„Das Endziel ist immer klar: Geld“

John Shier, Field CTO Commercial bei Sophos beschreibt die aktuelle Gefahrenlage für die Cybersicherheit, benennt einige Methoden und gibt einen Ausblick auf ein potenzielles künftiges Angriffsziel.

Von John Shier, Field CTO Commercial bei Sophos

Cyberkriminalität ist ein Business. Es unterliegt Trends, greift aktuelle Entwicklungen auf und ist permanent im Wandel. So ist der Ein- und Ausblick denn auch immer nur eine Momentaufnahme – mit oft Klassikern, manchmal Retro-Techniken aber auch bedenklichen Tendenzen.

Ein Trend: Übernahme anfälliger signierter Treiber und Taktiken staatlicher Gruppen
Die Wiederverwendung bestehender Angriffstechniken und das Aufkommen neuer Angriffe sind in der Bedrohungslandschaft üblich. Cyberkriminelle verwenden oft erfolgreiche Tools und Techniken weiter und werden dies so lange tun, bis sie nicht mehr funktionieren.

Einige ändern und passen ihre Tools und Techniken an, um sie an neuen Zielen auszurichten oder ähnliche Schwachstellen auf neue Weise auszunutzen. Mit der technologischen Entwicklung entstehen jedoch auch neue Angriffsmethoden, und Angreifer suchen ständig nach neuen Wegen, um Sicherheitsmaßnahmen zu umgehen. Angesichts immer besserer Schutzmöglichkeiten haben wir beobachtet, dass Cyberkriminelle anfällige signierte Treiber übernehmen, um Endpoint Detection and Response (EDR)-Tools zu umgehen. Wir beobachten auch, dass Cyberkriminelle nationalstaatlichen Gruppen nacheifern, indem sie deren Tools und Taktiken in ihre Angriffspläne integrieren.

Egal, welche Methode die Cybergangster anwenden, das Ziel ist immer Geld
Der bevorzugte Angriff variiert dabei von Cyberkriminellen zu Cyberkriminellen und hängt weitgehend von ihren Motiven, Fähigkeiten und der Möglichkeit ab, ihre Angriffe zu Geld zu machen. Die Motive und Know-how von Initial Access Brokers (IABs) beispielsweise konzentrieren sich darauf, im Netzwerk eines Unternehmens Fuß zu fassen und diesen Zugang an andere Cyberkriminelle zu verkaufen. Ransomware-Banden sind darauf spezialisiert, hochwertige Ziele wie Server zu verschlüsseln und in vielen Fällen auch Daten zu stehlen. Einige Cyberkriminelle sind Experten im Ausnutzen von Sicherheitslücken. Welcher Angriff auch immer bevorzugt wird, das Endziel ist klar: Geld.

Die meistwiederholten Attacken sind diejenigen, die den besten Erfolg versprechen. Bislang bestehen sie aus einer Ausnutzung von Schwachstellen und Phishing. Diese beiden Angriffsmethoden ermöglichen die meisten Netzwerkverletzungen, die oft zu der gängigsten Bedrohung führen: Ransomware.

Ransomware ist nach wie vor die meistverbreitete Bedrohung für Unternehmen
Viele große und kleine Unternehmen aus den unterschiedlichsten Branchen werden täglich Opfer von Ransomware. So wurden beispielsweise allein im März 459 Ransomware-Angriffe gemeldet. Fast ein Drittel dieser Angriffe war auf eine Zero-Day-Schwachstelle imGoAnywhere MFT-Tool für die sichere Dateiübertragung zurückzuführen, die angeblich von der Cl0p-Ransomware-Bande ausgenutzt wurde, um innerhalb von 10 Tagen Daten von vermeintlich 130 Opfern zu stehlen. Eine weitere Zero-Day-Schwachstelle in einem ähnlichen Softwareprodukt, MOVEit Transfer, wird derzeit aktiv von Cyberkriminellen ausgenutzt, wobei viele bekannte Unternehmen betroffen sind.

Es ist wichtig sich darüber im Klaren zu sein, dass Ransomware stets die letzte Stufe eines erfolgreichen Angriffs ist, zu dem auch Informationsdiebstahl, Downloader-Trojaner, Cryptominers und viele andere Bedrohungen gehören.

Lieferketten sind vermutlich ein kommendes Angriffsziel
Was die kommenden Monate angeht, können wir vermutlich von vermehrten Angriffen auf die Lieferkette ausgehen. Diese Attacken scheinen auf dem Vormarsch zu sein. Kompromittierungen der Lieferkette sind für Cyberkriminelle sehr attraktiv, da sie ihnen Zugang zu mehreren Opfern auf einmal verschaffen können. Solange die Cyberkriminellen hiermit Geld erbeuten können, werden diese Angriffe für sie effektiv sein und weitergehen. Unternehmen sollten daher nicht nur sicherstellen, dass sie gegen direkte Angriffe gewappnet, sondern auch in der Lage sind, Angriffe von vertrauenswürdigen Partnern abzuwehren.

Robuste Sicherheitspraktiken sind nötig
Da sich die Angriffsfläche immer weiter vergrößert, ist es für Einzelpersonen, Organisationen und Regierungen wichtig, wachsam zu bleiben, robuste Sicherheitspraktiken zu implementieren und in Bedrohungsdaten, proaktive Überwachung und Reaktionsmöglichkeiten auf Vorfälle zu investieren. Regelmäßige Sicherheitsbeurteilungen, Patch-Management, Schulungen von Mitarbeitenden und Partnerschaften mit Cybersicherheitsfachleuten sind entscheidend, um neuen Bedrohungen im sich ständig verändernden Cyberspace einen Schritt voraus zu sein.

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