# Sophos untersucht Dharma Ransomware-as-a-Service-Angriffe

*Kleine und mittelständische Unternehmen sind während der globalen COVID-19-Pandemie besonders betroffen*

**Wiesbaden, 13. August 2020 –** Sophos hat heute seinen neuen Report "Color by Numbers: Inside a Dharma Ransomware-as-a-Service (RaaS) Attack" veröffentlicht. Der Report gibt erstmals einen tiefen Einblick in das automatisierte Angriffsskript und das Toolset, das Cyberkriminellen von den Ransomware-Erstellern inklusive der Back-End-Infrastruktur und weiteren schädlichen Tools zur Verfügung gestellt wird. Der Bericht veranschaulicht zudem, wie Dharma im Jahr 2020 kleine und mittlere Unternehmen (KMUs) ins Visier nimmt.

Dharma ist seit 2016 bekannt und ist aufgrund seines dienstleistungsbasierten Massenmarkt-Geschäftsmodells eine der profitabelsten Ransomware-Familien überhaupt. Verschiedene Iterationen seines Quellcodes wurden online veröffentlicht oder zum Verkauf angeboten, so dass heute viele Varianten des Codes existieren.
Laut den Analysen von Sophos sind die Hauptziele der Dharma RaaS-Angriffe kleine und mittelgroße Unternehmen (KMU). 85 Prozent der Angriffe im Jahr 2020 konzentrierten sich auf Tools mit ungeschütztem Zugriff, wie beispielsweise das Remote Desktop Protocol (RDP). Zu diesen Erkenntnissen kam das Ransomware-Recovery-Unternehmen Coveware, das zudem herausfand, dass die Dharma-Lösegeldforderungen mit durchschnittlich 8.620 US-Dollar recht niedrig sind.

„Dharma ist eine Fast-Food-Franchise-Ransomware. Sie ist weit verbreitet und für fast jeden leicht zugänglich", sagt Michael Veit, Security-Spezialist bei Sophos. „Die Dharma Ransomware-as-a-Service-Angebote erweitern den Kreis der Personen, die Lösegeld-Angriffe ausführen können, deutlich. In normalen Zeiten ist dies schon beunruhigend genug. Aber gerade jetzt, wo sich viele Unternehmen der COVID-19-Pandemie anpassen müssen, viele Mitarbeiter remote beziehungsweise im Home-Office arbeiten und das IT-Personal dünn gesät ist, werden die Risiken dieser Angriffe noch größer. Die Notwendigkeit, Mitarbeiter mit Remote-Arbeitsplätzen zu versorgen hat anfällige Infrastrukturen und Endgeräte zur Folge, insbesondere bei kleineren Unternehmen. Die Dringlichkeit der Lage behindert das IT-Personal dabei, Systeme angemessen zu überwachen und zu verwalten."

Laut dem Sophos-Report verlassen sich Dharma-„Kunden" – auch Affiliates genannt –, sobald sie die Tools gekauft und ihr Ziel gefährdet haben, fast ausschließlich auf ein menügesteuertes PowerShell-Skript. Dieses installiert und startet die Komponenten, die zur Verbreitung von der Ransomware im Zielnetzwerk erforderlich sind. Wenn das Master-Skript ausgeführt wird, identifiziert es sich als „Toolbox" und startet den Angriff mit der Meldung „Have fun, bro!".

Der Angriffsprozess stützt sich in hohem Maße auf den Missbrauch von Open-Source-Tools sowie auf Freeware-Versionen kommerzieller Werkzeuge. Die Entschlüsselung ist ein überraschend komplexer zweistufiger Prozess. Betroffene, die sich an Affiliates wenden, um Wiederherstellungsschlüssel zu erhalten, bekommen in der ersten Stufe ein Tool, das Details aller verschlüsselten Dateien extrahiert. Die Affiliates geben diese extrahierten Daten anschließend an ihre Dienstleister weiter, die in der zweiten Stufe einen Entschlüsselungs-Code für die Dateien bereitstellen. Wie effektiv dieses Verfahren bei der tatsächlichen Wiederherstellung von Daten ist, hängt den Nachforschungen zufolge stark von den Fähigkeiten und der Stimmung der Mitgliedsorganisationen ab. Beispielsweise beobachtete Sophos gelegentlich, dass Partner einige der Schlüssel als Druckmittel zurückhielten, um zusätzliche Lösegeldforderungen zu stellen.

„Bei so vielen Lösegeldforderungen in Höhe von mehreren Millionen Dollar, hochkarätigen Zielen und fortgeschrittenen Gegnern wie WastedLocker sind Bedrohungen wie Dharma sehr aktuell. Sie ermöglichen es einer ganzen anderen Gruppe von Cyberkriminellen, mehrere kleinere Ziele zu treffen und so ein Vermögen zu scheffeln, achttausend Dollar auf einmal", sagt Veit.

**Tipps zur Verteidigung**

- Abschalten des Remote-Desktop-Protokoll (RDP), um Cyberkriminellen den Zugang zu Netzwerken zu verwehren. Wenn RDP dringend benötigt wird, sollte es hinter einer VPN-Verbindung stehen.
- Es sollte ein vollständiges Inventar aller im Netzwerk verbundenen Geräte zur Verfügung stehen. Neueste Sicherheits-Updates sollten installiert werden, sobald diese veröffentlicht sind, und zwar auf allen Geräten und Servern im Netzwerk.
- Regelmäßige Backups der wichtigsten und aktuellsten Daten sollten auf einem Offline-Speicher angelegt werden.
- Frühindikatoren für Ransomware-Angreifer sollten beachtet werden, um Ransomware-Attacken zu stoppen.
- Für die Sicherheit existiert kein Patentrezept. Ein mehrschichtiges, tiefgreifendes Sicherheitskonzept für die Verteidigung ist unerlässlich.

Weitere Informationen: SophosLabs Uncut

**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