Targeted Attack Exposes OWA Weakness

By Michael Mimoso

Published: 2015-10-06 · Archived: 2026-04-05 15:39:18 UTC

A targeted attack has been uncovered in which hackers were able to burrow onto the corporate network and steal thousands of username-password combinations via Outlook Web Access.

Attackers aiming for lateral movement inside an enterprise network have done well in the past to target domain controller credentials.

Researchers at Cybereason, however, have uncovered a targeted attack in which hackers were able to burrow onto the corporate network and steal thousands of username-password combinations via Outlook Web Access.

“Security professionals are very aware of the value of their domain-controllers, and consider those as the keys to the castle, without realizing that the OWA server gives essentially identical access,” said Cybereason CTO and cofounder Yonatan Striem-Amit.

The attack was carried out for months against an organization with 19,000 endpoints, and credentials for more than 11,000 user accounts were sniffed and stolen.

OWA enables remote access to Outlook and Exchange Server in organizations that wish to roll it out. And because it faces the Internet and internal infrastructure, it’s a tempting target for advanced attackers who wish to spy or steal on an organization’s activities.

“This configuration of OWA created an ideal attack platform because the server was exposed both internally and externally,” Striem-Amit said. “Moreover, because OWA authentication is based on domain credentials, whoever gains access to the OWA server becomes the owner of the entire organization’s domain credentials.”

In this case, the attackers used stolen credentials to load a malicious and unsigned dynamic library onto the OWA server. The module was used to open a backdoor to a command and control server and to record credentials for most of the accounts in the organization.

“Although it had the same name as another benign DLL, the suspicious DLL went unsigned and was loaded from a different directory,” Cybereason wrote in a report.

Striem-Amit added that a forensics investigation concluded there was no advanced malware used to gain initial entry in the attack.

“As there was no zero-day, the only ‘vulnerability’ is OWAs willingness to happily load unsigned DLLs, which is the default behavior in most servers and Windows-based machines,” he said.

This technique is a new twist for APT gangs, most of which rely on phishing as an initial foothold on a network. Once legitimate access is gained via stolen credentials, attackers try to pivot internally until landing on a resource

they covet—which in this case was all of the organization's OWA credentials.

The backdoored OWAAUTH.dll, was used by OWA for authentication against the organization's Active Directory server. The attackers also installed an ISAPI filter for IIS, which was used to filter HTTP requests to the server.

"This enabled the hackers to get all requests in cleartext after SSL/TLS decryption," Striem-Amit said. "The malware replaced the OWAAUTH [library] by installing an IIS filter in the registry, which enabled the malware to automatically load and persist on every subsequent server restart."

The DLL then loaded another HTTP module that grabbed the malware logic and backdoor, Cybereason said.

"The interesting part of this attack is the value they hackers got from this particular backdoor. Not only were they able to access the specific compromised server, they also got access to all the username/passwords of every user in the organization," Striem-Amit said. "This way, they get a very robust way to get in, and leverage any other compromised asset as complete access to every other resource."

The attackers were able to sit on the network and sniff for variables passed in request queries that looked like username-password combinations whenever users logged into OWA. The researchers said they found 11,000 such pairs, essentially for every identity and asset in the organization. The backdoor also contained a special parameter with the particular organization's name in it, lending more proof that they were specifically targeted. The backdoor allowed the attackers access to the OWA server where they could execute any code and using the stolen credentials, impersonate any user—all without attacking the domain controller, which was a target in some other high profile attacks.

"While most security professionals understand the sensitivity of data in the A/D server, the OWA server serves as a focal point for the exact same sensitive data," Striem-Amit said.
