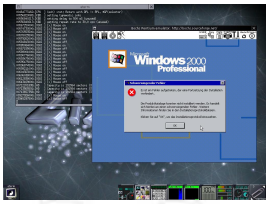


Mehr als zehn Hacker-Gruppen stürzen sich auf Microsoft-Exchange-Sicherheitslücken - ESET identifiziert bereits mehr 5.000 infizierte E-Mail-Server, vor allem in Deutschland

Die kürzlich publik gemachten Sicherheitslücken in Microsoft Exchange schlagen immer höhere Wellen. So entdeckten die Forscher des IT-Sicherheits-Herstellers ESET mehr als zehn verschiedene APT-Gruppen (Advanced Persistent Threats), welche die Schwachstellen derzeit verstärkt ausnutzen, um E-Mail-Server zu kompromittieren und an Unternehmensdaten zu gelangen. Die Bedrohung ist also nicht auf die chinesische Hafnium-Gruppe beschränkt, wie bislang vermutet wurde. ESET identifizierte weltweit rund 5.000 E-Mail-Server von Unternehmen und Regierungseinrichtungen, die kompromittiert wurden. Die meisten Ziele der Hackergruppen liegen in Deutschland. Die Telemetrie der Security-Experten zeigte das Vorhandensein von sogenannten Webshells. Diese bösartigen Programme oder Skripte ermöglichen die Fernsteuerung eines Servers über einen Webbrowser.

Einsatz von Frühwarnsystemen empfehlenswert

Der Einsatz sogenannter "Endpoint Detection und Response"-Lösungen (EDR-Lösungen) hätte in vielen Fällen den Diebstahl von Unternehmensdaten eingrenzen bzw. verhindern können. "Mit Hilfe von EDR-Lösungen, wie beispielsweise ESET Enterprise Inspector, wären Administratoren frühzeitig auf verdächtige Aktivitäten aufmerksam gemacht worden. So hätte der Abfluss von Unternehmensdaten trotz Ausnutzung des Sicherheitslücke frühzeitig registriert werden können, um diesen durch entsprechende Maßnahmen zu unterbinden", erklärt Michael Schröder, Security Business Strategy Manager bei ESET Deutschland.

Um den Sicherheitsstatus beurteilen zu können, sollten Exchange-Server auf die folgenden Erkennungen überprüft werden:

* JS/Exploit.CVE-2021-26855.Webshell.A
* JS/Exploit.CVE-2021-26855.Webshell.B
* ASP/Webshell
* ASP/ReGeorg

ESET-Analysen zeigen Cyberspionage-Gruppen auf

"Seit dem Tag der Veröffentlichung der Patches durch Microsoft beobachteten wir, dass immer mehr Hacker massenhaft Exchange-Server scannen und kompromittieren. Interessanterweise handelt es sich dabei durchweg um APT-Gruppen, die für Spionagetätigkeiten berüchtigt sind. Wir sind uns sicher, dass auch andere Gruppen, beispielsweise Ransomware-Betreiber, diese Exploits für ihre Zwecke ausnutzen und auf den Zug aufspringen werden", sagt Matthieu Faou, der die Forschungsarbeiten von ESET zu diesem Thema leitet. Die ESET-Forscher stellten ebenfalls fest, dass einige APT-Gruppen die Schwachstellen bereits ausnutzten, bevor die Patches zur Verfügung gestellt wurden. "Wir können daher ausschließen, dass diese Gruppen einen Exploit durch Reverse Engineering von Microsoft-Updates erstellt haben", fügt Faou hinzu.

Drei schnelle Tipps für Administratoren

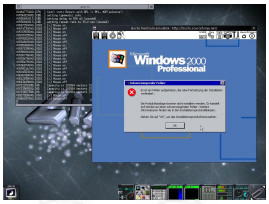
- Exchange-Server sollten so schnell es geht gepatcht werden. Dies gilt auch dann, wenn sie nicht direkt mit dem Internet verbunden sind.
- Administratoren wird geraten, nach Webshells und weiteren bösartigen Aktivitäten zu suchen und diese umgehend zu entfernen.
- Anmeldedaten sollten umgehend geändert werden.

"Der Vorfall ist eine sehr gute Erinnerung daran, dass komplexe Anwendungen wie Microsoft Exchange oder SharePoint nicht zum Internet hin offen sein sollten", rät Matthieu Faou.

APT-Gruppen und ihre Verhaltensmuster

Tick - kompromittierte den Webserver eines Unternehmens mit Sitz in Ostasien, das IT-Dienstleistungen anbietet. Wie im Fall von LuckyMouse und Calypso hatte die Gruppe wahrscheinlich schon vor Veröffentlichung der Patches Zugang zu einem Exploit.

LuckyMouse - infizierte den E-Mail-Server einer Regierungsbehörde im Nahen Osten. Diese APT-Gruppe verfügte wahrscheinlich mindestens einen Tag vor Veröffentlichung der Patches über einen Exploit, als dieser noch ein Zero-Day war.



Calypso - griff die E-Mail-Server von Regierungsstellen im Nahen Osten und in Südamerika an. Die Gruppe hatte wahrscheinlich Zugang zu dem Exploit als Zero-Day. In den folgenden Tagen griffen die Calypso-Betreiber weitere Server von Regierungsstellen und Unternehmen in Afrika, Asien und Europa an.

Websiic - zielte auf sieben E-Mail-Server ab, die Unternehmen (in den Bereichen IT, Telekommunikation und Technik) in Asien und einer staatlichen Einrichtung in Osteuropa gehören.

Winnti Group - kompromittierte die E-Mail-Server eines Ölunternehmens und einer Firma für Baumaschinen in Asien. Die Gruppe hatte wahrscheinlich schon vor Veröffentlichung der Patches Zugang zu einem Exploit.

Tonto Team - attackierte die E-Mail-Server eines Beschaffungsunternehmens und eines auf Softwareentwicklung und Cybersicherheit spezialisierten Beratungsunternehmens, beide mit Sitz in Osteuropa.

ShadowPad activity - infizierte die E-Mail-Server eines Softwareentwicklungsunternehmens mit Sitz in Asien und eines Immobilienunternehmens mit Sitz im Nahen Osten. ESET entdeckte eine Variante der ShadowPad-Backdoor, die von einer unbekannten Gruppe eingeschleust wurde.

"Operation" Cobalt Strike - zielte auf rund 650 Server, hauptsächlich in den USA, Deutschland, Großbritannien und anderen europäischen Ländern, nur wenige Stunden nach Veröffentlichung der Patches.

IIS-Backdoors - ESET beobachtete IIS-Backdoors, die über die bei diesen Kompromittierungen verwendeten Webshells auf vier E-Mail-Servern in Asien und Südamerika installiert wurden. Eine der Backdoors ist öffentlich als Owlproxy bekannt.

Mikroceen - kompromittierte den Exchange-Server eines Versorgungsunternehmens in Zentralasien, einer Region, die typischerweise Ziel dieser Gruppe ist.

DLTMiner - ESET entdeckte den Einsatz von PowerShell-Downloadern auf mehreren E-Mail-Servern, die zuvor über die Exchange-Schwachstellen angegriffen wurden. Die Netzwerkinfrastruktur, die bei diesem Angriff verwendet wurde, steht in Verbindung mit einer zuvor gemeldeten Coin-Mining-Kampagne.

Eine detaillierte Analyse veröffentlichen die IT-Experten auf dem ESET Security Blog: