Was ist Ransomware?

Ransomware ist eine Malware-Art, die den Zugriff auf das System eines Opfers oder auf persönliche Dateien verhindert, indem sie diese als "Geisel" halten und Lösegeld verlangen, um sie zu befreien. Wie in [1] angegeben, wurde dieser Angriffstyp Ende der 80er Jahre erstmals eingeführt, und das Lösegeld wurde per Post bezahlt. Heute ist die Technologie fortgeschritten, so dass die Autoren die Zahlung in Kryptowährung oder Kreditkarte verlangen.

Gemäß [2] wird eine Kategorisierung der Ransomware durch die verwendeten Mittel beschrieben. Wie aus der Quelle hervorgeht, können die Ransomware Angriffe von mild bis gefährlich sein:

Die erste Kategorie ist Scareware, zu der Rogue-Software und Betrug gehören. Das Opfer erhält möglicherweise Pop-up Nachrichten, dass Malware entdeckt wurde, und er muss bezahlen, um diese Nachrichten gelöscht zu werden. Dies ist nur ein Versuch, das Opfer zu erschrecken, aber die Dateien sind sicher. Die Nachrichten werden immer wieder auftauchen, aber es besteht kein Grund zur Sorge, nachdem das System einmal inspiziert wurde.

Eine andere Kategorie ist die Bildschirmsperre, die sich auf Terrorebene befindet. Wenn der Betroffene mit dieser Art von Malware infiziert ist, wird er vollständig von seinem Computer gesperrt. Die Hacker verwenden das FBI oder ein anderes Logo des US-Justizministeriums, um anzuzeigen, dass auf dem Gerät illegale Aktivitäten gefunden wurden und dass eine Geldstrafe gezahlt werden muss.

Letzt endlich sprechen sie über die verschlüsselnde Ransomware, die die schädlichste Ransomware von allen ist. In diesem Fall erfassen die Hacker Ihre Dateien, verschlüsseln sie und fordern die Zahlung vom Opfer, um die Dateien zurückzugeben. Dieser Art ist so gefährlich, weil die Dateien können nicht wiederherstellt werden, nur wenn Sie bezahlen. Aber selbst dann können Sie nicht sicher sein, dass Sie die Dateien zurückerhalten - zum größten Teil auch nach der Bezahlung sind die Dateien nicht mehr verfügbar.

Apropos Kategorien, in [1] und [3] werden weitere Möglichkeiten zur Unterteilung der Ransomware vorgeschlagen.

Sie teilen diese Malware nach Ausbreitung und nach Zahlungsmethode. Die erste Methode ist in drei Arten unterteilt: Exploitation-Kits, also vorgepackte Tools, ein Affiliate-Programm, in dem unterstützten Code entwickelt und verbreitet wird, und schließlich Malvertising-Kampagnen, in denen Spam-E-Mails auf verschiedene Benutzer abzielen. Bewegen Sie sich auf der zweiten Kategorie der Einstufung durch Zahlung [1] und [3] sich einig, dass es zwei Möglichkeiten gibt, zuerst durch Direktzahlung und zweiten Trog indirekte Zahlung, als Pre-Paid - Gutscheine zum Beispiel zu zahlen.

Wie bereits erwähnt, wurde Ransomware in den 1980er Jahren eingeführt und ist als PC Cyborg oder AIDS bekannt. Dadurch würde die C: Partition nach einem bestimmten Neustart des Geräts verschlüsselt und das Opfer aufgefordert, das Geld (189 US-Dollar) per Post zu senden. Die Verschlüsselung war einfach, so dass sie leicht rückgängig gemacht werden konnte und keine Gefahr darstellte.

Als die Welt anfing, von Ransomware betroffen zu werden, und später wieder in diesen Ausdruck eingeführt wurden, waren die Opfer normale Menschen mit individuellen Systemen. Später erkannten nur die Kriminellen das Potenzial der Ransomware und machten sich an die Geschäfte. Sie haben in der Branche viel Schaden angerichtet, was zu Datenverlusten und sinkender Produktivität geführt hat.

In der aktuellen Zeit wurden ab Ende 2016 mehr als 10% aller globalen Malware-Entdeckungen als Ransomware eingestuft.

Was zu tun, wenn infiziert?

Es gibt viele verschiedene Arten, wie Sie sich infizieren können. Die üblichste Art ist bösartige Spam-Mails, wo sich Malware Software sich drinnen versteckt.

Wenn Sie sich infizieren, denken Sie daran, dass Sie niemals das Lösegeld zahlen müssen. Dieser Rat wird vom FBI und anderen Behörden, die Lösegeldforderungen fordern, unterstützt. Wenn wir nur zahlen, fordern wir die Angreifer dazu auf, unsere Systeme und Dateien als "Geisel" zu halten. Das Problem ist, dass, auch wenn wir bezahlen, es unzählige Möglichkeiten gibt, Dateien zu verschlüsseln, und nicht alle Entschlüsselung haben. Daher besteht die Gefahr, dass wir unsere Dateien mit der falschen Entschlüsselungssoftware weiter verschlüsseln.

Sie können sich auch schützen, indem Sie Sicherheitsprodukte installieren, die Ihren Computer scannen und die Bedrohung entfernen. Möglicherweise werden die Dateien nicht wiederhergestellt, aber das Problem ist zumindest verschwunden.

Da die Ransomware wiederaufgetaucht ist, haben einige Informationssicherheitsorganisationen sowie Strafverfolgungsbehörden diese Bedrohung in Bedrängnis gebracht. Unter diesen Agenturen ist das No More Ransom Project zu beachten, das von der National High-Tech Crime Unit der niederländischen Polizei und dem Europol Cybercrime Center in Zusammenarbeit mit den beiden Sicherheitsunternehmen Kaspersky Lab und McAfee ins Leben gerufen wurde. Eine weitere wichtige Erwähnung ist das FBI Ransomware Prevention & Response-Projekt, bei dem das Federal Bureau of Investigation spezielle Abteilungen geschaffen hat, um die Menschen über Ransomware-Bedrohungen aufzuklären. Letztendlich, genau wie die US-Initiative, wurde in Großbritannien das National Cybercrime Security Center eingerichtet. Dazu gehörten dedizierte Webseiten, auf denen die Bürger Informationen erhalten, Unterstützung erhalten und anderen Menschen helfen, indem sie sich über dieses Thema informieren.

Wie kann man sich dagegen schützen?

Als Erstes müssen Sie in Sicherheitssoftware investieren, die sogar die verwundbare Software vor Malware schützt.

Sichern Sie Ihre Dateien mit regelmäßigen Backups, entweder in der Cloud, wo Verschlüsselung ein wichtiger Faktor ist, oder auf verschlüsselten externen Festplatten.

Als letztes müssen Sie sicherstellen, dass Ihre Software und Apps aktualisiert werden. Update bedeutet, dass Fehler und anfällige Hintertüren behoben wurden und diese jetzt sicherer sind.

Am wichtigsten ist es, sich zu erziehen und informiert zu bleiben. Erfahren Sie, wie Sie bösartige Programme und Apps erkennen und auch anderen beim Lernen helfen können.