Russische Hacker-Gruppe TrickBot greift mit dateiloser verschleierter Backdoor „PowerTrick“ an

Die Sicherheitsexperten von SentinelLabs warnen vor einem neuem Hacking-Tool der russischen Crimewave-Organisation TrickBot. Wie jüngste Untersuchungen des Forschungslabors von SentinelOne offenbaren, zeichnet sich die PowerShell-basierte Backdoor namens PowerTrick durch eine außerordentliche Verschleierung, Hartnäckigkeit und Auskundschaftungsfähigkeiten aus und richtet sich vor allem gegen erfolgsversprechende Ziele wie Banken und Finanzinstitute.

Anders als beim Einsatz größerer quelloffener Systeme wie etwa PowerShell Empire, ist das PowerTrick-Tool äußerst offensiv und flexibel und ermöglicht es den Angreifern, möglichst lange ungestört zu agieren und sich spontan auszubreiten. Ziel der PowerTrick-Backdoor sei es, auch effektive Sicherheitskontrollen und Beschränkungen zu umgehen, sich denen Gegebenheiten moderner Security-Maßnahmen erfolgreich anzupassen und auf diese Weise auch die am besten abgesicherten und Air Gap-geschützten Netzwerke zu bezwingen.

Dass das Tool dabei so erfolgreich ist und in vielen Fällen unentdeckt bleibt, liegt laut SentinelLabs vor allem daran, dass TrickBot – genau wie andere Angriffswerkzeuge der TrickBot-Gruppe – nur für gezielte Nachbearbeitungszwecke wie z.B. laterale Bewegungen und damit nur für eine kurze Zeitspanne zum Einsatz kommt.

Die Sicherheitsexperten von SentinelLabs haben nun nachgebildete Befehls- und Kontrollfelder entwickelt und stellen diese auch anderen Institutionen zur Verfügung, um Detection-Tests im Zusammenhang mit PowerTrick durchzuführen.

Erst vor kurzem war es den Spezialisten von SentinelLabs gelungen, eine Zusammenarbeit von TrickBot mit der nordkoreanischen Advanced Persistent Threat (APT)-Gruppe Lazarus zu aufzudecken. Bindeglied zwischen den beiden gefährlichen Cybercrime-Akteuren ist demnach das als „Anchor Project“ bekannte TrickBot-Toolset.

Ausführliche Informationen zu PowerTrick finden Sie im neuen SentinelLabs-Blog: https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy-powertrick-backdoor-for-high-value-targets/

Über SentinelOne
SentinelOne ist ein Pionier für autonomen Endpunktschutz und vereint die Prävention, Identifikation, Abwehr und Reaktion auf Angriffe jeglicher Art in einem einzigen Agenten. Dank dem Einsatz von künstlicher Intelligenz können Bedrohungen sowohl on-premises als auch in Cloud-Umgebungen automatisch und in Echtzeit eliminiert werden. Dabei ist die SentinelOne-Plattform ausgesprochen bedienerfreundlich und bietet eine herausragende Sichtbarkeit über alle kritischen Netzwerkvorgänge. Distributor in Deutschland, Österreich und der Schweiz ist Exclusive Networks.

Folgen Sie SentinelOne:
Website: sentinelone.com
Blog: https://www.sentinelone.com/blog/
Twitter: twitter.com/SentinelOneDE
LinkedIn: Linkedin.com/company/SentinelOne
YouTube: SentinelOne on YouTube