ultraviolet

THREAT REPORT:

May Means Black Basta

Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
5/16/2024

Contents

1 Executive Summary

Back in May 2023, we reported on Black Basta activity within the European Union. This past week, Black Basta was at it again with a ransomware attack against Ascension healthcare system in the United States. Since late April of 2024, Black Basta has been associated with ongoing campaigns against healthcare sectors. The group has been attributed with using legitimate tools to compromise organizations. Please monitor use of Microsoft's built-in 'Quick Assist', 'AnyDesk', and especially any instances of ConnectWise's 'ScreenConnect' still vulnerable to CVE-2024-1709, the trivial URL exploit which allows threat actors administrative access to targeted hosts.

2 Technical Analysis

Black Basta used to operate under the name Conti, which was linked to some previous Emotet campaigns. Conti gained international backlash when they breached Ireland's public healthcare system in May of 2021. Conti publicly released the decryption keys but still demanded payment for the data stolen. Conti was then hacked in February 2022, presumably due to their support of the Russian invasion of Ukraine. Black Basta emerged in April of 2022 by compromising a dozen companies internationally. In May of 2023, the group compromised the networks of German automotive manufacturer 'Rheinmetall' and Swiss electrification and automation technology provider 'ABB'.

On Friday, May 10th, 2024, CISA (Cybersecurity & Infrastructure Security Agency) released a cybersecurity advisory on Black Basta. The threat actor group has been attributed by the FBI, CISA, HHS and MS-ISAC with ransomware attacks which have 'stolen data from at least 12 out of 16 critical infrastructure sectors'[1]. The CISA alert shared IoC's (Indicators of Compromise) and TTP's (Tactics, Techniques and Procedures) with network defenders.

A typical attack chain starts with a spear phishing attempt, with some affiliates of the ransomware as a service (RaaS) group using Qakbot for initial access. Threat actors then tend to use harmless-looking filenames like 'Dell' or 'Intel' for instances of 'SoftPerfect' (netscan.exe) within the root drive. Affiliates typically move laterally with BITSAdmin, PsExec or by RDP (Remote Desktop Protocol). This is where researchers have also observed some affiliates utilizing Splashtop, ScreenConnect or Cobalt Strike beacons to remotely access target hosts within the network. At that point, the standard use of Mimikatz or other exploitable vulnerabilities on the target hosts then scrape for administrative credentials. Black Basta still likes to use ChaCha20 for encrypting data during the exfiltration phase.

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- Follow patching policy and apply updates for firmware, software and all operating systems in a timely manner
- Deploy and require multi-factor authentication where feasible
- Implement or maintain ongoing user training for how to identify and report phishing attempts

5 References

After Ascension ransomware attack, feds issue alert on Black Basta . (2022, May 10). Retrieved May 16, 2022, from https://therecord.media/black-basta-ransomware-alert-healthcare-fbi-cisa-hhs

[1]Https://www.cisa.gov/news-events/cybersecurity-adv. (2022, May 10). Retrieved May 16, 2024, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a

https://therecord.media/black-basta-ransomware-alert-healthcare-fbi-cisa-hhs. (2024, May 10). Retrieved May 16, 2024, from https://therecord.media/black-basta-ransomware-alert-healthcare-fbi-cisa-hhs

Windows Quick Assist abused in Black Basta ransomware attacks. (2022, May 15). Retrieved May 16, 2024, from https://www.bleepingcomputer.com/news/security/windows-quick-assist-abused-in-black-basta-ransomware-attacks/