SOPHOS

Sophos Experte:

„Cyber-Kriminelle sind Geschäftsleute.“

Im Interview spricht Chester Wisniewski, Sicherheitsexperte bei Sophos, über die Entwicklung und den aktuellen Markt der Cyberkriminalität am Beispiel von Ransomware und Co.

Eine erste CryptoWall-Ransomware-Welle traf Anwender gegen Ende des Jahres 2014. Ist CryptoWall auch heute noch eine Bedrohung?

CryptoWall ist immer noch die beliebteste Form der Ransomware, sie wird in 50 bis 75 Prozent aller Angriffsfälle verwendet. Es begann mit Version 2.0, mittlerweile sehen wir Version 4.0. Die Pionierarbeit hierzu leistete CryptoLocker, die erste Ransomware, die wirklich verlässlich verschlüsselte und schlimme Schäden verursachte. Zwischen dem 17. September und dem 31. Oktober 2014 räumte CryptoLocker in nur sechs Wochen den monetären Gegenwert von 33 Millionen Dollar ab. Das waren große Neuigkeiten in der kriminellen Szene.

Im Juni 2014 wurde die CryptoLocker-Gruppe in einer groß angelegten FBI-Aktion enttarnt und festgesetzt. Wie jede gute Idee fand aber auch diese ihre Nachahmer und so entstanden sechs oder sieben andere Gruppen, die sie kopierten, etwa CryptoWall, CryptoFence, TeslaCrypt, Locky, Maktub – zwei von ihnen nannten sich sogar CryptoLocker, weil der Name allein schon so viel Angst und Schrecken unter den Opfern verbreitete, dass diese gar nicht erst versuchten, sich zu wehren.

Wie unterscheidet sich Locky beispielsweise von CryptoLocker? Und warum werden speziell Krankenhäuser so oft angegriffen?

Locky verbreitet sich, wenn jemand den Anhang einer E-Mail öffnet, etwa "Die Rechnung Ihres Flugtickets von XY Airlines". Meist wird dann verlangt, ein Makro zu aktivieren und damit ist die Infektion geschehen.

Verschlüsselt die Ransomware dann das gesamte Laufwerk, wird das System lahm gelegt und der Computer ist nicht mehr funktionsfähig somit auch für die Täter-Opfer-Kommunikation nicht mehr nutzbar. Die CryptoWall-Hacker umgingen das, indem sie nur Dateien mit bestimmten Endungen verschlüsselten, etwa Word-Dokumente, Bilder und Filme, insgesamt zirka 40 bis 50 Dateitypen. Auch Locky arbeitet so. Cryptowall 4 verschlüsselt alles außer den Dateien, die der Computer zum Arbeiten benötigt.

Maktub, eine weitere neue Ransomware-Variante, zielte besonders auf Krankenhäuser ab. Hier ist aufgrund der sensiblen Informationen das meiste Geld zu

machen und entsprechend hoch sind die Summen, die die Kriminellen fordern. Immerhin ist es enorm wichtig, dass Ärzte sofortigen Zugriff auf Patientenakten haben. Hier funktioniert die Einschüchterung noch besser, als bei anderen Unternehmensformen.

Wie viel ist darüber bekannt, woher Ransomware stammt und wer die Hacker sind?

Im Falle der Internet-Kriminalität im Allgemeinen ist es egal, woher die Täter kommen – jedes Land hat welche. Viele kommen aus großen Städten, aber wir haben auch viele der Spuren in kleine Orte zurückverfolgen können. Vielleicht gibt es dort nicht so viele Möglichkeiten, Geld zu verdienen.

Viele der wichtigsten Akteure sind bekannt und werden verdächtigt, von ausländischen Regierungen geschützt zu werden. Sie bemühen sich nicht einmal, ihre Identitäten zu verschleiern. Sie sprechen mit uns und machen sich sogar über uns lustig. Offenbar bestechen sie regionale Beamte, haben nichts zu befürchten und fühlen sich entsprechend sicher. In der Vergangenheit haben sie sogar kleine Nachrichten für den Virenanalysten in der Malware platziert.

Wie kann man Ransomware bekämpfen?

Bei großen Malware-Angriffswellen erstellen wir häufig Arbeitsgruppen innerhalb der Sicherheitsbranche. Sophos, viele unserer Mitbewerber und Strafverfolgungsbehörden tauschen Informationen aus in der Hoffnung, einen besseren Schutz und auch Verhaftungen zu erreichen.

Eine bessere Zusammenarbeit zwischen den Nationen würde helfen, die Zahl der Malware-Autoren auszudünnen. Die Wahrheit aber ist, dass viele Regierungen einfach andere Sorgen haben. Internet-Kriminalität zu bekämpfen hat keine Priorität.

