"Diese Untersuchung erinnert uns daran, dass Patches allein nicht in jedem Fall vor allen Schwachstellen schützen können. Das Festlegen von Beschränkungen, die verhindern, dass ein Benutzer versehentlich ein bösartiges Dokument auslöst, hilft zwar, aber die Leute können immer noch dazu verleitet werden, auf die Schaltfläche 'Inhalt aktivieren' zu klicken.“ (Andrew Brandt, Principal Threat Researcher bei Sophos)

Der 36-Stunden-Exploit – eine Trockenübung?

Sophos-Untersuchung beschreibt, wie Cyberkriminelle einen kritischen Microsoft Office-Patch umgehen: sie passen einen neuartigen Remote-Code-Exploit (RCE) an ein anderes Dateiformat an und verwenden ihn dann nur 36 Stunden lang

Sophos hat heute Details zu einem neuartigen Exploit veröffentlicht, der einen Patch für eine kritische Microsoft Office-Sicherheitslücke (CVE-2021-40444) umgeht. Die Ergebnisse sind in einem neuen SophosLabs Uncut-Artikel mit dem Titel "Attackers test ‘CAB-less 40444’ exploit in a dry run," veröffentlicht. Der Bericht beschreibt, wie die Cyberkriminellen einen öffentlich verfügbaren Proof-of-Concept-Office-Exploit als Waffe nutzten, um die Datenklau-Malware Formbook zu verbreiten. Die Angreifer:innen verbreiteten die Malware dann etwa 36 Stunden lang über Spam-Mails, bevor sie verschwand.

Vom CAB zum "CAB-losen" Exploit. Eine Trockenübung?
Im September 2021 veröffentlichte Microsoft einen Patch, der Cyberkriminelle daran hindert, schädlichen Code auszuführen, der in ein Word-Dokument eingebettet ist, das ein Microsoft Cabinet (CAB)-Archiv herunterlädt, das wiederum eine schädliche ausführbare Datei enthält. Sophos Forscher:innen entdeckten, dass Angreifer den ursprünglichen Exploit überarbeitet haben, indem sie das schädliche Word-Dokument in einem speziell gestalteten RAR-Archiv platzierten. Die neuere, "CAB-lose" Form des Exploits umgeht erfolgreich den ursprünglichen Patch.
Die Daten zeigen, dass der geänderte Exploit etwa 36 Stunden lang in freier Wildbahn genutzt wurde. Laut den Sophos-Expert:innen könnte die begrenzte Lebensdauer des aktualisierten Angriffs bedeuten, dass es sich um ein Trockenübung handelte und die Angriffsmethorde bei zukünftigen Attacken wieder auftreten könnte.

"Theoretisch hätte dieser Angriffsansatz nicht funktionieren dürfen, aber er hat funktioniert", sagt Andrew Brandt, Principal Threat Researcher bei Sophos. "Die Vor-Patch-Versionen des Angriffs beinhalteten schädlichen Code, der in eine Microsoft Cabinet-Datei verpackt war. Als Microsofts Patch diese Lücke schloss, entdeckten Angreifer ein Proof-of-Concept, das zeigte, wie man die Malware in einem anderen komprimierten Dateiformat, einem RAR-Archiv, bündeln kann. RAR-Archive wurden schon früher zur Verbreitung von Schadcode verwendet, aber der hier verwendete Prozess war ungewöhnlich kompliziert. Wahrscheinlich war es nur deshalb erfolgreich, weil der Aufgabenbereich des Patches sehr eng definiert war und weil das WinRAR-Programm, das die Benutzer zum Öffnen des RAR-Archivs benötigen, sehr fehlertolerant ist und sich nicht daran zu stören scheint, wenn das Archiv fehlerhaft ist, beispielsweise weil es manipuliert wurde."

Die Infektionskette
Sophos fand heraus, dass die Angreifer:innen ein ungewöhnliches RAR-Archiv erstellt hatten, bei dem ein PowerShell-Skript dem schädlichen Word-Dokument vorangestellt war, das im Archiv gespeichert war.
Die Angreifer erstellten und verteilten Spam-E-Mails, die diese deformierte RAR-Datei als Attachment enthielten. In den E-Mails wurden die Empfänger:innen aufgefordert, die RAR-Datei zu entpacken, um auf das Word-Dokument zuzugreifen. Das Öffnen des Word-

Dokuments löste einen Prozess aus, der das Front-End-Skript ausführte, was schließlich zu einer Infektion mit der Formbook-Malware führte.

"Diese Untersuchung erinnert uns daran, dass Patches allein nicht in jedem Fall vor allen Schwachstellen schützen können", so Brandt. "Das Festlegen von Beschränkungen, die verhindern, dass ein Benutzer versehentlich ein bösartiges Dokument auslöst, hilft zwar, aber die Leute können immer noch dazu verleitet werden, auf die Schaltfläche 'Inhalt aktivieren' zu klicken. Es ist daher äußerst wichtig, die Mitarbeiter zu schulen und sie daran zu erinnern, dass sie bei per E-Mail verschickten Dokumenten misstrauisch sein sollten. Vor allem, wenn sie in ungewöhnlichen oder ungewohnten komprimierten Dateiformaten von Personen oder Unternehmen kommen, die sie nicht kennen. Im Zweifelsfall sollten sie immer beim Absender oder bei einem IT-Mitarbeiter nachfragen."

Bei der Sicherheitslücke CVE-2021-40444 handelt es sich um eine kritische Schwachstelle für die Remotecodeausführung (RCE), die Kriminelle ausnutzen können, um unbemerkt beliebigen Code oder Befehle auf einem Zielcomputer auszuführen. Microsoft hat im September eine dringende Entschärfung und einen Patch veröffentlicht. Sophos Forscher:innen entdeckten die 36-Stunden-Kampagne mit der neuen Schwachstelle Ende Oktober.
Sophos Endpoint-Produkte erkennen die waffenfähigen Archivdateien, die den "CAB-less - 40444"-Exploit enthalten, als Troj/PSDL-KP

Weitere Informationen finden Sie in dem Artikel auf SophosLabs Uncut.

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de