Ransomware-Gruppen entwickeln Affiliate-Modelle weiter

DragonForce und Anubis führen innovative Ansätze zur Erweiterung ihrer Aktivitäten ein und sehen sich selbst als Kartell.

Trotz erfolgreicher internationaler Strafverfolgungsmaßnahmen gegen prominente Ransomware-Gruppen zeigen Cyberkriminelle weiterhin Widerstandsfähigkeit und Anpassungsfähigkeit. Im Jahr 2025 beobachteten die Forscher der Counter Threat Unit (CTU) von Secureworks, ein Sophos-Unternehmen, dass die Ransomware-Betreiber DragonForce und Anubis neue Modelle einführten, um Affiliates zu gewinnen und Gewinne zu steigern.

DragonForce: Verteiltes Affiliate-Branding-Modell

DragonForce entstand im August 2023 als traditionelles Ransomware-as-a-Service (RaaS)-Modell. Nachdem die Betreiber im Februar 2024 begannen, ihr Angebot in Untergrundforen zu bewerben, stieg die Zahl der Opfer auf der zugehörigen Leak-Seite bis zum 24. März 2025 auf 136. In einem Beitrag vom 19. März 2025 kündigte DragonForce seine Neupositionierung als „Kartell“ an und stellte den Wechsel zu einem verteilten Modell vor, das es sogenannten Affiliates ermöglicht, ihre eigenen „Marken“ zu kreieren (siehe Abbildung 1).

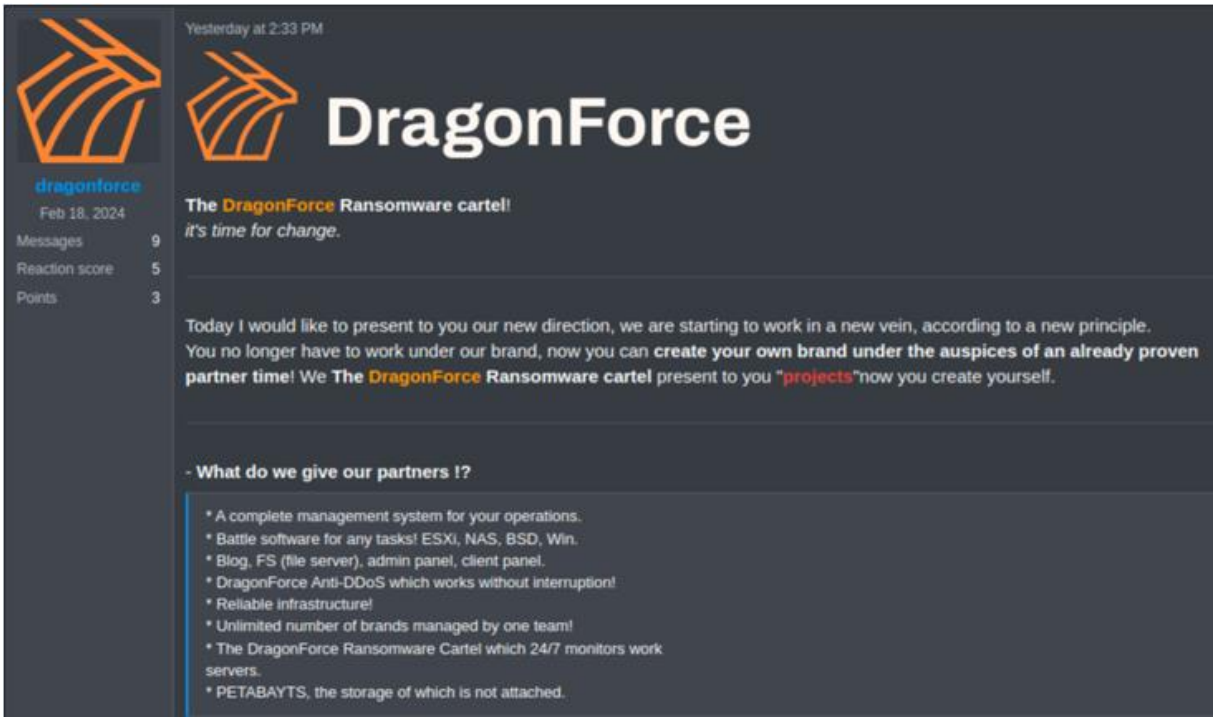

Abbildung 1. Ankündigung von DragonForce über den Wechsel zu einem anpassbaren Partnermodell.

