Der Aufstieg der Ryuk Ransomware: Maßnahmen gegen den hochentwickelten Erpressungstrojaner

Die Ryuk Ransomware hat unter Cyberkriminellen massiv an Popularität gewonnen. Die Zahl der entdeckten Angriffe stieg von nur 5.123 im 3. Quartal 2019 auf über 67 Millionen im 3. Quartal 2020, so das Ergebnis einer Sicherheitsstudie von SonicWall. Dies entspricht etwa einem Drittel aller Ransomware-Angriffe, die in diesem Quartal durchgeführt wurden. Die explosionsartige Zunahme von Ryuk hat zudem dazu geführt, dass die Gesamtzahl der im 3. Quartal 2020 gemeldeten Ransomware-Angriffe im Vergleich zum gleichen Zeitraum in 2019 um 40 Prozent gestiegen ist. Ryuk ist eine hochentwickelte Art von Ransomware, die gegen Organisationen auf der ganzen Welt eingesetzt wird, um sie aus ihren Computernetzen und Dateien auszusperren, bis das geforderte Lösegeld bezahlt wird. Ryuk verschlüsselt alle Zieldateien mit einer starken, auf AES-256 basierenden Verschlüsselung, mit Ausnahme der Dateien mit den Erweiterungen dll, lnk, hrmlog, ini und exe. Ryuk überspringt auch Dateien, die in den Verzeichnissen Windows System32, Chrome, Mozilla, Internet Explorer und Papierkorb gespeichert sind. Dieses Ausschlussverfahren soll vermutlich die Systemstabilität erhalten und Opfern den Zugriff auf einen Browser ermöglichen, um Lösegeldzahlungen zu leisten. Wie viele Ransomware versucht auch Ryuk, Datenträger-Schattenkopien zu löschen, um zu verhindern, dass die Opfer ihre Daten mit alternativen Mitteln wiederherstellen können.
Nach erfolgreicher Infektion der Zielsysteme, stellen die Täter Lösegeldforderungen in Höhe der geschätzten Zahlungskraft der Opfer. Nach Angaben von Forschern beträgt das durchschnittlich eingenommene Lösegeld etwa 750.000 Dollar (gezahlt in Bitcoin). Die bisher höchste bekannte Zahlung wird jedoch auf 34 Millionen Dollar geschätzt, die von einem unbekannten Unternehmen im Austausch für den Decryption Key übermittelt wurden. Die russische Gruppe, die hinter den Angriffen steckt, ist dafür bekannt, dass sie hocheffektive manuelle Hacking-Techniken und Open-Source-Tools einsetzt, um sich seitlich in kompromittierten Netzwerken zu bewegen. Dies hilft den Cyberkriminellen, Zugang zu möglichst vielen Verwaltungsbereichen zu erhalten und ihre Spuren zu löschen oder zu verwischen, bevor sie die Ransomware zur Detonation bringen, was verheerende Folgen hat.

Welche Ziele Cyberkriminelle ins Visier nehmen

Cyberkriminelle nehmen mit Ryuk ein breites Spektrum von Sektoren ins Visier. Eines der Ziele sind Einrichtungen im Gesundheitswesen, von denen viele besonders gefährdet sind. Denn Krankenhäuser und Gesundheitseinrichtungen verfügen häufig über eine Fülle veralteter Netzwerkinfrastrukturen, die nur unzureichend vor solchen Cyberangriffen geschützt sind. In den letzten Monaten haben Angriffe auf Krankenhäuser auf der ganzen Welt zu Störungen geführt. Im September 2020 legte ein Angriff Computersysteme im Universitätsklinikum Düsseldorf lahm und führte dazu, dass eine Patientin starb, da sie, statt in die nahegelegene Klinik, in ein weiter entferntes Krankenhaus gebracht werden musste. Es wird angenommen, dass Ryuk auch hinter dem jüngsten Ransomware-Angriff auf die Universal Health Services (UHS) steckt, die etwa 400 Krankenhäuser und Pflegezentren in den USA und in Großbritannien betreibt, und die Attacke damit einen der größten Cyberangriffe im Healthcare-Bereich in der Geschichte der USA darstellt.

Was Organisationen tun können, um sich wirksam zu schützen

Die Cybersicherheitsindustrie hat bereits zahlreiche Schritte unternommen, um Organisationen dabei zu helfen, sich gegen den Aufstieg von Ryuk zu verteidigen. So haben viele Anbieter von Advanced Threat Protection (ATP) kostenlose Policy Packs herausgebracht, mit denen Kunden ihre bestehenden Sicherheitstools und -lösungen aktualisieren können, um schnell verdächtige Netzwerkaktivitäten zu erkennen, die auf einen potenziellen Angriff durch Ryuk hinweisen. Hierzu gehören die Erkennung der massenhaften Bearbeitung von Dateien mit bekannten Ryuk-Ransomware-Erweiterungen, die Löschung von Volume-Schattenkopien und Versuche, eine Verbindung zu einer bekannten Command-and-Control-Infrastruktur herzustellen, die mit der Ransomware-Kampagne in Verbindung steht. Weiterhin können Organisationen die folgenden grundlegenden Schritte durchführen, um ihre Cybersicherheitsabwehr gegen Bedrohungen wie Ryuk zu stärken:

- Regelmäßige Datensicherungen: Die Durchführung regelmäßiger Sicherungen aller wichtigen Organisationsdaten ist eine der besten Möglichkeiten, die Störungen von Arbeitsabläufen im Falle eines erfolgreichen Angriffs zu minimieren. Die sichere Aufbewahrung dieser Backups außerhalb des Hauptnetzwerks verhindert, dass sie als Teil eines Angriffs gelöscht oder verschlüsselt werden.

- Sicherheitspatches auf dem neuesten Stand halten: Wie bereits erwähnt, sind die Anbieter von Cybersicherheitsdiensten bereits gut über Ryuk informiert, und die große Mehrheit hat ihre Produkte und Lösungen aktualisiert, um Ryuks Signaturen zu erkennen. Diese Aktualisierungen treten jedoch erst dann in Kraft, wenn Kunden die neuesten Sicherheits-Patches in ihren Netzwerken installieren. Daher ist es entscheidend, dass solche Patches

installiert werden, sobald sie veröffentlicht werden.

- Mitarbeiter über Cybersicherheit aufklären: Selbst fortschrittliche Cyber-Bedrohungen verlassen sich noch immer häufig auf die grundlegendsten Angriffsmethoden wie Phishing-E-Mails und Social-Engineering-Taktiken. Daher sollten in regelmäßigen Schulungen eine Aufklärung der Mitarbeiter durchgeführt werden, wie sie diese Angriffe erkennen können.

Ryuk stellt eine starke Bedrohung für Organisationen auf der ganzen Welt dar, insbesondere für Einrichtungen im Gesundheitswesen, von denen viele derzeit besonders anfällig sind. Daher ist es wichtig, dass Organisationen ihren bestehenden Schutz bewerten, Schwachstellen identifizieren und die richtigen Korrekturen umsetzen, um die Risiken dieser Angriffe zu minimieren.