„Gelächter im Dunkel“*: Absurde Geschichten aus der Cybercrime-Welt und was man daraus lernen kann

Von einem Ransomware-Angriff mit fünffacher Verschlüsselung über Cyberkriminelle der Kategorie Erbsenzähler bis hin zu, dreisten „Sicherheitsberichte“ – Sophos X-Ops blickt zurück auf einige der skurrilsten Vorfälle der letzten Jahre – und die wichtigsten Lehren, die sich daraus ziehen lassen.

Cybersicherheit ist normalerweise eine ernste Sache und zwar aus gutem Grund. Schließlich existieren sehr reale Risiken für Opfer von Cyberkriminalität: finanzielle Verluste, Reputationsschäden, Betriebsstörungen sowie psychisches Leid. Aber gelegentlich stößt Sophos X-Ops auf Bedrohungsakteure, die dieses Muster durchbrechen – sei es durch pure Dreistigkeit, echten Witz oder völlige Unfähigkeit.

Hier nun einige der skurrilsten Beispiele aus der Arbeit des Incident-Response-Teams und seinen Ausflügen ins Dark Web. Bei allem Kopfschütteln – es lässt sich aus jedem Fall etwas lernen.

Fall 1: Die Verschlüsselung: Extended Version
Bei einem Angriff, den Sophos X-Ops in seinem Whitepaper „Multiple Attackers“ untersucht hat, wurde ein Unternehmen von drei separaten und höchstwahrscheinlich auch unabhängig durchgeführten Ransomware-Angriffen getroffen, zwei davon innerhalb von zwei Stunden. Am Ende kamen die Ransomware Black Cat, LockBit und Hive darin vor, und das betroffene Unternehmen musste alle Angriffe nacheinander abarbeiten, um ihre Daten wieder zu erlangen, zum Teil mit Geld und auf jeden Fall mit sehr viel Aufwand.

Merke: Ein Cyberkrimineller kommt immer seltener allein
Zwar ein extremes Beispiel, aber da das Ransomware-Ökosystem immer effektiver und organisierter wird, konkurrieren die Angreifer um Ziele und stoßen dabei manchmal auf dieselbe angreifbare Organisation. Verschärft wird dies durch bestimmte Merkmale des Cybercrime-Geschäfts, wie IABs (Initial Access Broker), die Zugänge weiterverkaufen (wie es hier möglicherweise der Fall war), und Ransomware-Leak-Seiten, die Daten bereitstellen, die andere Angreifer später als Waffen einsetzen können.
Hier gibt es weitere Einblicke über verfeindete Ransomware-Gruppen, ihr Interesse an Allianzen, einen praktischen Leitfaden zur Prävention und ein Whitepaper für tiefere Einblicke in diese spezielle Bedrohungslandschaft.

Fall 2: Betrüger, die die Betrüger betrügen, die sie betrogen haben
Immer wieder beschäftigten sich die Sophos-Analysten mit einer faszinierenden Nische des Cybercrime-Ökosystems: Bedrohungsakteure, die andere Bedrohungsakteure ins Visier nehmen, sei es aus verletzten Eitelkeiten, Hahnenkampfgehabe oder einmal mehr den Streit ums liebe Geld (hier ein aktuelles Beispiel an Kleingeistigkeit in 2025).

Merke: Mit Kriminellen ist nicht gut Kirschen essen
Fühlen sich die Cyberkriminellen selbst auf den Schlips getreten, vergessen sie jegliche Vorsichtsmaßnahmen. Für Ermittler ergibt sich daraus eine reichhaltige Informationsquelle, schließlich sehen es die Kriminellen gar nicht ein, übers Ohr gehauen zu werden und wenden sich in den Marktplätzen und Foren an die „Schlichtungsstellen“. Die Sophos-Experten fanden so unter anderem Kryptowährungsadressen, Benutzernamen, Transaktions-IDs, E-Mail-Adressen, IP-Adressen, Namen von Opfern, Quellcode und Screenshots von Desktops.

Fall 3: One Hat, Two Hat, Black Cat, Blue Hat? – über illegale Pentester
Sophos hat in früheren Untersuchungen festgestellt, dass sich einige Ransomware-Gruppen gerne als „Pentester“ bezeichnen, um sich eine ungerechtfertigte Legitimität zu verleihen – einige bieten ihren Opfern sogar „Sicherheitsberichte“ an (natürlich erst nach Erhalt der Zahlung). Diese sind aber meistens so voller Rechtschreib- und Grammatikfehler sowie Obszönitäten, dass hier kaum ein Gut-aufgehoben-Gefühl aufkommt.

