Sophos Threat Report 2023:
Die Kommerzialisierung der Cyberkriminalität

Cyberkriminalität floriert als Geschäftsmodell, Ransomware ist Innovationstreiber und gestohlene Zugangsdaten fungieren als Cash-Cow

Wiesbaden, 17. November 2022 Sophos hat heute seinen Threat Report 2023 veröffentlicht. Der Report beschreibt unter anderem einen neuen Grad der Kommerzialisierung innerhalb der Cyberkriminalität, durch den zunehmend niedrigschwellige Einstiegsangebote für potenzielle Angreifer verfügbar sind: Fast alle Szenarien sind käuflich. Ein boomender Cybercrime-as-a-Service-Markt steht einer kriminellen Käuferschaft offen, die von technisch hoch versiert bis völlig unwissend reicht.

Hier die Themen des aktuellen Sophos Threat Reports in der Übersicht:

- Die "Cybercrime-as-a-Service"-Industrie hat eine neue Stufe der Kommerzialisierung erreicht, die viele Einstiegshürden für Interessenten von Cyberkriminalität beseitigt und bei entsprechender Liquidität fortschrittliche Bedrohungstaktiken in die Hände fast aller Kriminellen legt.
- Ransomware ist nach wie vor eine der größten Bedrohungen für Unternehmen, wobei sich Cyberkriminelle auf die "Innovation" ihrer Angriffstaktiken und Erpressungstechniken konzentrieren.
- Der Krieg in der Ukraine hat zu einer Umstrukturierung der kriminellen Allianzen und einer Neuordnung der Ransomware-Landschaft geführt.
- Cyberkriminelle setzen verstärkt auf den Diebstahl von Anmeldeinformationen, um gezielt Netzwerke zu infiltrieren.
- Bedrohungsakteure greifen weiterhin auf legitime Tools und ausführbare Dateien zurück, um Angriffe auszuführen, und bringen zunehmend ihre eigenen Schwachstellen ein.
- Mobile Geräte stehen im Mittelpunkt neuartiger Cyberkriminalität - sowohl Android- als auch iOS-Geräte sind betroffen.
- Eine der ältesten Formen der Kryptokriminalität - das Kryptomining - ist rückläufig, da Monero (eine der beliebtesten Währungen) an Wert verliert. Kryptobetrug hingegen ist in Südasien bereits eine wachsende Industrie.

Ransomware als Markttreiber und Blaupause für andere Malware-Gattungen
Kriminelle Untergrundmarktplätze wie Genesis ermöglichen seit langem den Kauf von Malware und Malware-Implementierungsdiensten ("Malware-as-a-Service") sowie den Verkauf gestohlener Zugangsdaten und anderer Daten in großen Mengen. In den letzten zehn Jahren hat sich mit der zunehmenden Beliebtheit von Ransomware eine ganze "Ransomware-as-a-Service"-Wirtschaft herausgebildet. Cyberkriminelle haben sich ein Beispiel am Erfolg dieser Infrastruktur genommen und ziehen nach. Jetzt, im Jahr 2022, hat sich das "As-a-Service"-Modell daher massiv ausgeweitet, und fast jeder Aspekt der Cyberkriminalität – von der Erstinfektion bis hin zu Möglichkeiten, die Entdeckung zu vermeiden – ist käuflich zu erwerben.

Zudem arbeiten auch cyberkriminelle Marktplätze immer mehr wie normale Unternehmen. Einige Marktplätze haben eigene Seiten für Stellengesuche und die Rekrutierung von Mitarbeitenden eingerichtet, wo die Arbeitssuchenden ihre Fähigkeiten und Qualifikationen in Kurzform angeben.

„Cyberkriminelle verkaufen heute Tools und Fähigkeiten, die sich früher nur in den Händen einiger der raffiniertesten Angreifer befanden als Dienstleistungen an andere Akteure," sagt Sean Gallagher, Principal Threat Researcher bei Sophos. „Im vergangenen Jahr haben wir zum Beispiel Anzeigen für OPSEC-as-a-Service gesehen, in denen die Verkäufer anboten, Angreifern dabei zu helfen, Cobalt Strike-Infektionen zu verstecken, und wir haben Scanning-a-Service gesehen, der Käufern Zugang zu legitimen kommerziellen Tools wie Metasploit gibt, damit sie Schwachstellen finden und dann ausnutzen können. Die Kommerzialisierung fast aller Komponenten der Cyberkriminalität eröffnet Angreifern aller Art neue Möglichkeiten."

