Media Alert von Check Point Software zu OpenAI:

Cyberkriminelle nutzen ChatGPT

San Carlos, Kalifornien – 12. Januar 2023 – In einem Bericht der Sicherheitsforscher von Check Point Research (CPR) im Dezember wurde mit ChatGPT ein kompletter Infektionsablauf durchgeführt, von der Erstellung einer überzeugenden Spear-Phishing-E-Mail bis hin zur Ausführung einer Reverse Shell, die Befehle in englischer Sprache annehmen kann. Es stellte sich damals die Frage, ob es sich hierbei nur um eine hypothetische Bedrohung handelt oder ob es bereits Bedrohungsakteure gibt, die OpenAI-Technologien für bösartige Zwecke einsetzen.

Die von CPR durchgeführte Analyse mehrerer grosser Untergrund-Hacking-Communities zeigt, dass es bereits erste Fälle gibt, in denen Cyberkriminelle OpenAI zur Entwicklung bösartiger Tools nutzen. Wie von den Sicherheitsexperten vermutet, zeigten einige der Fälle deutlich, dass viele Cyberkriminelle, die OpenAI nutzen, über keinerlei Entwicklungskenntnisse verfügen. Obwohl die in diesem Bericht vorgestellten Tools recht einfach sind, ist es nur eine Frage der Zeit, bis raffiniertere Bedrohungsakteure die Art und Weise, wie sie KI-basierte Tools zum Schaden einsetzen können, verbessern.

Infostealer, Verschlüsselungs-Tool und Erleichterung von ChatGPT für Cyberbetrug

Am 29. Dezember 2022 erschien in einem beliebten Untergrund-Hacking-Forum ein Thread mit dem Titel «ChatGPT - Benefits of Malware». Der Verfasser des Threads gab bekannt, dass er mit ChatGPT experimentierte, um Malware-Stämme und -Techniken nachzubilden, die in Forschungsveröffentlichungen und Berichten über gängige Malware beschrieben wurden. Als Beispiel gab er den Code eines auf Python basierenden Stealers weiter, der nach gängigen Dateitypen sucht, sie in einen zufälligen Ordner innerhalb des Temp-Ordners kopiert, in ein ZIP-Format packt und sie auf einen fest kodierten FTP-Server hochlädt. Ausserdem postete am 21. Dezember 2022 ein als USDoD bezeichneter Bedrohungsakteur ein Python-Skript, von dem er betonte, dass es das erste Skript sei, das er je erstellt habe. Ein weiteres Beispiel für die Nutzung von ChatGPT für betrügerische Aktivitäten wurde in der Silvesternacht 2022 gepostet und zeigt eine andere Art von cyberkriminellen Aktivitäten. Während sich die ersten beiden Beispiele eher auf die Malware-orientierte Nutzung von ChatGPT konzentrierten, zeigt dieses Beispiel eine Diskussion mit dem Titel «Abusing ChatGPT to create Dark Web Marketplaces scripts».

Fazit

Es ist noch zu früh, um zu entscheiden, ob ChatGPT-Fähigkeiten das neue Lieblingswerkzeug der Teilnehmer im Dark Web werden oder nicht. Die Cyberkriminellen haben jedoch bereits erhebliches Interesse gezeigt und stürzen sich auf diesen neuesten Trend zur Generierung von bösartigem Code. CPR wird diese Aktivitäten im Jahr 2023 weiterverfolgen.

Weitere technische Details der Analyse lesen Sie im Blog: https://research.check-point.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/

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 arbeiten.

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 vier Säulen, 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 namens Check Point Horizon, eine auf Prävention ausgerichtete Suite für Sicherheitslösungen. Check Point schützt über 100’000 Unternehmen jeder Grösse auf 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