In diesem Modell stellt DragonForce seine Infrastruktur und Werkzeuge bereit, verlangt jedoch nicht, dass Affiliates zwingend deren Ransomware einsetzen. Beworbene Funktionen umfassen Verwaltungs- und Kundenpanels, Verschlüsselungs- und Lösegeldverhandlungs-Tools, ein Dateispeichersystem, eine auf Tor basierende Leak-Seite mit .onion-Domain sowie Supportdienste.

Dieser Ansatz unterscheidet DragonForce von anderen RaaS-Angeboten und könnte eine breitere Affiliate-Basis ansprechen – von technisch weniger versierten Bedrohungsakteuren bis hin zu erfahrenen Kriminellen, die ihre eigene Malware einsetzen möchten, ohne selbst

Infrastruktur aufbauen zu müssen. Gleichzeitig birgt das geteilte System Risiken: Wird ein Affiliate kompromittiert, könnten auch Informationen anderer Affiliates offengelegt werden.

Anubis: Drei Erpressungsoptionen
Die Betreiber von Anubis nutzen eine andere Taktik zur Anwerbung von Affiliates. Dieses im Februar 2025 erstmals in Untergrundforen beworbene Erpressungsschema bietet drei Modi:

- **RaaS** – traditionelle Dateiverschlüsselung mit 80 Prozent Lösegeldanteil für Affiliates
- **Daten-Lösegeld** – Erpressung nur durch Datendiebstahl mit 60 Prozent Lösegeldanteil für Affiliates
- **Monetarisierung von Zugriffen** – Unterstützung bei der Erpressung bereits kompromittierter Opfer mit 50 Prozent Lösegeldanteil für Affiliates

Bei der Option „Daten-Lösegeld“ wird ein detaillierter „Untersuchungsartikel“ auf einer passwortgeschützten Tor-Website veröffentlicht, der die Analyse sensibler Daten des Opfers enthält. Das Opfer erhält Zugriff und einen Link zur Lösegeldverhandlung. Falls keine Zahlung erfolgt, wird mit der Veröffentlichung des Artikels auf der Anubis-Leak-Seite gedroht. Zusätzlich wird der Name des Opfers über ein X-Konto (ehemals Twitter) veröffentlicht. Die Täter drohen darüber hinaus, die Kunden des Opfers über den Vorfall zu informieren.

Anubis geht sogar noch weiter. Laut Werbung sollen Vorfälle an folgende Behörden gemeldet werden:

- Das britische **Information Commissioner’s Office (ICO)** (Datenschutz und Informationsrechte)
- Das **US-Gesundheitsministerium (HHS)**
- Die **Europäische Datenschutzbehörde (EDPB)**

Diese Eskalationstaktik ist zwar recht selten, hat jedoch Präzedenzfälle: Im November 2023 meldete die Bedrohungsgruppe GOLD BLAZER einen ALPHV-Angriff (auch als BlackCat bekannt) an die US-Börsenaufsicht SEC, nachdem das Opfer das Lösegeld nicht bezahlt hatte. Den Forschern sind keine weiteren Fälle bekannt, in denen andere Gruppen Vorfälle an Regulierungsbehörden gemeldet hätten.

Die Option „Monetarisierung von Zugriffen“ konzentriert sich auf Aktivitäten nach der Kompromittierung. Affiliates erhalten eine Analyse der Opferdaten zur Unterstützung bei der Lösegeldforderung (siehe Abbildung 2).

