Keine Solidarität unter Kriminellen: Wie sich Ransomware-Gruppen gegenseitig bekämpfen.

Eine Ransomware-Attacke genügt den meisten Unternehmen bereits als Belastungsgrenze. Aber zwei auf einmal sind ein Apokalypse-Szenario, wenn auch für Sicherheitsprofis durchaus spannend. Sophos hat den seltenen Fall genauer untersucht, der gleichzeitig ein Aufeinandertreffen von modernen und traditionellen Ransomware-Taktiken ist.

Sophos veröffentlicht seine Forschungsergebnisse zu einem zweifachen Ransomware-Angriff, bei dem ein Erpresserschreiben von den Operateuren der Karma-Ransomware 24 Stunden später durch die Conti-Gruppe verschlüsselt wurde. Conti, eine weitere Ransomware-Gemeinschaft, agierte zur selben Zeit im befallenen Netzwerk.

Die Sophos Analysten zeichnen den dualen Angriff detailliert in ihrem Bericht nach und erklären, wie sich beide Akteure Zugang via ungepatchtem Microsoft Exchange Server zum Netzwerk verschafften. Danach aber nutzten sie unterschiedliche Taktiken, um ihre Attacken auszuführen. Hier die genaue Analyse: Conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/.

Sean Gallagher, Senior Threat Researcher bei Sophos, erklärt, wie sich Karma und Conti verhielten: „Opfer einer zweifachen Ransomware-Attacke zu werden, ist für jede Organisation ein Alptraum-Szenario. Insgesamt lässt sich eine Periode von vier Tagen ausmachen, in der Conti- und Karma-Angreifer simultan im anvisierten Netzwerk agierten: sie bewegten sich umeinander, machten Downloads, führten Skripte aus, installierten Cobalt Strike und sammelten und exfiltrierten Daten.
Die Karma-Akteure rollten die letzte Phase ihres Angriffs als erste aus und hinterließen eine Erpressernotiz auf den Computern, die eine Bitcoin-Zahlung forderte. Als Ausgleich würden die gestohlenen Daten nicht veröffentlicht. Dann schlug Conti zu und verschlüsselte die Zieldateien mit einer eher traditionellen Ransomware-Methode – mit dabei ironischerweise auch der Karma Erpresserbrief.
Wir sehen in letzter Zeit immer mehr Fälle, in denen sich Hackergruppen, die die gleiche Ransomware für ihre Attacken nutzen, zusammentun und ProxyShell-Exploits ausnutzten, um das Zielnetzwerk zu infiltrieren. Es gibt auch Beispiele verschiedener Akteure, die die gleiche Schwachstelle ausnutzten, um sich Zugang zu ihrem Opfer zu verschaffen. Der jetzige Fall, bei dem zwei völlig unabhängige Ransomware-Gruppen zeitgleich ein Ziel attackierten zeigt, wie überlaufen und konkurrierend die Ransomware-Landschaft geworden ist.“

Die duale Attacke – eine zeitliche Abfolge

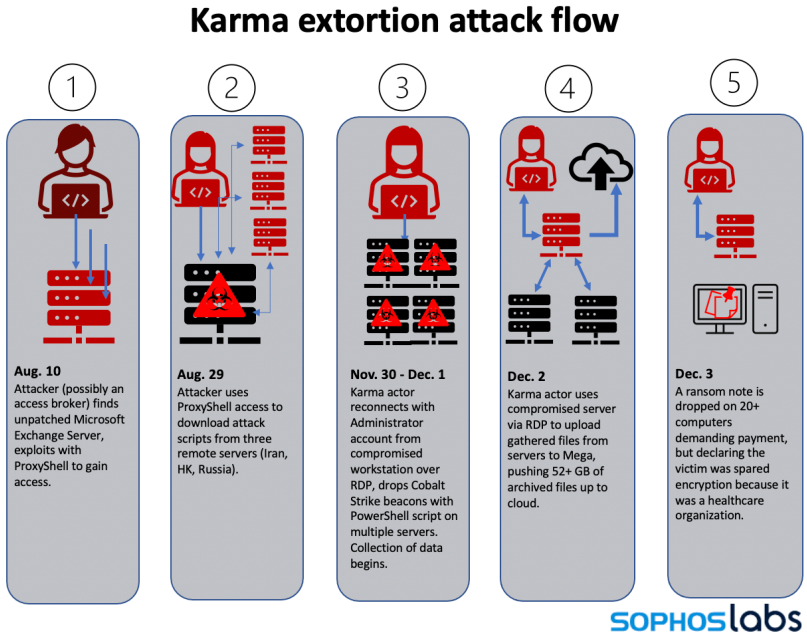
10. August 2021
Die Sophos Analysten gehen davon aus, dass an diesem Tag die Attacke gestartet wurde. Die Kriminellen, möglicherweise initiiert durch Access Broker, die als eine Art Makler im Cybercrime-Ökosystem fungieren und gestohlene Zugänge zu Systemen verkaufen, nutzen eine ProxyShell-Schwachstelle, um sich Zugang zum Netzwerk zu verschaffen und sichern sich auf dem kompromittierten Server einen Stützpunkt.

