22.04.2026 – 13:45 Uhr

APT-Report: Staatlich unterstützte Hacker teilen systematisch Netzwerkzugänge

APT-Report: Staatlich unterstützte Hacker teilen systematisch Netzwerkzugänge

Cyberangriffe erreichen durch neue Arbeitsteilung „Maschinengeschwindigkeit“

Wallisellen, 22. April 2026 – TrendAI™, der Enterprise-Cybersecurity-Geschäftsbereich von Trend Micro, veröffentlicht seinen Jahresbericht zu staatlich unterstützten Cyberangriffen (Advanced Persistent Threats / APTs). Die Analyse zeigt eine fundamentale Veränderung in der Bedrohungslandschaft: Angreifergruppen teilen systematisch Zugänge zu kompromittierten Infrastrukturen untereinander, setzen erstmals KI-gestützte Malware ein und dringend immer häufiger über Edge-Geräte in die Netzwerke ihrer Opfer ein.

Der Report „Nation-Aligned APTs in 2025” analysiert die Aktivitäten staatlich unterstützter Hackergruppen aus China, Russland und Nordkorea im Jahr 2025 und identifiziert vier zentrale Entwicklungen, die das strategische Umfeld für Unternehmen und Behörden grundlegend verändern.

Premier Pass-as-a-Service: Arbeitsteilung unter staatlichen Hackern

TrendAI beobachtet erstmals systematisch ein Modell, bei dem APT-Gruppen Zugänge zu kompromittierten Netzwerken wie einen „Priority Pass” untereinander weitergeben. Eine spezialisierte Gruppe verschafft sich initialen Zugang, andere übernehmen anschliessend Spionage, Datendiebstahl oder Sabotage, ohne den Einbruch selbst durchführen zu müssen. Diese Arbeitsteilung beschleunigt Angriffe erheblich und erschwert die Zuordnung zu einzelnen Akteuren. So wurden etwa die China-verbundenen Gruppen Earth Estries (auch bekannt als Salt Typhoon) und Earth Naga in denselben Netzwerksitzungen aktiv, was ein klarer Hinweis auf koordinierte Zusammenarbeit ist.

KI-gestützte Angriffsketten: Von Hilfswerkzeug zu autonomen Agenten

2025 markiert den ersten praktischen Einsatz grosser Sprachmodelle (LLMs) in aktiver Malware. Die Russland-verbundene Gruppe Pawn Storm (APT28) setzte die Malware LAMEHUG ein, die Befehle dynamisch über LLMs generiert. Weitere Gruppen nutzen KI für automatisierte Aufklärung und Zielerkennung. Angreifer setzen KI nicht länger nur als Unterstützung ein, sondern entwickeln autonome „AI Agents“, die sich in Echtzeit an Verteidigungsmassnahmen anpassen können. TrendAI erwartet, dass die nächsten 24 Monate zu einem „Wettlauf um Resilienz auf Maschinengeschwindigkeit“ werden.

„Staatlich unterstützte Cyberaktivitäten werden zunehmend industrialisiert”, sagt Feike Hacquebord, Principal Threat Researcher bei TrendAI. „Bedrohungsgruppen spezialisieren sich auf einzelne Phasen der Angriffskette und teilen anschliessend den Zugang zu kompromittierten Netzwerken, sodass andere Akteure direkt mit Spionage oder Sabotage beginnen können. Wird dieses Modell zusätzlich mit KI-gestützter Aufklärung und der automatisierten Suche nach Schwachstellen kombiniert, verkürzt sich die Zeit für die Durchführung komplexer Kampagnen drastisch.“

Supply Chain und Edge-Dominanz: Angriffe auf Lieferketten und Randinfrastruktur

Die Ausnutzung von Schwachstellen in Edge-Infrastruktur und Angriffe über Entwickler-Ökosysteme (z. B.

gefälschte Job-Angebote der nordkoreanischen Gruppe Void Dokkaebi) hat sich zur bevorzugten Route für langfristige, schwer erkennbare Persistenz entwickelt. Ein Beispiel: Angreifer versuchten, den Server eines taiwanesischen Softwareanbieters, mit potenziellem Zugriff auf die gesamte Lieferkette der Hightech-Fertigung, als Malware-Verteilpunkt zu nutzen.

Geopolitische Kopplung: Cyberangriffe als Begleitung militärischer Konflikte

Cyberoperationen sind heute eng mit geopolitischen Ereignissen und militärischen Operationen verzahnt. Der Report dokumentiert Angriffe auf Logistik- und Infrastrukturketten im Kontext der Unterstützung der Ukraine, Sabotage-Attacken auf Energie- und Verkehrsnetze sowie Spionagekampagnen, die zeitgleich mit diplomatischen Verhandlungen stattfinden. Nordkoreas Drohnenaufklärung in der Ukraine erfolgte parallel zu Cyberkampagnen. Diese Synchronisierung zeigt, dass Cyberraum und physische Kriegsführung zunehmend verschmelzen.

Handlungsempfehlungen für Unternehmen

Der Report zeigt, dass das grösste Risiko nicht in einem sprunghaften Anstieg der Angreifer-Fähigkeiten liegt, sondern in der Normalisierung KI-gestützter Cyberattacken. TrendAI empfiehlt Unternehmen deswegen, APT-Angriffe in ihre Sicherheitsstrategien fest einzubeziehen. Zentral sind:

- Integration von Supply-Chain-Risikomanagement und kontinuierliche Überprüfung von Zulieferern und Dienstleistern
- Etablierung schneller Erkennungs- und Eindämmungsmechanismen für KI-beschleunigte Angriffe
- Verstärkter Informationsaustausch mit Behörden und Branchenpartnern
- Einsatz von „Defensive AI´“ zur Antizipation und Neutralisierung autonomer Bedrohungen
- Regelmässige Incident-Response-Übungen und Red-Team-Tests unter Einbeziehung von APT-Szenarien

Betroffene Branchen

Die häufigsten Ziele staatlich unterstützter Angriffe waren 2025 Regierungsbehörden und Technologieunternehmen, gefolgt von kritischer Infrastruktur (Energie, Transport, Logistik), Fertigung und Finanzdienstleistern.

Weitere Informationen

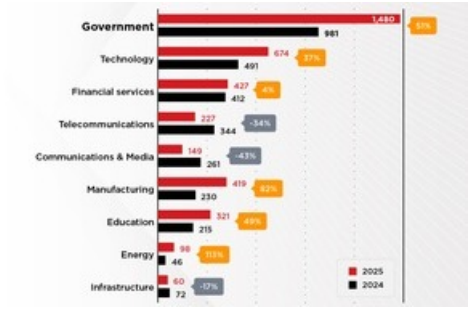
Den vollständigen Report *Nation-Aligned APTs in 2025: AI-Fueled Threats and the Shifting Global Cyber Balance* finden Sie hier: https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/2025-apt-report-staying-ahead-of-the-modern-threat-landscape

Pressestelle TrendAI™
c/o BRAND AFFAIRS AG

Mischa Keller / MSc Business Administration
Partner

Telefon: +41 44 254 80 00
E-Mail: trendmicro-media@brandaffairs.ch
Mühlebachstrasse 8 / 8008 Zürich / Switzerland

Medieninhalte



Diese Meldung kann unter https://www.presseportal.ch/de/pm/100103176/100939626 abgerufen werden.