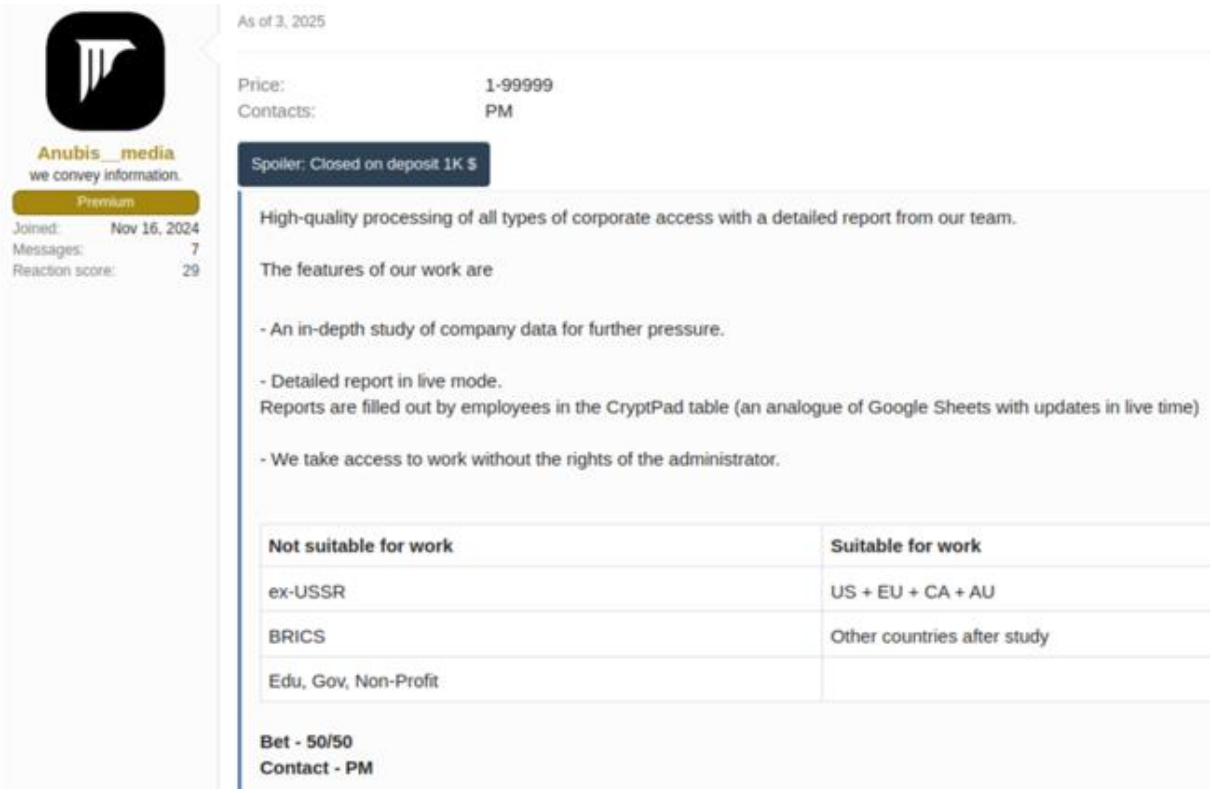

Abbildung 2. Werbung für den Anubis-Dienst „accesses monetization“.

In der Werbung wird angegeben, dass bestimmte Regionen und Sektoren ausgeschlossen sind. Wie viele Ransomware-Gruppen vermeidet Anubis Angriffe auf Organisationen in post-sowjetischen Staaten sowie auf Mitglieder der BRICS-Staaten (Brasilien, Russland, Indien, China, Südafrika, Ägypten, Äthiopien, Indonesien, Iran und Vereinigte Arabische Emirate). Auch Bildungseinrichtungen, Regierungsstellen und gemeinnützige Organisationen sind ausgenommen – Gesundheitsorganisationen werden allerdings nicht erwähnt, was sie als lohnendes Ziel erscheinen lässt.

Ausblick

Der 2024 State of the Threat Report von Secureworks, ein Sophos-Unternehmen, bestätigt, dass Ransomware weiterhin eine erhebliche Bedrohung für Organisationen darstellt. Auch wenn die Strafverfolgung erfolgreich Operationen stört, entstehen neue Modelle. Berichte von Dritten zeigen zwar, dass Lösegeldzahlungen rückläufig sind, was sich durch eine steigende Anzahl von Opfern auf Leak-Seiten belegen lässt. Da Cyberkriminelle jedoch finanzielle Gewinne anstreben, experimentieren sie mit innovativen Modellen und aggressiveren Taktiken.

Obwohl jede Organisation individuell abwägen muss, ob sie ein Lösegeld zahlt, garantiert eine Zahlung weder die Rückgabe von Daten noch den Schutz vor öffentlicher Bloßstellung. Ein proaktiver präventiver Ansatz kann effektiver sein. Die Cybersecurity-Experten empfehlen Unternehmen, regelmäßig Patches für Geräte mit Internetzugang zu installieren, eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA) als Teil einer Zugangskontrollrichtlinie zu implementieren, robuste Backups zu erstellen und ihr Netzwerk und ihre Endpunkte auf bösartige Aktivitäten zu überwachen. Darüber hinaus sollten Unternehmen einen Reaktionsplan für Vorfälle entwickeln und regelmäßig testen, um Ransomware-Aktivitäten schnell zu beheben zu können.

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

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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