Wie viele Menschen benötigt man für einen Ransomware-Angriff? Sprechen wir über ganze Cyber-Hacking-Unternehmen mit Office-Suiten und Pizza-Freitag, oder über einen schlecht gelaunten Außenseiter, der mit einer Tüte Chips und seinem Laptop auf dem Bett sitzt?

Eine einzelne Person kann eine Ransomware zirka innerhalb einer Woche schreiben. Wahrscheinlicher ist es jedoch, dass es sich um drei oder vier Personen handelt. Die bisherigen Malware Kits entstanden, indem die Malware selbst, Beratung und zusätzliche Tools für einen einmaligen, festen Preis zwischen 1.000 und 10.000 US-Dollar gekauft wurden. Im Lieferumfang enthalten ist ein Anpassungstool, so dass kleinere Konfigurationen, Aussehen und Branding verändert werden können.

Programmierkenntnisse sind nicht vonnöten. Der Kriminelle muss nur das Kit erwerben und jemanden finden, der es unter die Leute bringt, um die Rechner zu infizieren. Wir leben in einer Dienstleistungswirtschaft. Man loggt sich also in eines der Foren im Untergrund, kauft das Set von einem Kriminellen und beauftragt einen weiteren damit, die Software auf möglichst vielen PCs zu installieren. Die Bezahlung erfolgt pro infiziertem Rechner. Üblicherweise beauftragen die Kriminellen dann Spammer mit der Verbreitung.

Dies ist eine ebenso beliebte wie etablierte Taktik. User werden mit einer Spam-Software infiziert, die der Verursacher dann an andere Kriminelle für deren Machenschaften vermietet. Es ist ein sehr ausgereiftes und gut funktionierendes Business.

Warum sind Bitcoins für das Bezahlen von Ransomware so beliebt und wie macht man Bitcoins zu Bargeld, ohne erwischt zu werden?

Bitcoin ist nicht annähernd so anonym wie die Leute denken. Falsch eingesetzt öffnet es den Strafverfolgern Tür und Tor. Um Bitcoins zu verwenden und vor allem anonym zu bleiben, muss für jedes Opfer ein so genannte Bitcoin-Wallet, eine Geldbörse, erstellt werden. Dies macht die Malware bereits selbständig, wenn sie den PC infiziert, für die Kriminellen bedeutet es keinen extra Aufwand.

In der Regel führen die Gauner dann einige tausend Zahlungen in ein größeres Wallet und hier beginnt dann der Geldwäsche-Prozess. Das Geld kann nicht einfach aus einem der Bitcoin-Geldautomaten gezogen werden, dann müssten die Strafverfolgungsbehörden ja nur einen Polizisten abstellen, der das Treiben beobachtet. Vielmehr werden sie dem Bitcoin-Tumbling zugeführt – eine Art Waschservice. Hier werden verschiedene Bitcoins miteinander vermischt, um nicht mehr einzeln nachverfolgbar zu sein. Alternativ können auch Gaming-Accounts eingesetzt werden. Die Bitcoins landen in einem Casino in Antigua, man spielt eine Runde Black Jack und führt das Geld zurück in Bitcoins oder eine andere Währungseinheit.

Natürlich sind alle diese Transkationen über Log-Funktionen nachvollziehbar. Mit Hilfe von Big Data Analytics können die Geldbewegungen bis in die Nähe der Kriminellen zurückverfolgt werden.

Wie viel Schuld trifft da die Bitcoin Betreiber?

Die wissen natürlich, dass ihr Angebot von Verbrechern genutzt wird – was mich persönlich sehr irritiert. Wozu brauche ich denn einen Bitcoin Tumbling-Service wenn nicht, um Geld zu waschen? Anonymisierung wird nicht immer zum Bösen verwendet, ähnlich wie Tor und anderen Anonymisierungstechniken auch, aber für Kriminelle ist es natürlich eine gute Gelegenheit.

Viele Opfer von Ransomware zahlen, um ihre Dateien zurückzubekommen. Ist das Ihrer Meinung nach richtig?

Es ist ständig das Gleiche. Die Leute fragen: "Nun, was sollen wir tun?" Sie wissen natürlich, dass die Antwort lautet: „Zahl nicht!!“ Aber für Unternehmen, die ihre Daten von irgendwo wiederherstellen müssen, ist es unter Umständen günstiger, die Verbrecher zu bezahlen. Die kennen diese Kosten/Nutzen Rechnung natürlich auch – schließlich sind sie selbst Geschäftsleute.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de