Sextortion: Cybererpressung mit angeblich kompromittierenden Videos - Sextortion-Betrug doppelt so wahrscheinlich wie BEC-Angriffe

Cyberkriminelle haben betrügerische Sextortion-E-Mails bisher als grosse Spam-Kampagnen verteilt, jetzt erweitern die Angreifer ihre Taktik: Eine Analyse durch Sicherheitsforscher von Barracuda Networks ergab, dass einer von zehn Spear-Phishing-Attacken ein Sextortion-Angriff war. Damit ist es doppelt so wahrscheinlich, dass Mitarbeiter durch einen gezielten Sextortion-Angriff ins Visier genommen werden als durch Business Email-Compromise (BEC).

Sextortion: Vorgehensweise der Angreifer

Bei einem Sextortion-Angriff geben Cyberkriminelle vor, im Besitz eines kompromittierenden Videos zu sein, das angeblich auf dem Computer des Opfers aufgezeichnet wurde, und drohen, es mit allen Kontakten des Opfers zu teilen ? es sei denn, die Zielperson bezahlt. Typerweise werden Bitcoins verlangt und die Wallet-Details in der Erpressungsnachricht mitgeschickt. Sextortion-Angreifer nutzen bei der Kommunikation E-Mail-Adressen und gegebenenfalls Passwörter, die bei Datenlecks gestohlen wurden. Oftmals fälschen Angreifer auch die E-Mail-Adresse durch Spoofing und geben vor, Zugang zum Konto zu haben.

Sextortion-E-Mails werden in der Regel als Teil grösserer Spam-Kampagnen an Tausende von Zielpersonen gesendet, sodass die meisten durch Spam-Filtern entdeckt werden. Doch Kriminelle nutzen mittlerweile auch Social-Engineering, um traditionelle E-Mail-Sicherheitsgateways zu umgehen. Sextortion-E-Mails, die in Posteingänge gelangen, stammen meist von angesehenen Absendern und IPs. Hacker verwenden hierfür bereits kompromittierte Office 365- oder Gmail-Konten. Zudem enthalten Sextortion-E-Mails in der Regel keine bösartigen Links oder Anhänge, die von herkömmlichen Gateways erkannt werden. Angreifer haben auch begonnen, den Inhalt der E-Mails zu variieren und zu personalisieren, was es für Spamfilter schwierig macht, sie zu stoppen. Sextortion-Scams werden zudem aufgrund ihres vermeintlich peinlichen Inhalts von Opfern oft nicht gemeldet. IT-Teams sind sich dieser Angriffe deshalb häufig nicht bewusst.

Gängige Sextortion Betreffzeilen

Es zeigte sich, dass die Mehrheit der Betreffzeilen in den untersuchten Sextortion-E-Mails eine Form von Sicherheitswarnung enthält. Mehr als ein Drittel fordert eine Passwortänderung. Angreifer geben zudem oft die E-Mail-Adresse oder das Passwort des Opfers in der Betreffzeile an, damit die Zielperson die E-Mail öffnet. Im Folgenden einige Beispiele:

?Â name@emailaddress.com wurde angegriffen. Ã„ndern Sie Ihre Zugangsdaten.
?Â Ihr Konto wurde gehackt, Sie müssen es wieder freischalten.
?Â Ihr Konto wird von einer anderen Person genutzt.
?Â Ã„ndern Sie umgehend Ihr Passwort. Ihr Konto wurde gehackt.

Gelegentlich sind Angreifer auch direkter und verwenden bedrohliche Betreffzeilen:

?Â Du bist mein Opfer.
?Â Hör mir besser zu.
?Â Du hast nicht viel Zeit.
?Â Das ist meine letzte Warnung name@emailadresse.com

Branchen, die am stärksten von Sextortion betroffen sind

Laut der Untersuchung ist der Bildungsbereich am häufigsten von Sextortion-Angriffen betroffen, gefolgt von Regierungsstellen und Unternehmen im Bereich Business Services. Der starke Fokus auf den Bildungsbereich ist ein kalkulierter Zug der Angreifer. Bildungseinrichtungen haben in der Regel eine grosse und junge Benutzerbasis. Diese verfügt meist über weniger Sicherheitsbewusstsein und weiss oft nicht, wo sie sich im Fall eines solchen Angriffs Hilfe suchen kann. Aufgrund mangelnder Erfahrung mit dieser Art Bedrohung besteht ein grösseres Risiko, dass junge Menschen Opfer von Sextortion werden.
Durch einen mehrschichtigen Ansatz aus Technologien, Best Practices und umfangreicher Aufklärung kann so das Risiko durch Sextortion-Angriffe deutlich reduziert werden.