LockBit ransomware gang lurked in a U.S. gov network for months

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** April 12, 2022 10:15 AM **0**

A regional U.S. government agency compromised with LockBit ransomware had the threat actor in its network for at least five months before the payload was deployed, security researchers found.

Logs retrieved from the compromised machines showed that two threat groups had compromised them and were engaged in reconnaissance and remote access operations.

The attackers tried to remove their tracks by deleting Event Logs but the pieces of the files remained allowed threat analysts to get a glimpse of the actor and their tactics.

Initial compromise

The initial access allowing the attack was a protective feature that one of the agency's technicians left disabled following a maintenance operation.

According to researchers at cybersecurity company Sophos, the actor accessed the network through open remote desktop (RDP) ports on a misconfigured firewall and then used Chrome to download the tools needed in the attack.

The toolset included utilities for brute-forcing, scanning, a commercial VPN, and free tools that allow file management and command execution, such as PsExec, FileZilla, Process Explorer, and GMER.

Additionally, the hackers used remote desktop and remote management software like ScreenConnect, and later in the attack, AnyDesk.

From there, the attackers spent time laying low and just tried to steal valuable account credentials to expand their compromise of the network.

At some point, they snatched the credentials of a local server admin who also had Domain Administrator permissions, so they could create on other systems new accounts with administrator privileges.

Upping the game

In the second phase of the attack, initiated five months after the initial compromise, a more sophisticated actor appears to have taken over, leading Sophos to assume that a higher-level actor was now in charge of the operation.

> "The nature of the activity recovered from logs and browser history files on the compromised server gave us the impression that the threat actors who first broke in to the network weren't experts, but novices, and that they may later have transferred control of their remote access to one or more different, more sophisticated groups who, eventually, delivered the ransomware payload" - Sophos (https://news.sophos.com/en-us/2022/04/12/attackers-linger-on-government-agency-computers-before-deploying-lockbit-ransomware/)

The new phase started with installing the Mimikatz and LaZagne post-exploitation tool for extracting credentials sets from the compromised server.

The attackers made their presence more evident by wiping logs and performing system reboots via remote commands, alerting the system admins who took 60 servers offline and segmented the network.

A second error during this incident response disabled endpoint security. From this point, the two parties engaged in an open confrontation of measures and countermoves.

> "A steady stream of table-setting activities took place as the attackers dumped account credentials, ran network enumeration tools, checked their RDP abilities, and created new user accounts, presumably to give

themselves options in case they were interrupted" - Sophos (https://news.sophos.com/en-us/2022/04/12/attackers-linger-on-government-agency-computers-before-deploying-lockbit-ransomware/)

"On the first day of the sixth month of the attack, the attacker made their big move, running Advanced IP Scanner and almost immediately beginning lateral movement to multiple sensitive servers. Within minutes, the attacker has access to a slew of sensitive personnel and purchasing files," informs the report from Sophos.

Sophos joined the response effort and shut down the servers that provided remote access to the adversaries, but part of the network had already been encrypted with LockBit.

On a few machines, although the files had been renamed with LockBit's suffix, no encryption had taken place, so restoring them was a matter of reversing the renaming action.

Takeaway

The researchers say that implementing multi-factor authentication (MFA) protection would have lead to a different outcome, as it would have stopped the hackers from moving freely or at least significantly hinder their action on the compromised network.

Another critical security feature that could have slowed down the threat actors is a firewall rule blocking remote access to RDP ports.

Finally, this case highlights the issue of maintenance and incident response errors and the need to follow security checklists even in urgent situations.

Related Articles:

The Week in Ransomware - March 25th 2022 - Critical infrastructure (https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-25th-2022-critical-infrastructure/)

Ten notorious ransomware strains put to the encryption speed test (https://www.bleepingcomputer.com/news/security/ten-notorious-ransomware-strains-put-to-the-encryption-speed-test/)

Dozens of ransomware variants used in 722 attacks over 3 months (https://www.bleepingcomputer.com/news/security/dozens-of-ransomware-variants-used-in-722-attacks-over-3-months/)

Bridgestone Americas confirms ransomware attack, LockBit leaks data (https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/)

REvil ransomware member extradited to U.S. to stand trial for Kaseya attack (https://www.bleepingcomputer.com/news/security/revil-ransomware-member-extradited-to-us-to-stand-trial-for-kaseya-attack/)