FBI: BlackByte ransomware breached US critical infrastructure

bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/

Sergiu Gatlan

By
Sergiu Gatlan

- February 14, 2022
- 10:41 AM
- 0

The US Federal Bureau of Investigation (FBI) revealed that the BlackByte ransomware group has breached the networks of at least three organizations from US critical infrastructure sectors in the last three months.

This was disclosed in a TLP:WHITE joint cybersecurity advisory released Friday in coordination with the US Secret Service.

"As of November 2021, BlackByte ransomware had compromised multiple US and foreign businesses, including entities in at least three US critical infrastructure sectors (government facilities, financial, and food & agriculture).," the federal law enforcement agency said [PDF].

"BlackByte is a Ransomware as a Service (RaaS) group that encrypts files on compromised Windows host systems, including physical and virtual servers."

The advisory focuses on providing indicators of compromise (IOCs) that organizations can use to detect and defend against BlackByte's attacks.

The IOCs associated with BlackByte activity shared in the advisory include MD5 hashes of suspicious ASPX files discovered on compromised Microsoft Internet Information Services (IIS) servers and a list of commands the ransomware operators used during attacks.

The 49ers ransomware attack

In related news, NFL's San Francisco 49ers team revealed over the weekend that it's recovering from a BlackByte ransomware attack.

The threat actors claimed the attack, saying that they also stole data from the football org's servers during the incident and leaked almost 300MB worth of files on their data leak blog.

The 49ers confirmed the ransomware attack in a statement to BleepingComputer and said it only caused a temporary disruption to portions of its IT network.

BlackByte ransomware operation has been active since at least July 2021, when it started targeting corporate victims worldwide.

This gang is known for exploiting software vulnerabilities (including Microsoft Exchange Server) to gain initial access to their enterprise targets' network, illustrating that keeping your servers updated will most likely block their attacks.

In October, cybersecurity firm Trustwave created and released a free BlackByte decryptor, enabling some victims to restore their files for free after the ransomware gang used the same decryption/encryption key in multiple attacks.

The two agencies also shared a list of measures that can help admins mitigate BlackByte attacks:

- Implement regular backups of all data to be stored as air gapped, password protected copies offline. Ensure these copies are not accessible for modification or deletion from any system where the original data resides.
- Implement network segmentation, such that all machines on your network are not accessible from every other machine.
- Install and regularly update antivirus software on all hosts, and enable real time detection.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind. Do not give all users administrative privileges.

- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs for any unusual activity.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Use double authentication when logging into accounts or services.
- Ensure routine auditing is conducted for all accounts.
- Ensure all the identified IOCs are input into the network SIEM for continuous monitoring and alerts.

Related Articles:

Cybersecurity agencies reveal top initial access attack vectors

FBI, CISA, and NSA warn of hackers increasingly targeting MSPs

FBI: BlackCat ransomware breached at least 60 entities worldwide

FBI warns of ransomware attacks targeting US agriculture sector

US and allies warn of Russian hacking threat to critical infrastructure