Merke: Ransomware-Gruppen sind keine wohlwollendenSicherheitsexperten
Wie Sophos X-Ops in einem Artikel über die Beziehung zwischen Ransomware-Gruppen und den Medien festgestellte, wird Ransomware zunehmend professionalisiert und kommerzialisiert. Ein Symptom dafür ist, dass Ransomware-Gruppen versuchen, sich als legitime Sicherheitsexperten und -unternehmen darzustellen, indem sie „Pressemitteilungen“ und „Sicherheitsberichte“ veröffentlichen.

Fall 4: Eiscreme-Brandstiftung, russische Sträflinge als externe Mitarbeiter, E-Liquids an Schüler – Cyberkriminelle sehen überall (kriminelles) Potential
Cyberkriminelle stellen alles Mögliche mit ihren unrechtmäßig erworbenen Gewinnen an: Die Bandbreite ist unerschöpflich und lässt zumindest an Kreativität nichts vermissen. Hier einige der bizarrsten Überlegungen:

Auf die zunächst harmlose Frage eines Nutzers in einem russischsprachigen Cybercrime-Forum, ob es möglich wäre, mit 200.000 Rubel (etwa 2.400 US-Dollar) einen Eisstand zu eröffnen, eskalierten die Vorschläge schließlich in Brandstiftung – mit Anleitung und Materialliste.

Der Vorschlag in Foren, Softwareentwicklung, Hardwareherstellung und Cybersicherheit an russische Gefängnisinsassen auszulagern, hatte auch seine Fürsprecher (Entwicklung einfacher Malware könnte gelingen), wurde dann aber nicht weiterverfolgt.

Ein Bedrohungsakteur teilte Details zu einem fragwürdigen Geschäftsmodell – dem Verkauf von E-Liquids an Schulkinder. Er hatte allerdings nicht mit der elterlichen Fürsorge einiger Hacker gerechnet:, O-Ton: „Ich lese das als Elternteil ... hast du verdammt noch mal keine Kinder?, „HINTERLASS DEINE ADRESSE ... WIR KOMMEN JETZT, WO IMMER DU AUCH BIST“ und so weiter.

Merke: Mit der reinen Cyberattacke ist die kriminelle Energie noch nicht verpufft
Die Sicherheitsbranche behandelt Cyberkriminalität oft als isoliertes Phänomen und konzentriert sich auf Kill Chain, Bedrohungsinformationen und Abwehrmaßnahmen. Ermittlungen nach dem Motto „Dem Geld auf der Spur“ werden zwangsläufig komplexer und aufwändiger. Der Aufwand lohnt sich allerdings, da die Art und Weise, wie Cyberkriminelle ihre Gewinne einsetzen und investieren, zusätzliche Informationsmöglichkeiten in Bezug auf Zuordnung, Motivation, Verbindungen und mehr eröffnen kann.

Fazit:
Wie die obigen Beispiele zeigen, schrecken Angreifer – insbesondere weniger erfahrene – nicht vor Experimenten zurück. Viele ihrer Ideen stellen zwar keine wirkliche Bedrohung dar, doch das heißt nicht, dass unerfahrene Cyberkriminelle nicht trotzdem Schaden anrichten können. Letztendlich ist es egal, ob Ransomware-Gruppen und ihre Verbündeten über besondere Fähigkeiten verfügen oder weniger versiert sind, jeder Angriff kann erhebliche Auswirkungen auf ein Opfer haben. Daher sollten Netzwerkverteidiger die Werkzeuge sowie die Taktiken, Techniken und Verfahren (TTPs) berücksichtigen, die alle Ransomware-Gruppen und ihre Verbündeten im Kontext der in ihren Organisationen vorhandenen Technologieinfrastrukturen einsetzen könnten und entsprechende, koordinierte Abwehrmaßnahmen einrichten, die Technologie und menschliche Expertise kombinieren.

* Vladimir Nabokov entspinnt in seinem bekannten Unterhaltungsroman „Laughter in the Dark“ aus den Zwanzigern für seinen Helden eine tragische Geschichte mit vielen Verwirrungen und groteskem Finale.

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