Featured Articles 10.05.15

New OWA attack steals Outlook passwords

BY SECURITY DISPATCH (http://darkmatters.norsecorp.com/author/previouscontributors/)

()

Businesses beware. Security firm Cybereason researchers recently discovered a backdoor in Microsoft's Outlook Web Application (OWA) that steals passwords. Dan Godin of Ars Technica reported this morning (http://arstechnica.com/security/2015/10/new-outlook-mailserver-attack-steals-massive-number-of-passwords/?):

> *Researchers have uncovered advanced malware that can steal virtually all of a large organization's e-mail passwords*

> *by infecting its Outlook Web Application (OWA) mail server over an extended period of time.*

The attack allowed a malicious module to be loaded onto the Microsoft Outlook Web Application (OWA), where the attackers were able to record authentication credentials that provided them with backdoor capabilities. With the ability to collect and retain ownership over user credentials — the attackers were able to maintain persistent control over the targeted organization environment.

Researchers first noted that a suspicious DLL that had some very interesting characteristics:

- The suspicious DLL was unsigned
- The suspicious DLL was loaded from a different directory

Researchers stated in their lab analysis that the configuration of OWA:

> *…created an ideal attack platform because the server was exposed both internally and externally. 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. Later, we will see how the attacker extracted credentials from the OWA server using their malicious module.*

Nest, the hackers backdoored OWAAUTH.dll (an authentication mechanism) and installed an ISAPI filter on the IIS server, thus filtering HTTP requests. The lab analysis further elaborated that:

> *This enabled the hackers to get all requests in cleartext after SSL/TLS decryption. The malware replaced the OWAAUTH by installing an IIS filter in the registry, which enabled the malware to automatically load and persist on every subsequent server restart.*

To add icing to the directory cake — the hackers utilized the .NET assembly cache in order to avoid auditing or inspection. Next, the hackers hooked the request handlers and captured the OWA authentication tokens. It was also discovered that the malware searched all incoming requests for a special parameter: "<CustomerName>XXX" — upon finding the parameter, the "backdoor functionality would parse the remainder of the parameters."

This threat is insidious and network administrators should investigate their OWA configuration, security practices, and monitor OWA for potential backdoors.

Source: Webmail Server APT (http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Labs-Analysis-Webmail-Sever-APT.pdf): A New Persistent Attack Methodology Targeting Microsoft Outlook Web Application (OWA)

Security Dispatch

[Darkmatters] Security Blips...

▶ MORE POSTS (623)

(http://darkmatters.norsecorp.com/author/[illegible]

TOPICS: .NET ASSEMBLY, ACCOUNT CREDENTIALS, APT, ATTACK METHODOLOGY, ATTACK PLATFORM, AUTHENTICATION, BACKDOOR, CYBEREASON, HACKERS, HTTP REQUESTS, IIS, MICROSOFT OUTLOOK, OUTLOOK WEB APPLICATION, OWA, OWA SERVER, OWAAUTH.DLL,