Organisierte Cyberkriminalität: Die bösen Neun anstatt des dreckigen Dutzends

Im alten Katz- und Mausspiel zwischen Cybersecurity und Cyberkriminalität kommt es darauf an, wem ein kluger Schachzug einfällt, dem der andere folgen muss. Im Fall der „Bösen Neune“ sind es die Cyberkriminellen, die sich eine gute Idee aus der IT beziehungsweise Security zunutze machen und unverhohlen auf den Zug aufspringen, um ihre Machenschaften massiv auszuweiten: Cybercrime as a Service.

Während des Jahres 2022 haben die großen Cybercrime-Gruppen ein ganzes Service-Ökosystem für Kriminelle mit entsprechendem Geldbeutel und weitere Handlanger aufgebaut, das nach heutigem Kenntnisstand und zum Leidwesen der Opfer gut organisiert ist. Mehr noch: der As-a-Service-Ansatz in der Cyberkriminalität hat dazu geführt, dass vergleichsweise unerfahrene Cyberganoven über wirkungsvolle Angriffs-Tools verfügen, die sie ohne diese Services nicht bedienen könnten.

Die „Bösen Neune“ des Jahres 2022 sind:

Access-as-a-Service: Der Zugang zu kompromittierten Konten und Systemen wird einzeln oder in großen Mengen über Untergrunddienste verkauft, einschließlich Zugangsdaten für das Remote-Desktop-Protokoll (RDP) und VPN, Konten, Datenbanken, Web-Shells und ausnutzbaren Sicherheitslücken.

Malware Distribution/Spreading-as-a-Service: Dies bedeutet die Verbreitung von Malware in dedizierten Regionen oder Sektoren oder auch auf breiter Ebene. In den Angeboten, die das Sophos X-Ops Team für derartige Dienste gesehen hat, ist nicht in jedem Fall klar, welche Strategie zum Einsatz kam. Aber zu den möglichen Angriffsvektoren gehören Watering-Hole-Angriffe, die Ausnutzung von Schwachstellen oder die Kombination mit AaaS-Angeboten (Access-as-a-Service).

Phishing-as-a-Service: Hier handelt es sich um Bedrohungsakteure, die einen End-to-End-Service für Phishing-Kampagnen anbieten, einschließlich geklonter Webeseiten, Hosting, präparierter E-Mails zur Umgehung von Spam-Filtern sowie Panels zur Überwachung der Ergebnisse.

OPSEC-as-a-Service: Diesen Dienst hat Sophos X-Ops in einem kriminellen Forum zusammen mit Cobalt Strike gesehen. Der Verkäufer bietet den Interessenten an, sie mit einem OPSEC-Service (Operations Security) zu unterstützen, der entweder einmalig eingerichtet oder monatlich abonniert werden kann und dazu dient, Cobalt-Strike-Infektionen zu verbergen und das Risiko der Entdeckung und Zuordnung zu minimieren.

Crypting-as-a-Service: Dieser Cybercrime-Service ist ein gängiger Dienst, der in vielen Foren zum Kauf angeboten wird. Er verschlüsselt die Malware so, dass sie nicht erkannt wird – insbesondere nicht von Windows Defender und SmartScreen und in geringerem Maße auch nicht von traditionellen Antivirusprodukten. Der Dienst wurde beispielsweise für die einmalige Nutzung zu einem Preis von 75 US-Dollar oder für 300 US-Dollar für ein einmonatiges Abonnement angeboten, das eine unbegrenzte Nutzung des Dienstes beinhaltete.

Scamming-as-a-Service: Das Sophos X-Ops Team sah einige Beispiele für "Scamming-Kits", insbesondere im Zusammenhang mit Kryptowährungsbetrug, die in kriminellen Foren beworben wurden. Es war nicht immer klar, was genau verkauft wurde, aber eine Anzeige bot

eine fertige "Elon Musk Giveaway BTC Scampage" für 450 $ an. Dies ist eine beliebte Betrugsmasche auf Twitter und hat sogar in einem gefälschten Video die Runde gemacht.

Vishing-as-a-Service: Dies ist ein Voice-Phishing-Dienst ("Vishing"), bei dem ein Bedrohungsakteur ein Sprachsystem zur Entgegennahme von Anrufen zu mieten anbietet. Und das zusammen mit einem "KI-System", so dass der Mieter sich dafür entscheiden kann, dass seine Opfer mit einem Bot statt mit einem Menschen sprechen.

Spamming-as-a-Service: Spamming-as-a-Service ist ein alter Favorit, aber in kriminellen Foren immer noch weit verbreitet. Er bietet Massen-Spamming über eine Vielzahl von Mechanismen, einschließlich SMS und E-Mail. In einigen Fällen bieten die Cyberkriminellen an, die gesamte Infrastruktur von Grund auf neu einzurichten; in anderen Fällen betreiben sie die Infrastruktur und nutzen sie zum Versenden benutzerdefinierter Spam-Nachrichten.

Scanning-as-a-Service: Dieser kriminelle Service bietet den Nutzern Zugang zu einer Reihe legitimer kommerzieller Tools – darunter Metasploit, Invikti, Burp Suite, Cobalt Strike und Brute Ratel –, um Schwachstellen zu finden (und vermutlich auszunutzen). Die gesamte Infrastruktur wird nach Untersuchungen von Sophos X-Ops offenbar vom Verkäufer erstellt und gewartet, der an anderer Stelle behauptet, dass "Sie“ nur auf das Scan-Ergebnis im Postfach warten müssen".

Das wars? Eher nicht!
Für 2023 und darüber hinaus ist damit zu rechnen, dass die Professionalisierung der Cyberkriminalität weiter fortschreitet. Die Industrialisierung von Ransomware hat bereits die Entwicklung von Ransomware-"Affiliates" zu professionelleren, auf die Ausbeutung spezialisierten Unternehmen ermöglicht. Durch den Einsatz professioneller und offensiver Cybercrime-as-a-Services sind die Cyberkriminellen nicht mehr eindeutig mit spezifischen Ransomware-Operationen, staatlich organisierter Spionage oder anderen spezifischen Motiven in Verbindung zu bringen. Die professionalisierten Gruppen haben sich darauf spezialisiert, allen motivierten Akteuren, die bereit sind zu zahlen, Zugang zu kriminellen Handlungen zu verschaffen.
Diese Gruppen haben in vielerlei Hinsicht die Geschäftsmodelle der Cloud- und Web-Service-Branche nachgeahmt. Ähnlich wie IT-Abteilungen in Unternehmen das "As-a-Service"-Modell für immer mehr Operationen übernommen haben, kann heute fast jeder Aspekt der Cyberkriminalität ebenfalls an "Crime-as-a-Service"-Anbieter ausgelagert werden. Tendenz steigend.

Mehr dazu im Sophos Threat Report 2023.

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/
Twitter: @sophos_info

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