Achtung, Cyberkriminelle in Aktion: Neuer Lumma Stealer droht!

Eine neue Version des Lumma Stealers bedroht Cyber-Sicherheit. Entdecken Sie die Gefahren, Entwicklungen und Präventionsmaßnahmen.

Deutschland - In den letzten Wochen hat sich die Cybersecurity-Landschaft durch die entdeckte, verbesserte Version der Schadsoftware Lumma Stealer rasant verändert. Sicherheitsforscher von Trend Micro berichten über diese bedrohliche Weiterentwicklung, die nicht nur schwerer zu erkennen ist, sondern auch legitime Domains nutzt, um von ihren wahren Absichten abzulenken. Doch was genau macht Lumma Stealer zu einer der gefürchtetsten Malware der Szene? b2b-cyber-security.de liefert interessante Einblicke in die Anpassungsfähigkeit dieser Bedrohung.

Lumma Stealer ist nicht neu ¿ aktiv ist diese Malware seit mindestens August 2022. Laut check-point.com sind die Täter

hinter Lumma, die unter dem Pseudonym „Shamel“ operieren, bekannt für ihre Professionalität. Lumma wird im Rahmen von Malware-as-a-Service zu Preisen von 250 bis 20.000 US-Dollar angeboten. Diese Preisstruktur macht es auch unerfahrenen Cyberkriminellen möglich, auf leistungsfähige Tools zur Stehlen von Zugangsdaten zuzugreifen.

Technologien und Taktiken der Lumma Stealer

Die neue Version von Lumma bietet raffinierte Methoden, um Sicherheitsprüfungen zu umgehen. Auffällig ist, dass die Malware nicht nur Zugangsdaten, sondern auch Kryptowährungen und andere sensible Informationen stiehlt. Ihre Betreiber verwenden komplexe Taktiken, die oft durch diverse Updates und eine modulare Bauweise unterstützt werden, um sich stetig an Sicherheitsanalysen anzupassen. Verbreitet wird Lumma über kompromittierte Webseiten sowie gefälschte Software-Downloads, eine Methode, die den Kriminellen einen leichten Einstieg ermöglicht. Die Hacker setzen zudem auf Cloudflare, um ihre digitale Spur zu verwischen b2b-cyber-security.de.

Ein weiterer Aspekt, der Lumma Stealer besonders gefährlich macht, sind die vielfältigen Delivery-Methoden. Phishing-Angriffe haben sich in letzter Zeit erheblich weiterentwickelt und werden immer ausgeklügelter. Dabei werden über 57% der erkannten Bedrohungen durch Malware-as-a-Service generiert, wie der Darktrace Threat Report 2024 zeigt. Diese Erkenntnisse verdeutlichen, wie sehr Cyberkriminalität professionalisiert wird cloudcomputing-insider.de.

Die Auswirkungen der Takedown-Operationen

Im Mai 2025 kam es zu einem großen internationalen Einsatz, an dem Europol, das FBI und Microsoft beteiligt waren, um die

Infrastruktur von Lumma zu schwächen. Trotz des Erfolges, bei dem fast 2.500 Domains außer Gefecht gesetzt wurden, konnte die Malware ihre Taktiken schnell anpassen und ihre Operationen fortsetzen. Experten sind sich uneinig über die langfristigen Konsequenzen. Einige glauben, dass die Bedrohung durch Lumma jetzt geringer ist, während andere denken, dass die Crème de la Crème der Cyberkriminalitätum weiterhin am Werk ist und eventuell neue, sogar subtilere Methoden entwickeln könnte. Die steigende Nutzung von MaaS-Tools zeigt jedenfalls, dass die Cyber-Umgebung sich ständig weiterentwickelt check-point.com.

Zusammenfassend zeigt sich, dass die Anpassungsfähigkeit und Hartnäckigkeit der Betreiber von Lumma Stealer eine ernstzunehmende Bedrohung darstellt. Unternehmen sind gefordert, ihre Cyberresilienz zu verbessern und proaktiv gegen solche Gefahren vorzugehen. Angesichts der ständig wachsenden und sich entwickelnden Bedrohungslandschaft ist ein scharfer Blick auf Cybersecurity unerlässlich ¸ da liegt wahrlich was an! b2b-cyber-security.de.

Details	
Ort	Deutschland
Quellen	• b2b-cyber-security.de • www.checkpoint.com • www.cloudcomputing-insider.de