 2020

Alert ID 32c4f20c

View Alert

Tags OnePercent Group, FBI Flash, Ransomware

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.