SentinelLabs deckt bisher unbekannte Verbindung zwischen TrickBot Anchor und der ATP-Gruppe Lazarus auf

Forscherteam identifiziert eine der raffiniertesten Botnet-Gruppen in der Crimeware-Landschaft

Mountain View / München – 12. Dezember 2019 – **SentinelLabs, das Forschungslabor des Endpunktsicherheitsspezialisten SentinelOne, konnte erstmals eine Zusammenarbeit der Crimeware-Organisation Trickbot mit der nordkoreanischen Advanced Persistent Threat (APT)-Gruppe Lazarus bestätigen. Bindeglied zwischen den beiden gefährlichen Cybercrime-Akteuren ist demnach das als „Anchor Project" bekannte TrickBot-Toolset. Nach Angaben des Forscherteams – geleitet von Security-Experte Vitali Kremez – kommen die Anchor Project-Tools bei der Verbreitung von Malware zum Einsatz, die mit dem nordkoreanischen Regime in Verbindung gebracht werden.**

Anchor Project bietet ein All-in-One-Angriffsframework, das entwickelt wurde, um Unternehmensumgebungen mit benutzerdefinierten und vorhandenen Tools anzugreifen. Während es den meisten nationalstaatlichen Hacker-Gruppen in erster Linie darum geht, einen dauerhaften Zugang für Spionage, Überwachung und Datenexfiltration zu schaffen, ist die Lazarus-Gruppe auch mit der Finanzierung des nordkoreanischen Regimes beauftragt, weshalb sie sich die TrickBot Anchor-Infektionen zunutze machen, um ihre Aktivitäten zu monetarisieren. Die zunehmende Komplexität der Trickbot-Tools und die speziellen Intentionen der Lazarus-Gruppe dürften letztlich der Grund für die Zusammenarbeit beider Akteure sein.

Anchor Project kombiniert eine Vielzahl von Tools, die es Angreifern ermöglichen, sensible Daten zu exfiltrieren und langfristige Persistenz zu schaffen – ein typisches Ziel von Nationalstaaten. Das Toolkit unterstützt ferner die Erstinstallation von Malware, wobei es jegliche Spuren verbirgt und eine Entdeckung der Infektion auf diese Weise erschwert. Damit ist "Anchor Project" sowohl für nationalstaatliche Aktivitäten als auch typische Cyber-Raubüberfälle krimineller Gruppen gleichermaßen attraktiv. Als SentinelLabs bei der Untersuchung des Anchor Projects feststellte, dass Lazarus eine der wenigen Gruppen ist, die sowohl an der Datenexfiltration als auch am finanziellen Gewinn interessiert sind, hielt das Forscherteam sofort Ausschau nach einer möglichen Verbindung zwischen den beiden Gruppen und konnte alsbald feststellen, dass das zuvor mit Lazarus verknüpfte Tool "PowerRatankba" tatsächlich bei einem infiziertem Anchor-Opfer auftauchte.

„Hackergruppen wie TrickBot, die ihre Cybercrime-Dienste unterschiedlichen Zielgruppen für verschiedenste Zwecke bereitstellen, sind immer auf der Suche nach neuen Märkten und Absatzmöglichkeiten, um ihre Malware-Kits zu verkaufen", so Vitali Kremez von SentinelLabs. „Da nationalstaatliche Gruppen aber eher selten monetäre Ziele verfolgen, war es schon ungewöhnlich, dass TrickBot auch in diesem Bereich unterwegs ist. Dass wir TrickBot nun mit Lieferungen in Verbindung bringen konnten, die zuvor APT Malware-Toolkits von Lazarus zugeschrieben wurden, deutet auf eine Quantenverschiebung in der Welt der Cyberkriminalität hin."

Weitere Informationen zu den Forschungsergebnissen rund um das Anchor Project bietet der neue SentinelLabs Threat Research Blog. Die Sicherheitstechnologien von SentinelOne

bieten – anders als viele andere Next-Gen-Antivirus-Lösungen – wirksamen Schutz vor allen Techniken, die im Anchor Project verwendet werden,

Weitere Informationen zu SentinelLabs finden Sie unter https://labs.sentinelone.com/.

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