KASPERSKY lab

# ALLE HEBEL IN BEWEGUNG: ABWEHR VON RANSOMWARE AUF WORKSTATIONS UND SERVERN

www.kaspersky.de

*Ransomware ist einer der am schnellsten zunehmenden Malware-Typen. Die Angreifer brauchen sich bei Ransomware erst gar nicht die Mühe zu machen, wichtige Geschäftsdaten zu stehlen und dann weiterzuverkaufen – sie verschlüsseln sie einfach und verlangen dann ein „Lösegeld". Im Laufe der Jahre hat sich Ransomware von einer simplen Bildschirmsperre zu einer enormen Welle weitaus gefährlicherer Software weiterentwickelt. Deshalb sollten Sie nichts unversucht lassen, um Cryptolocker-Attacken abzuwehren.*

# WARUM IST RANSOMWARE ÜBERHAUPT EIN SOLCHES PROBLEM?

Wie funktioniert Ransomware, und warum ist sie so gefährlich? Diese Malware-Klasse basiert auf so genannten **Cryptors** – Trojaner, die sich verbreiten, sobald Sie einen entsprechend infizierten E-Mail-Anhang öffnen oder auf einen Link für eine speziell präparierte Webseite klicken. Das Modul verschlüsselt dann im Hintergrund alle Daten, die für Sie von Wert sein könnten. Hierzu gehören in der Regel persönliche Fotos, Archive, Dokumente, Datenbanken, Schaubilder usw. Nun verlangt der Cryptolocker die Zahlung eines Lösegelds – oft einen nicht unerheblichen Betrag –, bevor diese Dateien wieder entschlüsselt werden.

Anonymität hat für die Angreifer natürlich zu jedem Zeitpunkt oberste Priorität. Die Lösegeldforderung erfolgt deshalb z. B. in Bitcoins, wobei die Command-and-Control-Server in einem anonymen Netzwerk, z. B. Tor, verborgen werden. Gelingt es, den Datenverkehr zwischen Trojaner und Server abzufangen, wird die Dateientschlüsselung durch den Einsatz unorthodoxer Kryptografiemodelle, z. B. durch die Nutzung von Tor oder spezieller Verschlüsselungsalgorithmen, unmöglich gemacht (Trojan-Ransom.Win32.Onion nutzt z. B. alle diese Verfahren).

Mittlerweile verlangen Cryptolocker Lösegeld nicht nur für die Entschlüsselung von Benutzerdaten, sondern auch noch für einige zusätzliche „Dienstleistungen". Die Angreifer könnten den Einsatz z. B. durch eine zusätzliche Erpressung noch weiter erhöhen: „Entweder Sie zahlen, oder wir könnten uns gezwungen sehen, Ihren Browserverlauf an alle Ihre Kontakte zu verschicken."

# WIE VERBREITET IST RANSOMWARE?

| | Entdeckte Ransomware (mithilfe von Kaspersky Security Network) |
|---|---|
| 2014 | 121238 |
| 2015 | 448430 |
| **Gesamtzahl:** | **554267** |

2015 war die mithilfe des Kaspersky Security Networks entdeckte Zahl von Ransomware-Attacken beinahe viermal so hoch wie 2014: Es wurden fast **450.000 Angriffe** ermittelt. Es gibt eine Vielzahl unterschiedlicher Typen und Familien von Ransomware, z. B. CryptoWall, TeslaCrypt, TorrentLocker und Locky. **CTB-Locker**, ACCDFISA und GpCode gehörten dabei zu den berüchtigsten Malware-Typen. Das unten aufgeführte Zahlenmaterial aus dem Kaspersky Security Network vermittelt einen Eindruck vom Ausmaß der verschiedenen Ransomware-Attacken innerhalb der EU im Jahr 2015:

2015

| Einschätzung von Kaspersky Lab | Einzelne Benutzer (KSN) | Einzelne Benutzer (KSN), zusammen | Andere verwendete Namen für diese Malware |
|---|---|---|---|
| Trojan-Downloader.JS.Cryptoload + Trojan-Ransom.Win32.Bitman | 80017 1163 | 81180 | TeslaCrypt |
| Trojan-Ransom.NSIS.Onion + Trojan-Ransom.Win32.Onion | 16491 8571 | 25062 | CTB-Locker |
| Trojan-Ransom.Win32.Cryptodef | 7346 | 7346 | CryptoDefense (frühe Versionen), CryptoWall (spätere Versionen) |
| Trojan-Ransom.Win32.Snocry | 4998 | 4998 | |
| Trojan-Ransom.Win32.Cryakl | 4955 | 4955 | |
| Trojan-Ransom.Win32.Crypren | 1681 | 1681 | |
| Trojan-Ransom.Win32.Shade | 1390 | 1390 | |
| Trojan-Ransom.Win32.Crypmod | 1173 | 1173 | |
| Trojan-Ransom.Win32.Rack | 717 | 717 | TorrentLocker |
| Trojan-Ransom.Win32.CryFile | 395 | 395 | |

**Locky**, das möglicherweise bei der vor Kurzem ausgeführten Ransomware-Attacke auf das Hollywood Presbyterian Memorial Hospital zum Einsatz kam, wurde Mitte Februar diesen Jahres entdeckt und hat sich bereits als eines der beliebtesten im Umlauf befindlichen Ransomware-Tools erwiesen.

