Rund die Hälfte aller Phishing-Versuche weltweit zielen auf Microsoft-Marken ab

Der Brand Phishing Report von CPR hebt die Marken hervor, die Cyberkriminelle im letzten Quartal am häufigsten nachgeahmt haben, um Menschen dazu zu bringen, ihre persönlichen Daten preiszugeben.

San Carlos, Kalifornien – 25. Juli 2022 – Check Point Research (CPR), die Threat Intelligence-Abteilung von Check Point® Software Technologies Ltd. (NASDAQ: CHKP), einem weltweit führenden Anbieter von Cyber-Sicherheitslösungen, hat seinen Q2 2022 Brand Phishing Report veröffentlicht, der die am häufigsten von Cyberkriminellen imitierten Marken aufzeigt. Der auffälligste Anstieg bei der Ausnützung bekannter Technologieunternehmen war Microsoft, auf das 13 Prozent aller Phishing-Versuche weltweit entfielen, mehr als doppelt so viele wie im vorherigen Quartal. LinkedIn steht mit 45 Prozent der Phishing-Versuche an der Spitze der Liste. Jede zweite Phishing-E-Mail imitiert somit Microsoft-Marken, da Microsoft Eigentümer von LinkedIn ist. CPR vermutet, dass Cyberkriminelle weiterhin Remote Work als attraktiven Trend sehen, um daraus Kapital zu schlagen, da LinkedIn und Microsoft weltweit 58 Prozent der Brand-Phishing-Angriffe ausmachen.

Die zunehmende Nutzung von Microsoft-bezogenen Betrugsversuchen stellt eine Gefahr für Einzelpersonen und Unternehmen dar. Sobald jemand in den Besitz der Anmeldedaten ihres Kontos gelangt ist, hat er Zugriff auf alle dahinter liegenden Anwendungen wie Teams und SharePoint, aber auch das Outlook-E-Mail-Konto.

Brand Phishing-Angriffe nutzen das implizite Vertrauen in eine bekannte Marke aus, indem sie deren Markensymbolik übernehmen und oft eine ähnliche URL verwenden, um Malware zu installieren und sensible Daten zu stehlen. LinkedIn setzte seine Herrschaft als meist imitierte Marke fort, nachdem es im ersten Quartal zum ersten Mal in die Rangliste aufgenommen wurde. Neu in den Top Ten sind die Marken Adidas, Adobe und HSBC.

Top-10-Liste der am häufigsten nachgeahmten Marken im 2. Quartal 2022:

1. LinkedIn (45 %)
2. Microsoft (13 %)
3. DHL (12 %)
4. Amazon (9 %)
5. Apple (3 %)
6. Adidas (2 %)
7. Google (1 %)
8. Netflix (1 %)
9. Adobe (1 %)
10. HSBC (1 %)

Top 3 der am meisten imitierten Industriezweige im 2. Quartal 2022:

1. Soziale Medien
2. Technologie
3. Transport und Logistik

Omer Dembinsky, Data Research Group Manager bei Check Point, zum aktuellen Brand-Phishing-Report: «LinkedIn und Microsoft sind die beiden am häufigsten nachgeahmten Marken. Für uns ist dies ein deutliches Zeichen dafür, dass Cyberkriminelle Remote Work nach wie vor als attraktiven Trend betrachten, den es auszunutzen gilt. Phishing-E-Mails sind ein wichtiges Werkzeug im Arsenal eines jeden Hackers, da sie schnell eingesetzt werden können und mit relativ geringem Aufwand Millionen von Nutzern ansprechen. Sie geben Cyberkriminellen die Möglichkeit, den Ruf vertrauenswürdiger Marken auszunutzen, um den Benutzern ein falsches Gefühl der Sicherheit zu vermitteln, das genutzt werden kann, um persönliche oder geschäftliche Informationen zu stehlen und sich so einen finanziellen Vorteil zu verschaffen. Die Kriminellen werden jede Marke mit ausreichender Reichweite und dem Vertrauen der Verbraucher nutzen. Mit dem erstmaligen Auftauchen von Adidas, Adobe und HSBC in den Top Ten haben die Hacker ihre Aktivitäten also ausgeweitet. Verbraucher müssen deshalb vorsichtig sein und auf verräterische Anzeichen einer gefälschten E-Mail achten, wie schlechte Grammatik, Rechtschreibfehler oder seltsame Domains. Im Zweifelsfall sollten sie die Website der Marke aufsuchen und nicht auf einen Link klicken.»

Mehr dazu lesen Sie im Blog: https://blog.checkpoint.com/2022/07/19/linkedin-still-number-one-brand-to-be-faked-in-phishing-attempts-while-microsoft-surges-up-the-rankings-to-number-two-spot-in-q2-report/

Alle Berichte von Check Point finden Sie unter: https://blog.checkpoint.com/
Alle Berichte des Check Point Research Teams finden Sie unter: https://research.checkpoint.com/

Folgen Sie Check Point Research über:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_

Folgen Sie Check Point auf:
Twitter: https://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: https://blog.checkpoint.com
YouTube: https://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Über Check Point Research
Check Point Research (CPR) bietet führende Cyber-Bedrohungsinformationen für Check Point Software-Kunden und die grössere Intelligenz-Community. Das Forschungsteam sammelt und analysiert globale Cyber-Angriffsdaten, die auf der ThreatCloud gespeichert sind, um Hacker fernzuhalten und gleichzeitig sicherzustellen, dass alle Check Point Produkte mit den neuesten Schutzmassnahmen aktualisiert werden. Das Forschungsteam besteht aus über 100 Analysten und Forschern, die mit anderen Sicherheitsanbietern, der Strafverfolgung und verschiedenen CERTs zusammenarbeiten.

Über Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) ist ein führender Anbieter von Cyber-Sicherheitslösungen für Unternehmen und Regierungen weltweit. Die Lösungen des Check-Point-Infinity-Portfolios schützen Kunden gegen Cyber-Angriffe der 5. Generation mit einer in der Branche führenden Fangrate von Malware, Ransomware und anderen Bedrohungen. Infinity ruht auf drei Kernsäulen, die kompromisslose Sicherheit und Bedrohungsabwehr der Generation V in Konzern-Umgebungen bieten: Check Point Harmony für Remote-Benutzer; Check Point CloudGuard für die automatische Absicherung von Clouds; Check Point Quantum für den Schutz von Netzwerkperimetern und Rechenzentren – alles gesteuert durch das branchenweit umfassendste und intuitivste Unified Security Management. Check Point schützt über 100’000 Unternehmen jeder Grösse in der ganzen Welt.

Pressekontakte:
Check Point Software Technologies
Alvaro Amato
Country Manager Schweiz

Jenni Kommunikation AG
Sylvana Zimmermann
Tel: +41 44 388 60 80
E-Mail: sylvana.zimmermann@jeko.com

