Brand Phishing Report zeigt: Microsoft bleibt Köder Nummer eins

Wie auch im vergangenen Quartal bleibt Microsoft die am häufigsten imitierte Marke von Cyber-Kriminellen, gefolgt vom DHL und Amazon

San Carlos, Kalifornien – 15. Juli 2021 – Die Sicherheitsforscher von Check Point Research (CPR), der Threat-Intelligence-Abteilung von Check Point® Software Technologies Ltd. (NASDAQ: CHKP), haben den Brand Phishing Report mit den am häufigsten imitierten Marken des zweiten Quartals 2021 veröffentlicht. Cyber-Kriminelle nutzen oftmals den Deckmantel grosser Marken- oder Unternehmensnamen, um die eigenen Machenschaften zu verschleiern und ihre Opfer in die Falle zu locken. Auch im zweiten Quartal 2021 bleibt dabei Tech-Gigant Microsoft die Marke, die mit 45 Prozent von den Kriminellen am häufigsten imitiert wird. Die Spitzenplätze werden komplettiert durch den Paketdienst DHL mit 26 Prozent und den Versand-Riesen Amazon mit 11 Prozent.

Die komplette Top 10:

1. **Microsoft** (bezogen auf 45 % aller Marken-Phishing-Versuche weltweit)
2. **DHL** (26 %)
3. **Amazon** (11 %)
4. **Bestbuy** (4 %)
5. **Google** (3 %)
6. **LinkedIn** (3 %)
7. **Dropbox** (1 %)
8. **Chase** (1 %)
9. **Apple** (1 %)
10. **Paypal** (0.5 %)

Bei einem Brand-Phishing-Angriff versuchen die Akteure, die offizielle Website einer bekannten Marke zu imitieren, indem sie einen ähnlichen Domain-Namen oder eine entsprechende URL und ein ähnliches Webseitendesign wie die echte Website verwenden. Der Link zur gefälschten Website kann per E-Mail oder Textnachricht an die Zielpersonen gesendet werden, ein Benutzer kann während des Surfens im Internet umgeleitet werden, oder der Angriff kann von einer betrügerischen mobilen Anwendung ausgelöst werden. Die gefälschte Website enthält oft ein Formular, das dazu dient, die Anmelde-, Zahlungsdaten oder andere persönliche Informationen der Benutzer zu stehlen.

Omer Dembinsky, Data Research Group Manager bei Check Point Software, erläutert: „Cyberkriminelle versuchen immer häufiger, die persönlichen Daten von Menschen zu stehlen, indem sie sich als führende Marken ausgeben. Sie konzentrieren sich dabei stark auf die Bereiche Technologie, Versand und Einzelhandel. Microsoft führte die Liste an, in einem Quartal, in dem der Konzern vor einer neuen russischen Nobelium-Phishing-Kampagne warnte. Im ersten Quartal 2021 wurde der Einzelhandel interessanterweise vom Bankenwesen auf der Liste überholt, aber jetzt hat er seine Position in den Top drei zurückerobert, was möglicherweise auf die Amazon Prime Day-Verkäufe zurückzuführen ist. Tatsächlich wurden im Vorfeld des Amazon Prime Day in Q2 mehr als 2‘300 neue Domains mit ‚Amazon‘ im Namen registriert.

Leider ist das menschliche Element oft nicht in der Lage, falsch geschriebene Domains oder verdächtige Texte und E-Mails zu erkennen, und so geben sich Cyberkriminelle und ihre Machenschaften weiterhin als vertrauenswürdige Marken aus, um Menschen dazu zu bringen, ihre persönlichen Daten preiszugeben. Im 2. Quartal konnten wir ausserdem einen weltweiten Anstieg von Ransomware-Angriffen beobachten, die häufig zunächst über Phishing-E-Mails mit bösartigen Anhängen verbreitet werden. Wie immer empfehlen wir Nutzern, bei der Preisgabe ihrer Daten vorsichtig zu sein und zweimal nachzudenken, bevor sie E-Mail-Anhänge oder Links öffnen, insbesondere E-Mails, die vorgeben, von Unternehmen wie Amazon, Microsoft oder DHL zu stammen, da diese am ehesten nachgeahmt werden."

Weitere Informationen zum Brand Phishing Report finden Sie hier.

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 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

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

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

