Mamba Ransomware verschlüsselt nicht nur Dateien, sondern ganze Festplatten

Die neue Ransomware Mamba setzt auf eine Raubkopie der Open Source Software DiskCryptor und macht Betroffenen das Leben besonders schwer

Die gute Nachricht zuerst: Diese Mamba wurde bisher noch nicht in der freien Wildbahn gesichtet. Anders als ihre bissige Namensgeberin vermuten lässt ist sie weder besonders gut gemacht noch wirklich zuverlässig.

Die schlechte Nachricht: Anders als andere Ransomware-Formen, die sich auf Dateien beschränken, verschlüsselt Mamba die gesamte Festplatte. Und es kommt noch schlimmer: Zeigen sich Betroffene sogar zahlungswillig ist es dennoch unwahrscheinlich, dass die Festplatte jemals wieder entschlüsselt werden kann.

Dennoch ist Mamba interessant, denn ihre Schöpfer sind offenbar noch in der Test-Phase, auf der Suche nach etwas Neuem. Das Geschäftsmodell der Cyber-Kriminellen kann zum heutigen Zeitpunkt noch nicht genau erklärt werden.

Es gibt bereits eine Ransomware, die ähnlich arbeitet, genannt Petya. Sie verschlüsselt den Master-Index der Festplatte (auch Master File Table oder MFT genannt) und informiert die Verbraucher über einen Boot-Bildschirm im 1990er Jahre-Look darüber, wie sie sich aus ihrer misslichen Lage herauskaufen können. Rebooting? Fehlanzeige. Petya belässt zwar den Großteil der Rohdaten unverschlüsselt auf Sektorebene – allerdings außer Reichweite.

Mamba geht einen Schritt weiter: sie kriecht in jeden Sektor der Festplatte inklusive MFT, Betriebssystem, Anwendungen, freigegebene und persönlichen Daten. Dabei kommt Mamba mit sehr geringem Programmieraufwand aus: die Malware installiert und aktiviert eine Raubkopie der Open-Source-Software DiskCryptor.

Wie Mamba infiziert

Verbraucher sollten sorgfältig prüfen, welche E-Mails sie öffnen – besonders dann, wenn es nach den üblichen Dokumenten aussieht: Rechnungen, Bestellbestätigungen, Zahlungsaufforderungen, Anfragen und so weiter.
Wird eine infizierte Datei versehentlich geöffnet, passiert zuerst nicht viel: Mamba fragt, ob eine App eines unbekannten Entwicklers installiert werden darf. Nach einer Weile rebootet der Rechner. Vor dem Neustart installiert sich Mamba heimlich als Windows-Dienst mit dem Namen Defragmentation Service, ausgestattet mit lokalen Systemprivilegien.

Malware, die als LocalSystem-Dienst ausgeführt wird, ist auch ohne Anmeldung aktiv, läuft unsichtbar vom Windows-Desktop und hat eine nahezu vollständige Kontrolle über den lokalen Computer. Nach dem Neustart installiert sich DiskCryptor im Hintergrund, zu finden im Verzeichnis C unter dem Namen C:\DC22.

Der nächste Reboot des Computers erfolgt nicht automatisch, so dass alle Dateien noch verfügbar sind, das DiskCryptor Protokoll enthält sogar das Passwort im Klartext.

Normalerweise ist Skepsis angesagt bei Software, die vetrauliche Daten wie Passwörter in Klartext-Log-Dateien ablegt. In diesem Fall kann es die Rettung sein: Verbraucher können die Option Decrypt im DCRYPT Dienstprogramm nutzen, um die Verschlüsselung mit Hilfe

des Passworts rückgängig zu machen. Dies natürlich nur, wenn die Hintergrundverschlüsselung überhaupt bemerkt wurde. Wenn nicht, kommt die böse Überraschung samt Zahlungsaufforderung nach dem nächsten Reboot.

Leider wurde DiskCryptor in den vergangenen zwei Jahren kaum weiterentwickelt und ist mit den meisten aktuellen Windows-Versionen nicht mehr kompatibel. Auf jedem unterstützten Mac findet sich eine Disk im GPT-Format, gleiches gilt für die neueren Windows-Computer.. In diesem Fall installiert sich DiskCryptor dennoch, funktioniert aber nicht wie gewünscht. Nach dem Reboot ist nicht einmal die Zahlungsaufforderung sichtbar. Und auch bei einigen älteren Festplatten war „Missing Operation System" die letzte Nachricht.
Das größte Problem ist allerdings, dass in diesem Fall eine Entschlüsselung der Daten auch mit vorhandenem Key nicht möglich ist.

Was zu tun ist

„Wir empfehlen im Falle von Ransomware nicht zu zahlen, auch wenn es sich um private Daten mit womöglich einem hohen ideellen Wert handelt oder Firmendaten, die aufwändig neu beschafft werden müssen", so Sascha Pfeiffer. „Womöglich müssen sich Betroffene mit dem Verlust der Daten abfinden und eine Neuinstallation vornehmen. Es gibt noch keine gesicherten Erkenntnisse dazu, wie die Gauner mit dem Erpressungsvorgang umgehen und ob die Daten wieder freigegeben werden. Am besten ist jedoch eine gute AV-Lösung, um die Schädlinge gleich von Anfang an abzuwehren. Es gibt eine Fülle guter Sicherheitslösungen sowohl für Unternehmen als auch für Privatanwender. Beispielsweise Sophos Home, eine kostenlose Sicherheitslösung für den Privatgebrauch auf Enterprise-Niveau. Keinen Schutz zu installieren, ist schlicht nicht mehr zeitgemäß."

https://www.sophos.com/de-de/lp/sophos-home.aspx

Sophos, 28. September 2016

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

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