# Billig und plump: Kriminelle setzen auf neue Ransomware „Marke Eigenbau“. Ist das das Ende von professioneller Ransomware-as-a-Service?

*Ransomware-as-a-Service ist seit einem Jahrzehnt ein lukratives Geschäft und fest in den Händen professionell organisierter Gruppen. Doch jetzt können Kriminelle, die keine Lust auf die teuren Bausätze haben, auf eine schnell zusammengeschusterte Ramsch-Ransomware ausweichen. Sophos hat die sogenannte „Junk Gun“-Ransomware und ihre Bedeutung für den Malware-Markt untersucht.*

**Wiesbaden, 23. April 2024.** Sophos veröffentlicht einen neuen Report mit dem Titel ‘Junk Gun‘ Ransomware: Peashooters can still pack a punch. Der Titel erinnert an eine Ära in den USA in den 60er und 70er-Jahren, als mit billigen und teils schlecht funktionieren Waffen, später „Junk Guns“ genannt, der Markt überschwemmt wurde – eine Entwicklung, die sich zurzeit ähnlich in der Cybercrime-Szene wiederholt. Der Report gibt erstmals Einblicke in eine aufstrebende Bedrohung in der Ransomware-Landschaft: Seit Juni 2023 hat das Spezialistenteam Sophos X-Ops 19 „Junk Gun“-Ransomware-Varianten ausgemacht. Billig, selbst produziert und eher plump aufgebaut tauchen die Programme im Darknet auf. Dahinter stecken eher rudimentär ausgebildete Entwickler, die mit einfachen und günstigen Ransomware-Modellen den etablierten Ransomware-as-a-Service-Markt (RaaS) aufrollen wollen.

**Hat das RaaS-Modell ausgedient?**
Anstatt Ransomware als Affiliate-Produkt zu verkaufen oder zu erwerben – wie es im Cybercrimemarkt seit Jahren Standard ist – bauen und verkaufen die Cybercrime-Emporkömmlinge primitive Ransomware-Modelle selbst, zu einer einmaligen Gebühr. Für einige Kriminelle ideal, um damit kleine und mittelständische Unternehmen oder Einzelpersonen anzugreifen.

„Seit einem oder zwei Jahren beobachten wir, dass Ransomware einen gewissen Sättigungsgrad erreicht hat. Es ist immer noch eine der gängigsten und ernsthaftesten Bedrohungen für Unternehmen, aber laut unserem aktuellen Active Adversary Report hat sich die Anzahl der Angriffe auf einem bestimmten Level eingependelt und das RaaS-Geschäft als gängiges Betriebsmodell für die meisten Haupt-Ransomware-Gruppen etabliert. Vor zwei Monaten verschwanden einige der größten Ransomware-Player von der Bildfläche und in der Vergangenheit machten einige der Ransomware-Partner ihrem Ärger über die Profit-Orientierung von RaaS Luft. Nichts in der Cybercrimewelt bleibt wie es ist und vielleicht sind wir gerade Zeitzeugen, wie diese billigen Versionen von Ransomware der nächste Evolutionsschritt sind, besonders für Kriminelle mit wenig Kenntnissen, die eher auf den schnellen Profit statt auf einen ruhmreichen Angriff setzen“, ordnet Christopher Budd, Director Threat Research bei Sophos, ein.

**Ransomware zum einmaligen Schnäppchenpreis**
Sophos listet im Report eine dieser Eigenbau-Varianten im Darknet zum Preis von 375 US-Dollar auf, eindeutig günstiger als einige RaaS-Kits für Partner, die mit mehr als 1.000 US-Dollar zu Buche schlagen. Laut Analyse haben die Cyberkriminellen bereits vier dieser Varianten in Angriffen eingesetzt. Während die Fähigkeiten der Junk-Gun-Ransomware sich stark von den RaaS-Varianten unterscheiden, können jedoch zwei Argumente punkten: die Schadsoftware braucht zum Laufen wenig oder sogar gar keine unterstützende Infrastruktur und die Nutzer sind nicht verpflichtet, ihren Gewinn mit den Entwicklern zu teilen.

**Anzeigen und Tutorials zum Selberbasteln**
Junk-Gun-Ransomware-Diskussionen finden hauptsächlich in Englisch-sprachigen Foren im Darknet statt und richten sich an Kriminelle mit wenig technischen Kenntnissen – ganz im Gegensatz zu den oft russischsprachigen Foren, die von bekannten und gut ausgebildeten Angriffsgruppierungen besucht werden. Diese neuen Varianten eröffnen einen reizvollen Weg für kriminelle Novizen, in die Ransomware-Welt zu starten. Neben Anzeigen für die Ransomware-Schnäppchen gibt es Beiträge zu Tipps und Trick und How-to-Tutorials.

**Angriffe von Junk-Gun-Ransomware laufen womöglich unterm Radar**
„Diese Arten von Ransomware werden keine Millionen-Dollar-Lösegelder wie bei Clop oder Lockbit einfordern, aber getreu dem Motto ‚Masse statt Klasse" können sie recht effektiv bei KMUs sein und das Debüt für eine größeren Verbreitung darstellen. Während das Phänomen der Junk-Gun-Ransomware relativ neu ist, erhielten wir bereits Einblicke in den Ehrgeiz der Erfinder, um dieses Ransomware-Modell weiter zu verbreiten. Und wir haben viele Posts von weiteren Kriminellen gesehen, die ihre eigene Ransomware-Variante kreieren wollen", kommentiert Budd. „Noch beunruhigender ist allerdings, dass diese neue Ransomware-Bedrohung eine ernsthafte Herausforderung für die Verteidigung darstellt: Da Angreifer diese Modelle gegen KMUs einsetzen und die Lösegeldforderungen gering sind, bleiben die meisten Attacken unentdeckt und unveröffentlicht. Das hinterlässt eine Informationslücke für die Verteidiger, die die Sicherheits-Gemeinschaft dann ausfüllen muss."

**Social Media von Sophos für die Presse**
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

**Über Sophos**
Sophos ist ein weltweit führender und innovativer Anbieter fortschrittlicher Lösungen zur Abwehr von Cyberangriffen, darunter Managed Detection and Response (MDR) sowie Incident Response Services. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 600.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr. Die Dienste und Produkte von Sophos sind über die cloudbasierte Management-Konsole Sophos Central verbunden und werden vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen.

Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung. Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.

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