Attacks/Breaches | 4 MIN READ NEWS

CISA: Multiple APT Groups Infiltrate Defense Organization

Advanced attackers gained access to Microsoft Exchange services, conducted searches of email, and used an open source toolkit to collect data from the network for nearly a year.

Robert Lemos
Contributing Writer, Dark Reading

October 05, 2022

Source: Panther Media via Alamy

Multiple advance persistent threat (APT) groups gained access to the network of a US-based defense organization in January 2021, extensively compromising the company's computers, network, and data for nearly a year, three government agencies stated in a joint advisory on Oct. 4.

The attackers had access to the organization's Microsoft Exchange Server and used a compromised administrator account to collect information and move laterally in the IT environment as early as mid-January 2021, according to the advisory issued by the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI).

The attackers gained access to email messages and defense contract information, collected credentials to elevate user privileges, and deployed a custom exfiltration tool, CovalentStealer, to move the data to an external server.

Most of the techniques used software already on the system or widely available open source tools, Katie Nickels, director of intelligence at Red Canary, a managed detection and response (MDR) firm, said in a statement sent to Dark Reading.

"While many people think that state-sponsored actors always use advanced techniques, this report demonstrates that many of the tools and techniques these actors use are known to defenders and can be detected," she stated.

For instance, a new Exchange vulnerability could have been used for initial access, but there are plenty of Exchange vulnerabilities that remain unpatched in corporate networks, Nickels said.

"The advisory notes that actors did exploit multiple known vulnerabilities from 2021 to install webshells on the Exchange server later in the intrusion," she said. "There have been multiple Exchange vulnerabilities over a span of years, and given the challenges of patching on-premise Exchange servers, many of these vulnerabilities remain unpatched and give adversaries an opportunity to compromise a network."

Impacket: An Open Source, Common Vecto

"The APT cyber actors used existing, compromised credentials with Impacket to access a higher privileged service account used by the organization's multifunctional devices," the advisory stated.

As for CovalentStealer, it includes two configurations that specifically target the victim's documents using predetermined file paths and user credentials. It then encrypts collected data and uploads the files to a folder on the Microsoft OneDrive cloud storage service, an action that can be configured to happen only at certain times and limited to certain types of data.

The use of such a custom tool can make detection and mitigation more difficult, but most of the actions taken by the threat groups use known tools and techniques, Red Canary's Nickels stated.

"Impacket regularly makes the Red Canary 'top 10' list of threats observed in customer environments — in September, it was the fourth most prevalent threat we observed," she said.

Impacket can be detected if companies have visibility into the processes running on the endpoint and traffic on the network, although a third of detections were from legitimate testing activities, she said.

State-Sponsored, Financial Techniques Converge

The warning of an extensive attack comes as defense contractors remain in the crosshairs. Data breaches and ransomware incidents have grown as a concern for all organizations. And while custom malware can make cyber-espionage operations difficult to detect, the much more common data breaches, such as those faced by Uber and the Los Angeles Unified School District, use known tools and vulnerabilities, according to Mike Wiacek, CEO and founder of Stairwell, a cybersecurity intelligence platform.

"For commercial organizations, it's important to remember that an actor does not need to be an 'advanced persistent threat' to scan for open network shares holding sensitive data," he said in an analysis shared with Dark Reading. "Security hygiene is vital in ensuring that sensitive data is not sitting on open network shares, where a single compromised set of VPN credentials can then lead to valuable intellectual property being lost."

The federal advisory made specific recommendations to organizations in the Defense Industrial Base (DIB) to prevent compromises and minimize the damage caused by successful APT groups. CISA recommends that organizations monitor log files for signs of suspicious communications, especially those using unusual virtual private server (VPS) or virtual private network (VPN) services. Segmenting networks, monitoring systems for anomalous behavior, and restricting the use of remote-access tools are among the practices the US agencies recommend.