**TeslaCrypt**, Proben wurden erstmals im Februar 2015 entdeckt. Die Ransomware-Variante mutiert ständig, um der Entdeckung zu entgehen. TeslaCrypt wurde in den Medien allgemein als „Fluch" von Computer-Gamern dargestellt, da es diese Ransomware speziell auf spielespezifische Dateitypen (Spielstandspeicherung, Benutzerprofile usw.) abgesehen hat. Zu den geografischen Zielgebieten dieses Trojaners gehören die USA, Deutschland, Spanien und weitere Länder.

# SICHERHEITSLÖSUNGEN

Trotz all der hoch entwickelten Mechanismen, die heutzutage in Malware enthalten sind, lässt sich die Bedrohung durch Ransomware für Sie und Ihr Unternehmen entschärfen. Die Ransomware-Strategie von Kaspersky Lab besteht aus einer Reihe von Gegenmaßnahmen zur Bekämpfung von Ransomware.

Ihre **Sicherheitslösung sollte jederzeit eingeschaltet sein**, wobei Sie möglichst viele der enthaltenen Schutzfunktionen aktivieren sollten. Entscheidend ist darüber hinaus **eine regelmäßige Aktualisierung der Lösung**.

Es ist derzeit unmöglich, durch moderne Crypto-Malware verschlüsselte Dateien wieder zu entschlüsseln. Die einzige Möglichkeit, Ihre Daten wirkungsvoll vor einem Angriff zu schützen, besteht also einer Datensicherung. Ein **allgemeines Backup** (z. B. mithilfe von Acronis oder eines anderen Spezialprodukts), reicht jedoch selbst bei regelmäßiger Ausführung nicht aus, da hierbei kürzlich geänderte Dateien nicht berücksichtigt und dem Risiko ausgesetzt werden, durch verschlüsselte Dateien überschrieben zu werden.

## Host-basierte Sicherheit

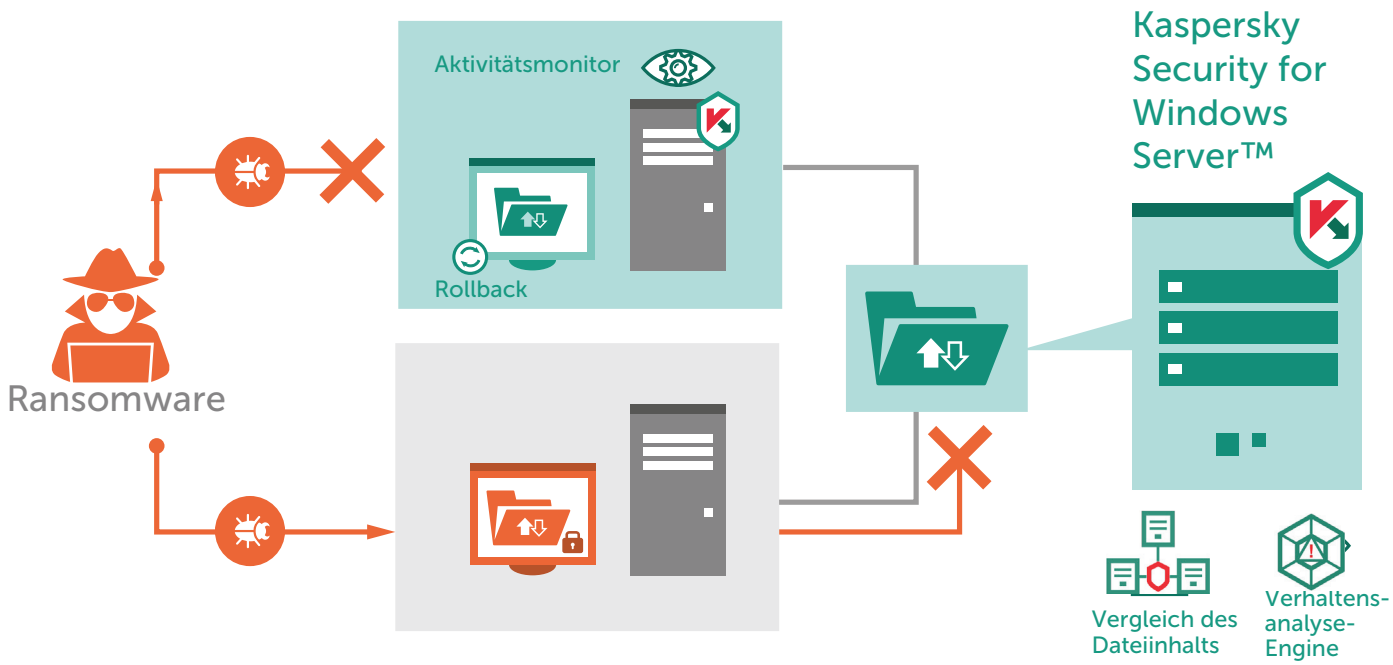
Dies ist einer der Gründe, warum in Produkten von Kaspersky Lab unsere Aktivitätsmonitor-Technologie eingesetzt wird. Der host-basierte Kaspersky-Aktivitätsmonitor analysiert die relevantesten Systemereignisdaten, einschließlich Informationen zu Dateiänderungen. Wird ein verdächtiges Programm registriert, das versucht, die persönlichen Dateien eines Benutzers zu öffnen, erstellt der Aktivitätsmonitor umgehend eine lokale Backup-Kopie davon. Stellt sich die Anwendung als Crypto-Malware (oder eine andere Schadsoftware) heraus, werden die unerwünschten Änderungen automatisch vom Kaspersky-Aktivitätsmonitor rückgängig gemacht. Sie erhalten lediglich eine Benachrichtigung zur stattgefundenen Aktivität – es gibt keine Unterbrechung, und ein Eingreifen durch den Benutzer ist ebenfalls nicht erforderlich.