Verschiebung cyberkrimineller Partnerschaften durch Ukraine-Krieg
Traditionell sind, bzw. waren Ukrainer und Russen seit langem Partner im Cybercrime-Geschäft – vor allem, wenn es um Ransomware geht. Mit Ausbruch des Krieges sind jedoch einige Banden auseinandergebrochen. Dies führte unter anderem zu den Conti Leaks – der Veröffentlichung der Chat-Protokolle dieser Ransomware-Gruppe. Ein anderer Twitter-Account behauptete auch, die angeblichen Mitglieder von Trickbot, Conti, Mazo, Diavol, Ryuk und Wizard Spiders ausgespäht zu haben. Insgesamt ist die internationale Arbeit gegen Ransomware dennoch nicht einfacher geworden. So haben sich Ransomware-Gruppen neuformiert, und es scheint unter anderem, dass ein neues "REvil" aufgetaucht ist.

Ransomware bleibt beliebt und innovativ
Ransomware ist trotz des Ausbaus der Infrastruktur für Cyberkriminalität weiterhin sehr beliebt und äußerst profitabel. Im vergangenen Jahr haben die Betreiber von Ransomware daran gearbeitet, ihren potenziellen Angriffsdienst zu erweitern, indem sie andere Plattformen als Windows ins Visier genommen und neue Sprachen wie Rust und Go eingeführt haben, um nicht entdeckt zu werden. Einige Gruppen, allen voran Lockbit 3.0, haben ihre Operationen diversifiziert und "innovativere" Methoden zur Erpressung von Opfern entwickelt.

"Wenn wir über die zunehmende Raffinesse des kriminellen Untergrunds sprechen, gilt dies auch für die Welt der Ransomware. Lockbit 3.0 zum Beispiel bietet jetzt Bug-Bounty-Programme für seine Malware an und holt sich von der kriminellen Gemeinschaft Ideen zur Verbesserung seiner Operationen. Andere Gruppen sind zu einem "Abonnementmodell" für den Zugriff auf ihre erbeuteten Daten übergegangen, und wieder andere versteigern sie. Ransomware ist in erster Linie ein Geschäft geworden", so Gallagher.

Heiße Ware Zugangsdaten
Die sich entwickelnde Ökonomie des Untergrunds hat nicht nur Anreize für das Wachstum von Ransomware und der "As-a-Service"-Industrie geschaffen, sondern auch die Nachfrage nach gestohlenen Zugangsdaten erhöht. Mit der Ausweitung von Webdiensten können verschiedene Arten von Anmeldeinformationen, insbesondere Cookies, auf vielfältige Weise genutzt werden, um in Netzwerken tiefer Fuß zu fassen und sogar Multifaktorauthentifizierung zu umgehen. Der Diebstahl von Anmeldedaten ist auch eine der einfachsten Möglichkeiten für Kriminelle, Zugang zu Untergrundmärkten zu erhalten und ihre "Karriere" zu beginnen.

Über den Sophos Threat Report 2023
Der Sophos Threat Report 2023 beruht auf Untersuchungen und Erkenntnissen von Sophos X-Ops, einer neuen, funktionsübergreifenden Einheit, die drei etablierte Teams von Cybersecurity-Experten bei Sophos (SophosLabs, Sophos SecOps und Sophos AI) miteinander verbindet. Sophos X-Ops umfasst mehr als 500 Cybersecurity-Experten weltweit, die in der Lage sind, ein vollständiges, multidisziplinäres Bild einer zunehmend komplexen Bedrohungslandschaft zu zeichnen. Wenn Sie mehr über die täglichen Cyberattacken und TTPs erfahren möchten, folgen Sie Sophos X-Ops auf Twitter und abonnieren Sie aktuelle Artikel und Reports zu Bedrohungsforschung und Sicherheitsoperationen von den vordersten Frontlinien der Cybersicherheit.

Den gesamten Report finden Sie hier: https://www.sophos.com/en-us/content/security-threat-report

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

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. 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 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.
Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und 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