# Maze-Ransomware-Triple und doch kein Tor: Angreifer trotz modifizierter Attacken erfolglos

*Sophos hat eine Maze-Ransomware-Attacke analysiert, bei der auf drei verschiedene Arten versucht wurde, 15 Millionen Dollar an Lösegeld von einer Organisation zu erbeuten. Alle drei Angriffsversuche schlugen aufgrund geeigneter Maßnahmen fehl. Sie zeigen jedoch die Beharrlichkeit und Anpassungsfähigkeit der Angreifer.*

**Wiesbaden, 21. September 2020 –** Sophos veröffentlichet seinen neuen Report „Maze Attackers Adopt Ragnar Locker Virtual Machine Technique". In diesem Bericht beschreiben die Security-Experten, wie Cyberkriminelle bei einem Angriff auf drei unterschiedliche Arten versuchten, die Ransomware Maze bei ihrem Opfer zu aktivieren. Als Lösegeld verlangten die Gangster 15 Millionen Dollar. Maze ist eine der berüchtigtsten Ransomware-Familien und seit 2019 aktiv. Sie entwickelte sich aus der ChaCha-Ransomware und ist eine der ersten, die Datenverschlüsselung mit Informationsdiebstahl kombinierte.

**Drei Angriffsvarianten auf ein und dasselbe Opfer**
Die Cybergangster hinter Maze sind hartnäckig und versuchen die Ransomware auf unterschiedliche Arten im Unternehmen zu verbreiten. Forensische Untersuchungen ergaben, dass die Angreifer mindestens sechs Tage vor ihrem ersten Versuch, die Ransomware zu aktivieren, in das Netzwerk eingedrungen waren. Während dieser Zeit erkundeten sie die Netzinfrastruktur, starteten reguläre Tools von Drittanbietern, stellten Verbindungen her und leiteten Daten zu einem Cloud-Speicherdienst. Diese Schritte dienten der Vorbereitung für die eigentliche Ransomware.

Nach Aktivierung der Ransomware verlangten die Cyberkriminellen ein Lösegeld in Höhe von 15 Millionen Dollar. Das Opfer zahlte die Summe jedoch nicht und als die Angreifer merkten, dass der erste Angriff fehlgeschlagen war, starteten sie einen zweiten, modifizierten Versuch. Dieser wurde von Security-Lösungen und dem Sophos Managed Threat Response (MTR)-Team, das für die Reaktion auf den Vorfall zuständig war, entdeckt und abgewehrt. Doch die Maze-Angreifer gaben noch nicht auf. Beim dritten Versuch verwendeten sie eine neu konfigurierte Version der Ragnar Locker VM-Technologie unter Einsatz von Windows 7 anstelle der Windows XP-VM. Zudem konzentrierten sie den Angriff nur auf einen Dateiserver. Auch dieser Versuch wurde erkannt und blockiert.

„Die Angriffskette, die vom Sophos MTR-Team nachverfolgt wurde, zeigt die Agilität und Hartnäckigkeit der Angreifer. Sie veranschaulicht auch ihre Fähigkeit, Tools schnell zu ersetzen und neu zu konfigurieren, um für eine weitere Runde in den Ring zurückzukehren", sagt Peter Mackenzie, Incident Response Manager bei Sophos. „Der Einsatz der VM-Technologie von Ragnar Locker mit starkem Footprint und hohem Bedarf an CPU-Leistung könnte ein Zeichen für die wachsende Frustration der Angreifer sein, nachdem die ersten beiden Ransomware-Angriffe fehlgeschlagen sind."

**Tipps zur Abwehr von Cyberattacken**
Zur Abwehr von Cyberattacken, insbesondere von Ransomware, empfehlen die Sophos-Security-Spezialisten eine Verkleinerung der Angriffsfläche. Dies kann durch mehrschichtige und Cloud-basierte Security-Lösungen mit wirksamem Ransomware-Schutz erreicht werden. Zudem sollten Mitarbeiter geschult sein und wissen, worauf sie achten müssen. Auch kann das Einrichten oder beauftragen eines Threat-Hunting-Services entscheidend dazu beitragen, aktive Attacken zu identifizieren.

Der Komplette Report steht zum Download bereit unter:
https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

**Über Sophos**
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 53.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien. Weitere Informationen unter www.sophos.de.

**Pressekontakt:**

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

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