„Fake it ‘til you make it“

Nordkoreanische Hackergruppe NICKEL ALLEY täuscht IT-Experten mit gefälschten Jobs. Das Ziel: Kryptowährungen und Unternehmensspionage

Die nordkoreanische Hackergruppe NICKEL ALLEY setzt ihre perfiden „Contagious Interview“-Kampagnen fort: Mit gefälschten LinkedIn-Unternehmensprofilen, fingierten Jobangeboten und manipulierten GitHub-Repositorien lockt sie gezielt Softwareentwickler in die Falle. Das Ziel: Die Installation des gefährlichen PyLangGhost RAT – einem Remote-Access-Trojaner, der nicht nur Kryptowährungen stiehlt, sondern auch den Weg für Industriespionage und Supply-Chain-Angriffe ebnet.

Die Masche: Fake-Jobs, Fake-Websites, Fake-Code
NICKEL ALLEY geht mit System vor: Die Gruppe erstellt scheinbar seriöse LinkedIn-Seiten für erfundene Unternehmen und ergänzt diese mit GitHub-Accounts, die vermeintlich harmlosen Code hosten. Im Rahmen fingierter Bewerbungsgespräche werden ahnungslose Kandidaten aufgefordert, „technische Aufgaben“ in einer von den Angreifern kontrollierten Weboberfläche zu lösen. Dort wartet die Falle: Ein scheinbarer Fehler auf der Website fordert die Opfer auf, einen lokalen Befehl auszuführen – der in Wahrheit den PyLangGhost RAT herunterlädt und installiert.

Die Websites der Fake-Unternehmen wirken auf den ersten Blick professionell, enthalten aber oft grobe Fehler – wie etwa den unveränderten Platzhaltertext „IT solutions & Corporate template“ im Seitentitel. Die Angreifer nutzen zudem die Taktik des „ClickFix“, bei der Opfer durch vorgetäuschte technische Probleme zur Ausführung schädlicher Befehle verleitet werden.

PyLangGhost RAT: Die unsichtbare Gefahr
Die Angreifer nutzen zudem den vielseitigen PyLangGhost RAT Trojaner. Er ermöglicht den Cyberkriminellen vollständige Kontrolle über infizierte Systeme. Er kann nicht nur Dateien verwalten und Anmeldeinformationen stehlen, sondern hat es gezielt auf Browser-Erweiterungen und Krypto-Wallets abgesehen. NICKEL ALLEY fordert die Opfer explizit auf, den Schadcode auf ihren Firmenrechnern auszuführen, was ein klares Indiz dafür ist, dass es den Angreifern nicht nur um Kryptowährungen, sondern auch um den Zugang zu sensiblen Unternehmensdaten geht.

Empfehlung für Schutzmaßnahmen
Angesichts der zunehmenden Professionalisierung der Angreifer raten Sicherheitsexperten zu vier wichtigen Maßnahmen:

- **Misstrauen bei unaufgeforderten Jobangeboten:** Besonders Entwickler in der Finanz- und Technologiebranche sollten unaufgeforderte Recruiting-Nachrichten auf LinkedIn oder per E-Mail kritisch prüfen.
- **Vorsicht bei technischen Aufgaben in Bewerbungsprozessen:** Die Ausführung von Befehlen, die von unbekannten Websites oder GitHub-Repositorien stammen, sollte ein absolutes No-Go sein.
- **Monitoring von Command-Execution:** IT-Abteilungen sollten ungewöhnliche Befehle, die über Browser-Clipboard-Daten, PowerShell oder aus dem %TEMP%-Verzeichnis gestartet werden, besonders im Auge behalten.
- **Sensibilisierung der Belegschaft:** Unternehmen sollten ihre Mitarbeiter für die Gefahren von Social-Engineering-Angriffen schulen – insbesondere, wenn es um die Ausführung von Code auf Firmenrechnern geht.

Hintergrund: NICKEL ALLEY und die nordkoreanische Cyber-Bedrohung
NICKEL ALLEY agiert im Auftrag der nordkoreanischen Regierung und ist bekannt für ihre ausgeklügelten Angriffe auf die IT-Branche. Die Gruppe nutzt nicht nur gefälschte Jobangebote, sondern kompromittiert auch npm-Paket-Repositorien und etabliert Typosquatting-Pakete, um Entwickler zu täuschen. Die aktuelle Kampagne unterstreicht die wachsende Gefahr durch staatlich gesteuerte Cyberangriffe, die gezielt auf die Software-Lieferkette und die IT-Infrastruktur von Unternehmen abzielen.

Der komplette englischsprachige Blogbeitrag mit zusätzlichen technischen Informationen steht hier.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
press@sophos.com

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de