Phishing-Angriffe steigen durch COVID-19 um 220 Prozent

12.11.2020, 14:15 | IT, New Media & Software

Pressemitteilung von: *F5 Networks*
Presseagentur: *Fink & Fuchs AG*

Phishing and Fraud Report von F5 Labs zeigt: COVID-19-bezogene Betrügereien und immer raffiniertere Attacken verschärfen weltweite Gefahrenlage

München, 12. November 2020 – Die COVID-19-Pandemie führt weiterhin zu deutlich verstärkten Phishing- und Betrugsversuchen, wie eine aktuelle Analyse von F5 Labs belegt. Laut der heute veröffentlichten vierten Ausgabe des Phishing and Fraud Report sind Phishing-Vorfälle auf dem Höhepunkt der weltweiten Pandemie im Vergleich zum Jahresdurchschnitt um 220 Prozent gestiegen. Auf Basis der Daten des Security Operations Center (SOC) von F5 wird die Zahl der Phishing-Vorfälle im Jahr 2020 im Vergleich zum Vorjahr um 15 Prozent zunehmen. Doch diese Zahl könnte sich durch die zweite Welle der Pandemie noch erhöhen.

Die drei Hauptziele für COVID-19-bezogene Phishing-Mails sind demnach betrügerische Spendenaufrufe für angebliche Wohltätigkeitsorganisationen, das Sammeln von Zugangsdaten und die Zustellung von Malware. Zudem erreichte die Zahl der Zertifikate mit den Begriffen „covid“ und „corona“ im März einen Höchststand von 14.940 – ein Anstieg von 1102 Prozent gegenüber dem Vormonat.

„Das Risiko, Opfer von Phishing-Attacken zu werden, ist höher denn je – denn Betrüger verwenden zunehmend digitale Zertifikate, um ihre Websites als echt erscheinen zu lassen“, sagt Roman Borovits, Senior Systems Engineer bei F5. „Die Angreifer springen auch schnell auf emotionale Trends auf, so dass COVID-19 die bereits gefährliche Lage weiter verschlimmert. Leider zeigen unsere Untersuchungen, dass Security-Kontrollen, Nutzerschulungen und das allgemeine Bewusstsein weltweit immer noch zu wünschen übriglassen.“

Neue Methoden

Wie in den vergangenen Jahren stellte F5 Labs erneut fest, dass Betrüger bei den Namen und Adressen ihrer Phishing-Sites immer kreativer werden. Im Jahr 2020 haben bislang 52 Prozent der Phishing-Sites Namen und Identitäten von bekannten Marken in ihren Adressen verwendet. Amazon wurde in der zweiten Hälfte des Jahres 2020 dabei am häufigsten für Angriffe ausgenutzt. Paypal, Apple, WhatsApp, Microsoft Office, Netflix und Instagram gehörten ebenfalls zu den zehn am häufigsten imitierten Marken. Bei der Verfolgung des Diebstahls von Zugangsdaten bis zu deren Verwendung bei aktiven Angriffen ermittelte F5 Labs, dass Kriminelle nach dem Phishing eines Opfers innerhalb von vier Stunden versuchten, gestohlene Passwörter einzusetzen. Einige Angriffe erfolgten sogar in Echtzeit, um die Erfassung von Sicherheitscodes bei Multi-Faktor-Authentifizierung (MFA) zu ermöglichen.

Cyberkriminelle werden zudem skrupelloser beim Kapern seriöser, aber anfälliger URLs. Allein auf WordPress entfielen 20 Prozent der generischen Phishing-URLs im Jahr 2020, drei Jahre zuvor waren es noch 4,7 Prozent. Darüber hinaus sparen Cyberkriminelle zunehmend Kosten, indem sie Gratis-Registrierungsstellen wie Freenom für bestimmte länderspezifische Top-Level-Domains (ccTLDs) wie .tk, .ml, .ga, .cf und .gq, nutzen. So ist .tk heute die fünfthäufigste registrierte Domain der Welt.

