Pressemeldung / Aktueller Kommentar von SentinelOne vom 8. Juli 2020

Cyber-Angriffe durch Kaperung von E-Mail-Antwortketten: Was ist das und wie kann man sich schützen?

Matthias Canisius, Regional Director Central and Eastern Europe bei SentinelOne

E-Mail-Phishing ist nach wie vor der führende Vektor für Malware-Infektionen in Unternehmen, und Business E-Mail Compromise (BEC) die Ursache Nummer eins für finanzielle Verluste aufgrund von Internet-Kriminalität in Organisationen. Während typische Phishing- und Spearphishing-Angriffe versuchen, den Absender mit einer gefälschten Adresse zu täuschen, wird bei Angriffen über Antwortketten auf raffinierte Art und Weise eine legitime E-Mail-Korrespondenzkette gekapert, um Malware in eine bestehende E-Mail-Konversation einzuschleusen. Ein Beispiel für diese Angriffe ist die Valak-Malware, welche jüngst von SentinelLabs-Forschern analysiert wurde.

Wie funktionieren Angriffe über E-Mail-Antwortketten?
Das Einschleusen von Malware über E-Mail-Antwortketten beginnt mit der Übernahme eines E-Mail-Kontos. Die Angreifer verwenden eine Methode wie Phishing, Brute Force oder Social Engineering, um Zugriff auf ein oder mehrere E-Mail-Konten und beginnen dann damit, Konversationen zu beobachten und auf die richtige Gelegenheit zu warten, um Malware oder bösartige Links an einen oder mehrere Teilnehmer einer laufenden Korrespondenzkette zu schicken.

Diese Technik ist besonders effektiv, da zwischen den Empfängern bereits ein Vertrauensverhältnis aufgebaut wurde. Der Bedrohungsakteur fügt sich weder selbst als neuer Korrespondent ein noch versucht er, die E-Mail-Adresse eines anderen zu fälschen. Vielmehr sendet der Angreifer seine mit Malware versehene Nachricht von dem echten Konto eines der Teilnehmer aus. Da der Angreifer Zugriff auf den gesamten Thread hat, kann er seine böswillige E-Mail auf den Kontext einer laufenden Konversation abstimmen. Zusätzlich zu der Tatsache, dass der Empfänger dem Absender bereits vertraut, erhöht diese Vorgehensweise maßgeblich die Chance ein Opfer dazu zu bewegen, einen bösartigen Anhang zu öffnen oder auf einen gefährlichen Link zu klicken.

Welche Arten von Malware nutzen Antwortketten als Angriffsvektor?
Angriffe auf E-Mail-Antwortketten wurden zum ersten Mal im Jahr 2017 beobachtet. Im Jahr 2018 begannen auch Gozi ISFB/Ursnif Banking-Trojaner-Kampagnen mit dieser Technik, obwohl in einigen Fällen die Korrespondenzkette selbst nur gefälscht wurde, um die Legitimität zu erhöhen; in anderen Fällen kompromittierten die Angreifer legitime Konten und nutzten sie sowohl zur Übernahme bestehender Threads als auch zu Spam-Attacken auf andere Empfänger. Bösartige Anhänge können VBScript und PowerShell über Office-Makros nutzen, um Workloads wie Emotet, Ursnif und andere Loader- oder Banking-Trojaner-Malware zu übertragen.

Massen-Spoofing-E-Mails werden oft mit Betreffzeilen oder Textnachrichten verschickt, die für die meisten Empfänger wenig aussagekräftigen Kontext aufweisen, was sofort Verdacht erregt. Bei E-Mail-Antwortketten-Angriffen können jedoch die üblichen Warnindikatoren fehlen. Angriffe über E-Mail-Antwortketten sind oft sorgfältig ausgearbeitet und weisen keine Sprachfehler auf. Das bedeutet, dass selbst die vorsichtigsten und am besten ausgebildeten Mitarbeiter Gefahr laufen, Opfer dieser Art von Taktik zu werden.

Vier Möglichkeiten zur Prävention von Angriffen per E-Mail-Antwortkette
1. Da Antwortketten-Angriffe auf Konto-Kompromittierungen beruhen, sollte zuallererst sichergestellt werden, dass sich alle Mitarbeiter des Unternehmens die bewährten Sicherheitsverfahren befolgen. Dazu gehören Zwei- oder Mehrfaktor-Authentifizierung, eindeutige Passwörter für jedes Konto und Passwörter, die mindestens 16 Zeichen lang sind.

2. Zweitens sollte die Verwendung von Office-Makros beschränkt oder ganz verboten werden, wo immer dies möglich ist. Obwohl dies nicht die einzigen Mittel sind, mit denen böswillige Anhänge ein Gerät kompromittieren können, bleiben Makros ein üblicher Angriffsvektor.

3. Das Einführen von Security Awareness Trainings kann eine große Hilfe dabei sein, Angestellte im Hinblick auf Gefahren durch Phishing zu schulen. E-Mail-Benutzer müssen ihr Bewusstsein dafür schärfen, wie Phishing-Angriffe funktionieren und wie die Angreifer ihre Techniken weiterentwickeln. Entscheidend ist, dass ihnen beigebracht wird, alle Anfragen zum Öffnen von Anhängen oder zum Anklicken von Links mit einer gewissen Vorsicht zu behandeln, unabhängig von der Quelle.

4. Außerdem – und dieser Punkt ist am wichtigsten – sollte sichergestellt werden, dass alle Endpunkte mit einer modernen, vertrauenswürdigen EDR-Sicherheitslösung geschützt sind, die die Ausführung von in Anhängen oder Links verstecktem bösartigem Code stoppen kann, bevor er Schaden anrichtet. Althergebrachte Antivirus-Lösungen wurden nicht für moderne, dateilose und polymorphe Angriffe gebaut. Eine automatisierte KI-basierte Plattform der nächsten Generation ist das absolute Minimum in der heutigen Cybersicherheits-Bedrohungslandschaft.

Fazit
Angriffe per E-Mail-Antwortkette sind eine weitere Form des Social Engineering, die von Bedrohungsakteuren eingesetzt wird, um ihre Ziele zu erreichen. Anders als in der physischen Welt mit ihren hart kodierten Naturgesetzen gibt es in der Cyberwelt keine Regeln, die nicht durch Manipulation der Hardware, der Software oder des Benutzers geändert werden können. Dies gilt jedoch für Verteidiger ebenso wie für Angreifer. Indem Unternehmen die Kontrolle über alle Aspekte unserer Cyber-Umgebung behalten, können Angriffe abgewehrt werden, bevor sie auftreten oder der Organisation dauerhaften Schaden zufügen. Unternehmen sollten ihre Geräte absichern, ihre Benutzer und Mitarbeiter schulen, so dass die Angreifer es schwerer haben Lücken ausfindig zu machen.

Kontakt
Kafka Kommunikation GmbH & Co.
Dr. Bastian Hallbauer-Beutler
Lukas Reck
Kafka Kommunikation
089 74 74 70 580
sentinelone@kafka-kommunikation.de