Fin6 – Wie eine Hackergruppe operiert

Von Frank Kölmel

Kreditkartendaten stehen schon lange im Fokus von Cyberkriminellen. Eine Hackergruppe namens Fin6 ist auf mobile Kartenterminals in Hotels, Gastronomie und Einzelhandel spezialisiert. Wie die Hacker dabei vorgehen und welche Mengen an Kartendaten von ihnen zum Verkauf angeboten werden, beschreibt Frank Kölmel. Damit könnte die Gruppe rund 400 Millionen US-Dollar eingenommen haben. Red.

Ein beliebtes Ziel von Cyberangriffen sind ec- und Kreditkartenterminals, denn mit diesen Daten lässt sich leicht viel Geld verdienen. Die Hackergruppierung Fin6 hat sich auf Kartenterminals spezialisiert – angefangen mit dem Ausspionieren der Daten in PoS-Terminals bis hin zum Verkauf der gestohlenen Kartendaten auf dem digitalen Schwarzmarkt. Fin6 konzentriert sich dabei vor allem auf mobile Kartenterminals in Hotels, Gastronomiebetrieben und dem Einzelhandel. Die Daten werden einzig und allein zu dem Zweck entwendet, sie zu verkaufen und damit Geld zu machen.

1. Schritt: Der Klau der Zahlungskartendaten. Diese werden direkt am PoS-System entwendet, indem die Gruppierung entweder im Vorfeld eingekaufte und eingetauschte Anmeldedaten für den Zugang benutzt oder über die bereits installierte Malware Grabnew auf das Terminal des Opfers zugreift. Wie die Malware ursprünglich ihren Weg auf das System gelangt, lässt sich nicht eindeutig nachvollziehen.

2. Schritt: Fin6 installiert eine eigene PoS-Malware, die von Fire Eye als Trinity bezeichnet wird. Dazu verwendet die Gruppe mindestens zwei Downloader (namens Hardtack und Shipbread), um sich damit einen Backdoor-Zugang zu den kompromittierten Systemen zu verschaffen. Diese Tools nehmen Verbindung zu den externen Command-and-Control-Servern der Gruppe auf, um Shellcode herunterzuladen und auszuführen. Nachdem der Backdoor-Zugang gesichert ist, verschafft sich Fin6 über den Windows Credential Editor weitestgehende Zugriffsrechte auf das befallene System. Über Metasploits PsExec NTDSGRAB-Modul gelangt die Gruppe an eine Kopie der Active-Directory-Datensätze, aus denen sie Passwort-Hashes herausziehen kann, die sie offline crackt.

3. Schritt: Zusätzlich zum Sammeln der Zugangsdaten erstellt die Hackergruppe mithilfe öffentlich zugänglicher Tools eine Karte des internen Netzwerks und spioniert Active Directory, SQL-Server und NETBIOS aus. Besonders in dieser Aufklärungsphase sammelt die Gruppe Informationen über Systeme, die SQL-Instanzen laufen haben, um dort Schemata für verschiedene Datenbanken und SQL User Accounts zu hinterlegen. Zu den verwendeten Tools zählen dabei Microsofts eigenes SQL-Abfrage-Tool, Query Express, und Adfind. Im Laufe eines einzigen Tages attackiert die Gruppe so mehr als 900 SQL-Server, um dort die Ergebnisse ihrer Spionage abzulegen und künftige Operationen zu unterstützen.

4. Schritt: Mithilfe der erbeuteten Daten beginnt Fin6 anschließend damit, auch andere Systeme zu infizieren und die Operation auszuweiten. Dazu benutzen sie gestohlene Admin-Zugangsdaten in Verbindung mit Remote Command Execution-Tools wie PsExec und Remote Command Executor, um weitere Systeme zu infiltrieren. Um die Präsenz im angegriffenen System zu gewährleisten und den interaktiven Zugang aufrechtzuerhalten, setzt die Gruppe das öffentlich verfügbare Plink Command Line Utility ein, um SSH-Tunnel zu ihren eigenen Command-and-Control-Servern herzustellen. Über diese SSH-Tunnel wird Remote Desktop Protocol-Traffic geroutet und gleichzeitig interaktive RDP-Sitzungen im befallenen Netzwerk gestartet.

5. Schritt: Die PoS-Malware Trinity zieht gezielt Bezahlkartendaten aus dem Arbeitsspeicher der befallenen Systeme. Dazu erstellt sie zunächst Mutexes namens m_number3 und MuTex-Check und zieht

Zum Autor

Frank Kölmel, Vice President Central and Eastern Europe, FireEye, München

sich zurück, falls eine der beiden bereits existiert. Anschließend arbeitet sich die Malware durch die aktuellen Prozesse und untersucht den Speicherbedarf eines jeden Prozesses. Dabei werden Prozesse mit Modulnamen, die kürzer als fünf Zeichen sind, sowie einige spezifische Prozessnamen, die üblicherweise keine Bezahlkartendaten aufweisen, übersprungen. Trinity loggt gekaperte Daten in einem Verzeichnis auf der Festplatte, üblicherweise in %WINDIR%\temp oder %WINDIR%\help. Anschließend verschlüsselt die Malware die Daten mit einer einfachen Ersatz-Chiffre und Single Byte XOR mit dem Schlüssel 0xAA.

