

Die Anatomie einer Phishing-Attacke

Auch wenn die meisten Leute wissen, was Phishing ist, ist nur wenigen klar, wie weit Kriminelle bereit sind zu gehen, um eine Phishing-Attacke zu starten. Cyberkriminelle versenden nicht nur E-Mails mit gefälschten Unternehmenslogos wie LinkedIn oder Facebook, sie untermauern ihre Attacken sorgfältig mit klickfähigen gefälschten Werbeanzeigen, durch Spoofing bekannter Online-Marken und erstellen legitim aussehende Phishing-Websites, um sensible Daten einzuholen, die das ahnungslose Opfer eintippt.

SCHRITT 1

IDENTIFIKATION DES OPFERS

Massen-Phishing-Attacke

- Nicht zielgerichtet, große Gruppe von Opfern.

Gezielte Phishing-Attacke

- Spezielle Gruppe oder bekannte Persönlichkeit.



\$2,3 MRD.

Betrag, den Unternehmen laut eines FBI-Berichts in den vergangenen drei Jahren aufgrund gezielter Spear-Phishing-Angriffe auf CEOs verloren haben.



SCHRITT 2

Markennamen

- Phisher wählt einen Markennamen für die Verteilung der Massen-E-Mail wie LinkedIn, PayPal oder FedEx.
- Unter Verwendung einer neu erstellten Domain oder einer gehackten Website erstellt der Phisher Seiten, die den Internetseiten der bekannten Marke ähneln.



EINRICHTEN DER QUELLE

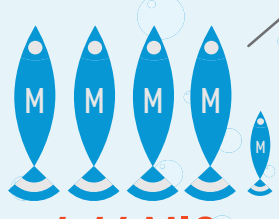
Anzahl der gefälschten Phishing-Seiten, die auf einer einzigen gehackten Website gefunden wurden

Ausgefeilte Inhalte

- Phisher entwickelt eine E-Mail mit legitim aussehendem Inhalt wie rechtliche oder finanzielle Informationen.
- Er spooft die E-Mail-Adresse von jemandem aus dem Zielunternehmen oder einem bekannten Kontakt des anvisierten Opfers.

SCHRITT 3

VERBREITEN DER ANGRIFE



4,44 MIO.

Anzahl der Phishing-URLs, die im 2. Quartal 2016 verteilt wurden

Massenverteilung

- Phisher versendet eine Massen-E-Mail mit Markenlogos/-name und Links zu gefälschten Internetseiten.
- Er platziert Links zu gefälschten Internetseiten in Banner-Anzeigen, auf Social Media oder in Textnachrichten.

Gezielte Verteilung

- Phisher versendet die E-Mail an ein speziell-anvisiertes Opfer oder eine Gruppe.

SCHRITT 4

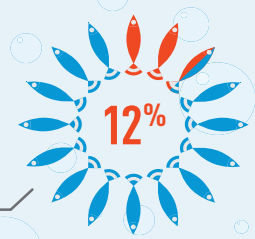
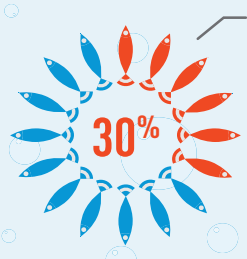
OPFER TÄUSCHEN

Klicken auf gefälschte Links

- Opfer klicken auf einen Link in der E-Mail und geben sensible Zugangsdaten in die gefälschte Internetseite ein.

Antworten direkt auf eine E-Mail-Anfrage

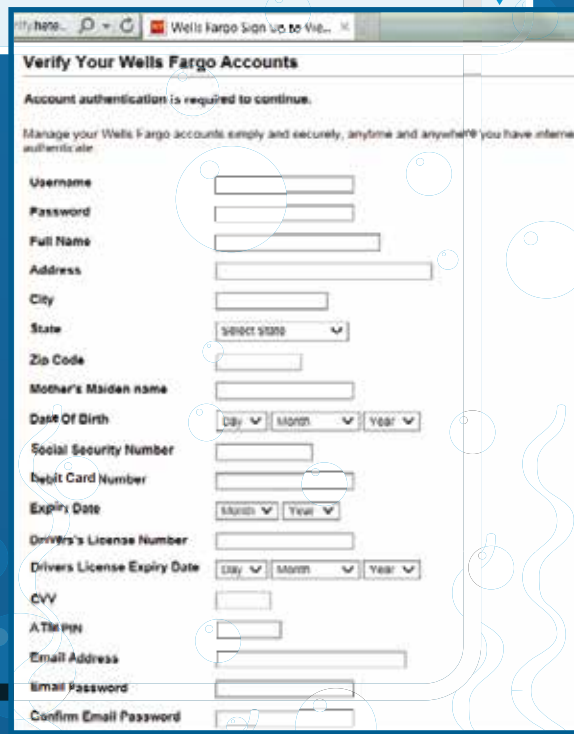
- Opfer antwortet direkt auf eine E-Mail mit den verlangten Informationen wie Zugangsdaten oder Finanzinformationen.



Anteil der Phishing-E-Mails, die von Opfern geöffnet werden*

Anzahl der gefälschten Links, die von Opfern angeklickt werden*

*SQUELLE: 2016 Verizon Untersuchungsbericht zur Datenverletzung



SCHRITT 5

AUSWEITEN / MONETARISIEREN

Entwicklung zusätzlicher Attacken

- Phisher verwendet gestohlene Zugangsdaten für die nächste Phase der Attacke (wie eine APT oder Advanced Persistent Threat).
- Er sammelt zusätzliche E-Mail-Adressen aus gehackten Konten für zukünftige Attacken.

Finanzieller Vorteil

- Phisher verkauft die gestohlenen Zugangsdaten auf dem Schwarzmarkt.
- Phisher stiehlt Geld unter Einsatz der Zugangsdaten für ein Bankkonto, PayPal oder eine gefälschte Überweisung.



Betrag, der von kleinen und mittelständischen Unternehmen bei finanziellen Phishing-Betrügen durch einen vor Kurzem von Interpol verhafteten Cyberkriminellen gestohlen wurde