Black Basta Threat Actor Emerges as a Major Threat to the Healthcare Industry

Threat Bulletins **TLP:WHITE** **Alert Id: 1b76422a** **2024-05-10 12:10:11**

The notorious ransomware group, Black Basta, has recently accelerated attacks against the healthcare sector. Health-ISAC is urging all Healthcare and Public Health (HPH) sector entities to review this threat bulletin and follow the recommended actions below.

Black Basta emerged in early 2022 and quickly became one of the most active ransomware-as-a-service (RaaS) threat actors. They use double extortion tactics, encrypting victims' data and threatening to leak sensitive information on their public leak site on Tor, named Basta News. The group has allegedly extorted over 100 million dollars since its emergence, making it one of the most prolific active ransomware strains.

The threat actor is financially motivated and has opportunistically targeted the healthcare sector as a part of their malicious operations. In the past month, at least two healthcare organizations, in Europe and in the United States, have fallen victim to Black Basta ransomware and have suffered severe operational disruptions. Taking these latest developments into consideration, Health-ISAC has assessed that Black Basta represents a significant threat to the healthcare sector. Members are strongly advised to keep an eye on the threat actor and their tactics, techniques and procedures (TTPs).

Black Basta's malware, written in C++, targets both Windows and Linux systems. It encrypts data using ChaCha20 and RSA-4096 and attempts to delete shadow copies and backups.

The group has been linked to the defunct Conti threat actor group due to similarities in their operations. There are suspicions that the group is also linked to another actor FIN7 due to similarities in their tools and TTPs. The level of sophisticated TTPs deployed by the group corresponds to a more mature operation which could be explained by connections to the more established threat actors like Conti and FIN7.

The threat actor is using spearphishing attacks and has also been seen buying compromised credentials through Initial Access Brookers (IABs) to obtain means of initial access.

In some of the previous attacks the group also used the following vulnerabilities to breach organizations:

- ConnectWise ScreenConnect authentication bypass vulnerability - **CVE-2024-1709**, and path-traversal vulnerability - **CVE-2024-1708**
- Microsoft Windows common log file system driver elevation of privilege vulnerability - **CVE-2022-35803**
- VMware OpenSLP vulnerability - **CVE-2021-21974**
  Fortra GoAnywhere MFT pre-authentication command injection vulnerability **CVE-2023-0669**

Black Basta uses advanced techniques to evade detection by security solutions and hinder file recovery from backups. These include obfuscation and polymorphism, Living Off the Land (LotL), anti-analysis and sandbox detection, memory execution, disabling security solutions, and deleting backups. These techniques make it difficult for antivirus solutions to detect and prevent file recovery without the decryption key. The ransomware also uses legitimate system tools AnyDesk, AteraAgent and Splashtop, and processes to move laterally into the network, and execute malicious actions. Other common tools identified being used by the Black Basta affiliates in the infection chain are Qakbot (aka QBot), SystemBC, Mimikatz, Cobalt Strike, and Rclone.

Organizations are advised to remain vigilant to any suspicious activity in their environments and to apply recommendations from the following section.

More technical analysis, as well as mapped TTPs, are available in Kroll's analysis: Black Basta - Technical Analysis.

Recommendations:

- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.
- Regularly update software and operating systems to patch vulnerabilities.
- Implement strong email security measures to prevent phishing attacks.
- Limit account access privileges across organizations.
- Use a combination of antivirus, anti-malware, and firewall solutions to protect against threats.
- Regularly back up data and ensure backups are isolated and immutable.
- Conduct cybersecurity awareness training for employees to recognize and report suspicious activities such as phishing attempts.
- Monitor networks for suspicious activity and have an incident response plan in place.
- Create and implement a business continuity plan to ensure minimal operational disruptions in case of a ransomware incident.

Reference(s): Kroll, HHS, sectrio, incibe, Fortinet, Reuters, HHS

Sources:

Ransomware Roundup - Black Basta

Black Basta: Response and Recovery Actions

Threat Profile: Black Basta (HC3)

Black Basta - Technical Analysis

Ransomware Group ‘Black Basta’ Has Raked In More Than $100 Million -Researchers

Tags: Black Basta 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