6. Schritt: Um die gestohlenen Daten schließlich aus dem System zu extrahieren, benutzt die Hackergruppe ein Script, um sich systematisch durch eine Liste von befallenen PoS-Systemen zu arbeiten. Dabei werden die Daten in ein nummeriertes Log-File kopiert, bevor die Originale entfernt werden. Die Log-Files werden in einem ZIP-Archiv komprimiert, das durch die Umgebung über ein Zwischensystem auf das System der Angreifer transportiert wird. Von dort kopiert die Gruppe die gestohlenen Daten per FTP auf ihren externen Command-and-Control-Server. In einem anderen Fall hat Fin6 eine alternative Extraktionsmethode angewandt, bei der sie die Bezahlkartendaten auf einen öffentlichen Filesharing-Service hochgeladen haben.

Gestohlene Daten im Card Shop

Die gestohlenen Daten werden in einem sogenannten Card Shop verkauft. Diese Shops werden in verschiedenen Cybercrime-Foren beworben und bieten Kriminellen regelmäßig Zugang zu Millionen von gestohlenen Bezahlkartendaten, was einer der letzten Schritte für Cyberkriminelle bei der Monetarisierung ihrer erbeuteten Daten darstellt. Dieser spezielle Shop verkauft schon seit 2014 von Fin6 extrahierte Daten. In jedem Fall tauchten die Daten innerhalb von sechs Monaten nach dem Beginn der Aktion von Fin6 im Shop auf. In manchen Fällen können mehr als zehn Millionen Karten, die auf einen spezifischen, mit Fin6 in Verbindung gebrachten Diebstahl zurückgehen, im Shop identifiziert werden. Üblicherweise wird ein Großteil der gestohlenen Daten schnell gekauft, um den Diebstahl auszunutzen.

Eine kleine Berechnung des Profits

Der Verkauf gestohlener Bezahlkartendaten ist ein profitables Geschäft für alle am Diebstahl und Verkauf beteiligten Parteien. In einem Fall, der zu Fin6 zurückverfolgt werden kann, wurden Daten von rund 20 Millionen Karten gestohlen. Da diese Karten größtenteils aus den USA stammten und zu diesem Zeitpunkt eine US-Karte durchschnittlich für etwa 21 Dollar im Shop verkauft wurde, hätte der Umsatz, falls alle Daten zum Vollpreis verkauft worden wären, rund 400 Millionen Dollar betragen.

Tatsächlich schafft der Shop diesen Umsatz nicht ganz, da nicht alle Daten verkauft werden. Liegen sie aber länger, verlieren sie schnell an Wert – Käufer wollen nur die neuesten Daten. Zusätzlich bietet der Shop, abhängig von verschiedenen Faktoren, auch Discounts auf gekaufte Ware an. Cyberkriminelle, die sich im Shop die gestohlenen Daten kaufen, können davon ausgehen, dass sie durch betrügerische Transaktionen einen deutlichen Gewinn machen.

Nicht alle Daten, die in diesem spezifischen Shop verkauft wurden, können eindeutig einem bestimmten Vorfall oder einer bestimmten Gruppe zugeordnet werden. Außerdem ist noch unklar, in welcher Verbindung die Betreiber des Shops zu den Hackern stehen, die die Daten stehlen. Es ist möglich, dass die Shopbetreiber Beziehungen zu verschiedenen Hackergruppen haben. Es könnten auch Mitglieder von Fin6 zu den Betreibern des Shops gehören oder die Daten lediglich zum Weiterverkauf an die Seite verkaufen.

Fazit: Wer verhindern möchte, dass sein Unternehmen einem solchen Datenklau zum Opfer fällt und Schaden von seinen Kunden abwenden möchte, muss sich absichern.

Ein wichtiger Bestandteil einer umfassenden Security-Strategie ist die Analyse der Bedrohungsdaten (Threat Intelligence). Diese hängt von verschiedenen Faktoren ab. Da ist zunächst der Überblick über die allgemeine Bedrohungslage und die Möglichkeit, Bedrohungen über Länder, Industrien und Organisationen hinweg zu erkennen sowie detaillierte Informationen über die Vorgehensweise von Angreifern zu erhalten. Außerdem benötigt man erfahrene Analysten, die die gewonnenen Erkenntnisse ordnen und interpretieren können. Am Ende ist es ein Zusammenspiel aus Technologie und Threat Intelligence, das den umfassendsten Schutz für ein Unternehmen bietet.

Die Beobachtung von Fin6 zeigt, wie echte Threat Actors agieren. Sie gewährt nicht nur einen Einblick in die technischen Einzelheiten des Angriffs sondern auch in den Faktor Mensch – nämlich die Interaktion zwischen Kriminellen oder kriminellen Gruppen und wie im Untergrund nicht nur Daten ausgetauscht werden, sondern auch Tools, Nutzerdaten und Zugänge.

Threat Intelligence für Händler und Emittenten

Im Oktober 2015 haben Visa Inc. und Fire Eye die gemeinsame Entwicklung von Tools und Dienstleistungen angekündigt, um Händler und Kreditkartenherausgeber im Kampf gegen großangelegte Cyberattacken auf Zahlungsdaten zu unterstützen. „Visa and Fire Eye Community Threat Intelligence" (CTI) führt Informationen beider Unternehmen über gezielte Angriffe zusammen. So sollen Händler und Kreditkartenherausgeber Angriffe auf ihre IT und Zahlungsinfrastruktur rasch erkennen und entsprechend reagieren können.