Täuschend echt

Im Jahr 2020 intensivierten Phisher auch ihre Bemühungen, betrügerische Seiten so echt wie möglich erscheinen zu lassen. F5 SOC-Statistiken ergaben, dass die meisten Phishing-Websites Verschlüsselung einsetzen. Dabei verwenden 72 Prozent gültige HTTPS-Zertifikate, um die Opfer zu täuschen. Sogar sämtliche Drop Zones – die Ziele der von Malware versandten gestohlenen Daten – nutzen TLS-Verschlüsselung gegenüber 89 Prozent im vergangenen Jahr.

Künftige Bedrohungen

Aktuellen Untersuchungen von Shape Security zufolge, die zum ersten Mal in den Report integriert wurden, zeichnen sich zwei große Phishing-Trends ab. Infolge verbesserter Sicherheitskontrollen und -lösungen für den Bot-Verkehr (Botnet) nutzen Angreifer immer mehr Klickfarmen. Dabei versuchen Dutzende von „Fern-Arbeitern“ systematisch, sich mit kürzlich erlangten Zugangsdaten auf einer Ziel-Website anzumelden. Die Verbindung startet ein Mensch per Standard-Webbrowser, wodurch die Erkennung des Betrugs erschwert wird.

Hier kann selbst eine relativ geringe Prozentzahl von Angriffen schlimme Folgen haben. So analysierte Shape Security beispielsweise 14 Millionen monatliche Anmeldungen bei einem Finanzdienstleister und verzeichnete eine Betrugsrate von 0,4 Prozent. Das entspricht jedoch 56.000 betrügerischen Anmeldeversuchen – und die Zahlen werden weiterhin steigen.

Als zweiten Trend verzeichneten die Forscher von Shape Security einen Anstieg der Echtzeit-Phishing-Proxies (RTPP), die Multi-Faktor-Authentifizierungscodes (MFA) erfassen und verwenden können. Der RTPP agiert als Person-in-the-Middle und fängt die Transaktionen eines Opfers mit einer echten Website ab. Da der Angriff in Echtzeit erfolgt, kann die böswillige Website den Prozess der Erfassung und Wiedergabe von zeitlich begrenzten Authentifizierungen wie MFA-Codes automatisieren. Sie kann sogar Session-Cookies stehlen und wiederverwenden. Zu den kürzlich aktiv genutzten RTTPs gehören Modlishka und Evilginx2.

„Phishing-Angriffe werden so lange erfolgreich sein, wie sich Menschen in irgendeiner Weise psychologisch manipulieren lassen“, so Borovits weiter. „Security-Kontrollen und Webbrowser müssen zwar immer besser in der Lage sein, Benutzer auf betrügerische Websites hinzuweisen. Doch Nutzer und Unternehmen müssen auch kontinuierlich in den neuesten Techniken der Betrüger geschult werden. Dabei sind aktuelle Trends wie COVID-19 in den Mittelpunkt zu stellen.“

Die Studie

Der diesjährige Phishing and Fraud Report untersucht Phishing-Vorfälle basierend auf der Erfahrung des F5 Security Operations Center (SOC) aus den letzten fünf Jahren. Er zeigt detailliert aktive und bestätigte Phishing-Websites, die von OpenText Webroot BrightCloud Intelligence Services bereitgestellt werden. Zudem analysiert er Dark-Web-Marktdaten von Vigilante. Zusammen ergeben diese Informationen ein vollständiges und konsistentes Bild der Welt des Phishings.

Portrait

Über F5
F5 (NASDAQ: FFIV) gibt den weltweit größten Unternehmen, Dienstleistern, Behörden und Verbrauchermarken die Freiheit, jede App sicher, überall und mit Vertrauen bereitzustellen. F5 bietet Cloud- und Sicherheitslösungen, die es Unternehmen ermöglichen, die von ihnen gewählte Infrastruktur zu nutzen, ohne Geschwindigkeit und Kontrolle zu beeinträchtigen. Weitere Informationen finden Sie unter f5.com. Sie können uns auch auf LinkedIn und Facebook besuchen, um weitere Informationen über F5, seine Partner und Technologien zu erhalten.

News-ID: 1107404 • Views: 1017 (Stand: 13.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1107404/Phishing-Angriffe-steigen-durch-COVID-19-um-220-Prozent.html