LogRhythm®
The Security Intelligence Company

WIE RANSOMWARE FUNKTIONIERT

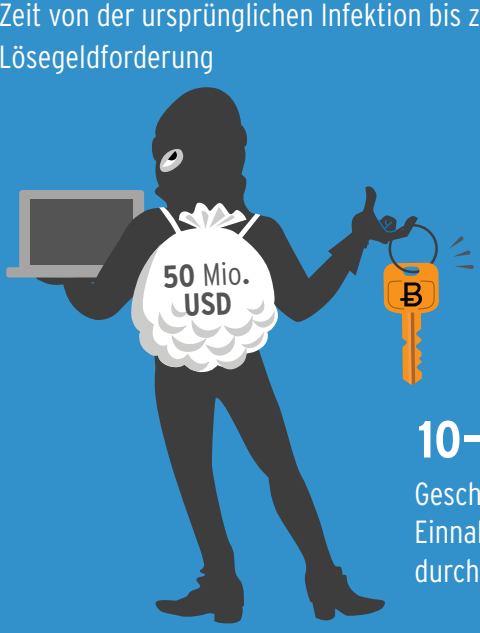
Ransomware gewinnt an Dynamik!
In den letzten drei Jahren ist Ransomware in das Rampenlicht der IT-Bedrohungslandschaft gerückt. Das FBI rechnet damit, dass Kriminelle 2016 mehr als 1 Mrd. USD mit Ransomware-Angriffen erbeuten werden.[1]

Was genau ist Ransomware?
Ransomware ist eine bösartige Software, die es einem Hacker erlaubt, den Zugang zu den wichtigen Informationen einer Privatperson oder eines Unternehmens einzuschränken und dann irgendeine Form von Zahlung zu verlangen, meist in Bitcoins, um die Einschränkung aufzuheben.

209 Millionen Betrag, den IT-Kriminelle im Q1 2016 mit Ransomware erbeutet haben[1]

1 Milliarde Verluste, die nach Schätzung des FBI 2016 durch Ransomware entstehen werden[1]

Zeit von der ursprünglichen Infektion bis zu einer Lösegeldforderung

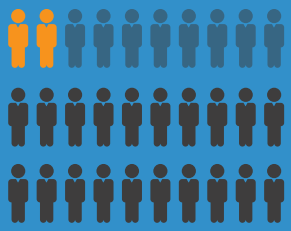


10–50 Mio. USD
Geschätzte monatliche Einnahmen von IT-Kriminellen durch Ransomware[3]

72%
Prozentsatz der Unternehmen, die nach einem Ransomware-Angriff mindestens 2 Tage nicht auf ihre Daten zugreifen konnten[4]

32%
Prozentsatz der Unternehmen, die den Datenzugriff 5 Tage oder länger verloren[4]

86%
Angriffe, von denen mindestens **2** Mitarbeiter betroffen waren[4]



47%
Angriffe, von denen mehr als **20** Mitarbeiter betroffen waren[4]

$17.000
Betrag, den das Hollywood Presbyterian Medical Center 2016 zahlte, um seine Dateien entsperren zu lassen und zum Normalbetrieb zurückkehren zu können[5]

$100.000
Betrag, den das Krankenhaus pro Tag allein dadurch verlor, dass es keine Patienten-CTs durchführen konnte[5]

[1]CNN-Money, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/, 15. April 2016
[2]Security Magazine, „'Ransomware' Attacks to Grow in 2016", 23. November 2016
[3]David Common, CBC News, „Ransomware: What You Need to Know", 11. März 2015
[4]Blogpost von Intermedia, „When ransomware strikes your business, are you prepared? Our new report findings may surprise you". 17. März 2016
[5]PYMNTS.com, „City Held Hostage – Via Bitcoin Ransomware", 22. März 2016

DIE 5 PHASEN
eines Ransomware-Angriffs

Ein Ransomware-Angriff besteht aus 5 verschiedenen Phasen. Zu verstehen, was in jeder Phase geschieht, und die Indicators of Compromise [IOCs] (Befallanzeichen) zu kennen, erháht die Wahrscheinlichkeit, einen Angriff erfolgreich abzuwehren – oder zumindest seine Folgen zu mindern.

Der zeitliche Ablauf eines Angriffs ist sehr konzentriert. Von der Ausnutzung und Infektion bis zum Erhalt einer Lásegeldforderung vergehen oft nur 15 Minuten. Die frçhen Warnzeichen zu erkennen ist die entscheidende Voraussetzung, um einen Angriff erfolgreich zu stoppen.

1

Phase 1: Ausnutzung und Infektion (T -00:00)

Damit ein Angriff erfolgreich ist, muss die bösartige Ransomware-Datei auf dem Computer ausgeführt werden. Dies geschieht oft über eine Phishing-E-Mail oder ein Exploit Kit. Im Fall der CryptoLocker-Malware ist das Angler-Exploit Kit eine bevorzugte Methode, um die Ausführung zu erreichen.

2

Phase 2: Bereitstellung und Ausführung (T -00:05)

Während dieser Phase wird die eigentliche ausführbare Ransomware auf dem System des Opfers bereitgestellt. Nach der Ausführung setzt sich die Ransomware mittels Persistenz-Mechanismen im System fest.

3

Phase 3: Vernichtung von Sicherungskopien (T -00:10)

Ein paar Sekunden später macht sich die Ransomware an die Sicherungsdateien und -ordner auf dem System des Opfers und entfernt sie, um eine Wiederherstellung zu verhindern. Das ist eine Besonderheit von Ransomware - andere Arten von krimineller Software machen sich nicht die Mühe, Sicherungsdateien zu löschen.

4

Phase 4: Dateiverschlüsselung (T -02:00)

Sobald die Sicherungskopien vollständig entfernt wurden, führt die Malware mit dem Command-&-Control--Server (C2) einen sicheren Schlüsselaustausch durch und richtet damit die Verschlüsselungsschlüssel ein, die auf dem lokalen System verwendet werden sollen.

5

Phase 5: Benachrichtigung des Benutzers und Cleanup (T -15:00)

Nachdem die Sicherungskopien entfernt wurden und die Verschlüsselung abgeschlossen ist, werden die erpresserische Forderung und die Zahlungsanweisungen präsentiert. Oft erhält das Opfer eine Zahlungsfrist von ein paar Tagen. Danach steigt das Lösegeld.

Und ähnlich wie bei den Nachrichten in „Mission Impossible", die sich selbst zerstören, entfernt sich die Malware schließlich vom System, um keine nennenswerten Spuren zu hinterlassen, die helfen würden, bessere Abwehrmechanismen gegen die Malware zu entwickeln.

Ransomware-Angriffe gewinnen zunehmend an Dynamik. Weil diese Angriffe für die Täter so lukrativ sind, werden sie sicherlich häufiger, noch schädlicher und deutlich teurer werden.

Der Erfolg Ihres Unternehmens bei der Abwehr von Ransomware-Angriffen hängt stark von Ihrer Vorbereitung und den Tools ab, die Sie einsetzen, um Ihre Systeme zu überwachen und verdächtige Aktivitäten zu erkennen, auf sie zu reagieren und sie zu neutralisieren.

Erfahren Sie unter www.logrhythm.com, wie Sie einen Ransomware-Angriff schnell erkennen und neutralisieren können.

LogRhythm®
The Security Intelligence Company