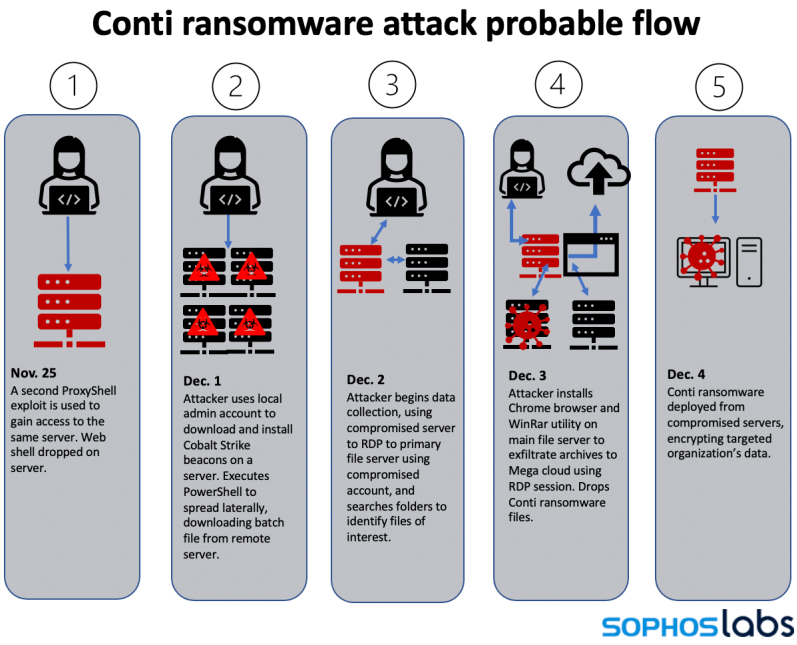
30. November 2021
Die Untersuchung offenbart, dass fast vier Monate verstrichen, bevor Karma am 30. November 2021 auftauchte und mehr als 52 GB an Daten in die Cloud exfiltrierte.

3. Dezember 2021
An diesem Datum finden gleich drei Aktionen statt:

- Die Karma-Angreifer hinterlassen eine Erpressernotiz auf 20 Computern mit der Forderung nach Lösegeld, sonst würden sie die Daten nicht entschlüsseln.
- Conti operierte derweil still im Hintergrund und exfiltrierte Informationen.
- Für Hilfe gegen die Karma-Attacke holte sich das Opfer das Sophos Incident Response Team an Bord.

4. Dezember 2021
Conti rollt seine Ransomware aus. Das Sophos-Team verfolgte in den forensischen Untersuchungen den Start der Conti-Attacke auf eine andere ProxyShell-Schwachstelle, die am 25. November 2021 eingesetzt wurde.





Gallagher empfiehlt als Schutzvor solchen Angriffen die Kombination von Technologie und menschlicher Expertise: „Ob der anfängliche Access Broker den Zugang an zwei verschiedene Ransomware-Gruppen verkauft hat, oder ob der vulnerable Exchange Server nur ein unglückliches Ziel für multiple Ransomware-Angreifer war, bleibt ungewiss. Fakt ist, dass eine zweifache Ransomware-Attacke möglich war. Dies ist ein schlagkräftiges Argument dafür, bekannte Schwachstellen sofort zu patchen und auf ein kommunizierendes IT-Security-System zu setzen, das Angreifer in jeder Phase ihrer Attackenkette identifizieren und blockieren kann. In einem weiteren Schritt kann die proaktive, Menschen-geführte Bedrohungssuche jegliches verdächtige Verhalten genauestens untersuchen. Dazu gehören etwa unerwartete Remote-Logins oder der Gebrauch legitimer Werkzeuge über ihr normales Muster hinaus – all diese Situationen können frühe Anzeichen für eine unmittelbar bevorstehende Ransomware-Attacke sein."

Weitere Informationen zum Conti und Karma Angriff auf den Gesundheitsdienstleister gibt es hier: http://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/

Auch Sicherheitsunternehmen werden attackiert

Letzte Woche hat ein ukrainischer Sicherheitsforscher Chat-Protokolle und Dateien der Conti-Gruppe von mehreren Jahren veröffentlicht. In diesen Protokollen wird erwähnt, wie die Conti-Gruppe auch versucht hat, Lizenzen von Sophos Intercept X zu erwerben, und dabei gescheitert ist. Dem Chat zufolge taten sie dies, um ihre neueste Malware zu testen und herauszufinden, ob sie von Sophos-Produkten erkannt werden würde. Dies ist eine gängige Praxis der Cyberkriminellen und daher sind bei Sophos diverse Präventionsmaßnahmen aktiv. Aus den Chat-Protokollen geht hervor, dass die Versuche von Conti, Sophos-Produkte zu umgehen, erfolglos waren und dass sie daraufhin eine Testversion aktivierten, um im nächsten Schritt eine Lizenz zu erwerben. Ziel von Conti war es, die Sophos Lösung für ihr kriminelles Handeln zu studieren. Beim Versuch des Lizenzerwerbs wurde das fiktive Unternehmen DocSoft mit angeblichem Sitz in Kiew, Ukraine, von den Sophos Sicherheitsmechanismen erkannt. Nachdem der Partner vor Ort gemeinsam mit Sophos eine Videokonferenz vorschlug, um eventuelle Missverständnisse auszuschließen, wurde die Transaktion von der Conti-Gruppe abgebrochen.
Unter diesem Link wird das Vorgehen detailliert beschrieben:
https://news.sophos.com/en-us/2022/03/04/countermeasures-and-observability-key-to-defending-against-attackers-trying-to-buy-security-products/

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