#1 Choice of DIGITAL WORLD

eScan™
Anti-Virus & Content Security

RANSOMWARE

eScan debuts new Technology for Detection and Mitigation

www.escanav.de

Wir begannen, uns mit Ransomware zu beschäftigen, als sie anfing im Jahr 2012 an Bedeutung zu gewinnen, wie auch immer, Ransomware ist schon fast eine Dekade präsent.

Während der Anfangsphase war die Wirkung von Ransomware Furcht und Schock, da anders als bei Trojanern oder Malware oder APTs die Anwesenheit von Ransomware sofort ersichtlich und die Botschaft laut und deutlich war „ Sie sind infiziert". In all diesen Jahren beobachteten wir die verdeckten Methoden eines Virus, während es im Hintergrund ein System infizierte, resident blieb und andere Systeme infizierte, darüber hinaus haben viele dieser Viren damit begonnen, die Logik von Kommando und Kontrolle zu implementieren, womit wichtige Informationen heimlich gestohlen wurden.

Das Niveau der Fachkenntnisse einen solchen Virus zu schreiben war enorm, da der Autor Wege finden musste, um immer ein oder zwei Schritte den Erkennungsmechanismen voraus zu sein und zur gleichen Zeit den Kriminellen die Möglichkeit zu geben, die gestohlenen Daten zu verwenden.
Diese Kriminellen vermieteten diese stark infizierten Systeme, allgemein bekannt als Zombie-Computer, auch an andere Kriminelle, die dann ihre ruchlosen Aktivitäten, nämlich versenden von Spam, DDOS-Attacken, Bitcoinmining usw. durchführen konnten. Egal, wenn wir über Ransomware sprechen, während der ersten Tage, war sie gedacht als ein höchst anspruchsvolles Code-Stück, seit es Verschlüsselung gibt.

Ransomware-Ersteller erweiterten jedoch auch ihre Taktik und begannen mit der Identifizierung von wichtigen Dateien, die angegriffen werden würden.
Es gibt zahlreiche Verschlüsselungsbibliotheken, die nicht nur von erfahrenen Programmierern, sondern auch durch die Script-Anfängern verwendet werden können.

Es war nicht unbedingt notwendig als Programmierer ein Verschlüsselungsexperte zu sein, seit alle Informationen leicht zugänglich und das Interesse des Ransomware-Autors folgende Punkte waren:

1. Fähigkeit, sich in das System zu schleichen

2. Die Dateien anhand ihrer Erweiterungen zu verschlüsseln

3. Die Verschlüsselungs-Schlüssel zurück an den CNC-Server zu übertragen

Ransomware-Infektionsvorgänge kamen in verschiedenen Formen, begannen als eine komprimierte Binärdatei und als die verschiedenen Anbieter begannen, solche Dateien zu blockieren, begannen wir Ransomware zu in eingebetteten Makros in Doc oder Docx-Dateien zu erkennen.

In jüngster Zeit begannen sie, Javascripts, VB-Scripts und Powershell basiertes Scripting zu nutzen, um Ransomware zu erstellen. Um diese zu bekämpfen, begannen die Anbieter Skriptmodule zu blockieren, aber wie lange soll dieses Katz- und Mausspiel noch weitergehen? Forscher haben herausgefunden, dass es immer schwieriger wird, das Elixier zu finden, welches Ransomware im Keim erstickt.

Die Erkennung von Ransomware ist nicht die einzige Lösung, das Abschalten des DGA basierten CNC wird die Verbrecher einfach 3-4 Wochen zurückwerfen. Unter Umständen kann es sein, dass Ransomware sich nicht nur in das gut geschützte Umfeld einer End-Point Security Lösung einschleicht, sondern auch Firewalls / Security Appliances umgeht und lokale Dateien wie auch Netzwerkdateien verschlüsselt. Herkömmliche Backupsysteme stützten sich auf die Tatsache, dass sie von bestimmten Ordnern, die als wichtig angesehen werden, eine Sicherung vornehmen.

Ransomware hält sich an bestimmt Dateien, die in einigen Fällen wird sie Bilddateien verschlüsseln und hinterlässt kleine Abbilder davon, um Ihnen zu zeigen, was verloren sein könnte, wenn das Lösegeld nicht gezahlt wird. Wir bei eScan, verfolgen aktiv Ransomware auf allen Ebenen, analysieren, studieren das Verhalten und finden verschiedene Möglichkeiten heraus, um diese Bedrohung zu erkennen und abzumildern, zudem bieten wir einen Mechanismus für eScan Benutzer, um unverwüstlicher zu sein.

eScan stellt jetzt erstmalig eine **Proaktive Verhaltensbasierte Analyse Engine** (PBAE) vor, die die Aktivität aller Prozesse auf dem lokalen Computer überwacht, und falls die PBAE Aktivitäten oder ein Verhalten erkennt, das auf Ransomeware zurückzuführen ist, wird die rote Fahne gezeigt und der Prozess unterbrochen, um weitere Schäden abzuwenden. Allerdings ist Ransomware auch bekannt dafür, dass sie auf Netzwerkfreigaben Dateien verschlüsselt, in solchen Fällen, wenn ein infiziertes nicht geschütztes System versucht auf die Netzwerkfreigabe eines geschützten Systems zuzugreifen, um dort die Dateien zu ändern, wird PBAE die Netzwerksitzung sofort abbrechen.

In unserem Kampf gegen Ransomware arbeiteten wir an einem intelligenten Shadow-Backup-Mechanismus, welcher während solcher Eventualitäten ausgelöst werden kann, damit die Anwender schnell die Nachbeben der Ransomware überwindet.

Ransomware der Art Locky, Zepto, Crysis, Crypto, um einige zu nennen, zusammen mit ihren Varianten wird relativ einfach von eScan mit der **Proaktiven Verhaltensbasierten Analyse Engine (PBAE)** bewältigt. Darüber hinaus haben wir die Ereignisse von unserem Cloud-Server untersucht und waren erfolgreich bei der Aufdeckung tausendender Ransomware Angriffe seit der Einführung der **Proaktiven Verhaltensbasierten Analyse Engine.**