Der Kaspersky-Aktivitätsmonitor sorgt für die Sicherheit von Benutzerdaten und unterbindet die indirekte Finanzierung von Cyberkriminellen durch Lösegeldzahlungen,mit denen diese „Schattenbranche" unterstützt wird und so die Entwicklung noch gefährlicherer Malware fördert.
Ein weiterer unserer host-basierten Ansätze zur Minderung des Risikos durch Cryptolocker besteht in der Erstellung von Regeln für die Programmstart-Kontrolle, mit der die Ausführung nicht genehmigter Programme verhindert wird.

## Server-basierte Lösung zur Abwehr von Ransomware

Einige Hosts innerhalb des Sicherheitsperimeters greifen möglicherweise auf gemeinsame SMB/CIFS-Verzeichnisse auf Unternehmensservern zu. Und nicht auf jedem Host ist der Aktivitätsmonitor aktiviert. Einige von ihnen sind möglicherweise vollkommen ungeschützt oder arbeiten mit Sicherheitssoftware, die keinen Schutz vor Ransomware bietet. In diesem Fall hat jeder Cryptor, der per E-Mail oder über einen anfälligen Browser eindringt, außerdem Zugang zu diesen gemeinsam genutzten Verzeichnissen auf Unternehmensservern. In diesem Szenario können die Daten nur mithilfe von **serverseitiger Sicherheitssoftware** geschützt werden.

Die Anti-Ransomware-Funktionalität von Kaspersky Lab steht deshalb nicht nur für Endpoints, sondern auch für Windows-Server zur Verfügung. Kaspersky Security for Windows Server besitzt eine neuartige Schutzschicht, die speziell für die Abwehr von Bedrohungen durch Cryptor-Software entwickelt wurde. Durch Überwachung von benutzerdefinierten Datenverzeichnissen, darunter auch Dateifreigaben, **vergleicht unsere Lösung den Inhalt aller Dateien**, bevor und nachdem auf sie zugegriffen wurde. Natürlich bedeutet der Eingriff eines Cryptolockers eine erhebliche Änderung des Dateiinhalts – schließlich wird dieser verschlüsselt! Unser Mechanismus entdeckt also zuverlässig die Aktivitäten von Ransomware und blockiert ihre weitere Ausführung.




Zusätzlich zur **Erkennung** gibt es in Kaspersky Security for Windows Server einen Mechanismus zur Verhinderung von Ransomware-Angriffen. Obwohl die SMB/CIFS-Protokolle uns keine Informationen über die Prozesse auf dem Ransomware-Host liefern, erfahren wir aus ihnen zumindest die IP-Adresse des Hosts. Unsere **Host-Blocker**-Technologie verhindert dann, dass dieser infizierte Host in irgendeiner Art und Weise auf die freigegebenen Verzeichnisse zugreifen kann.

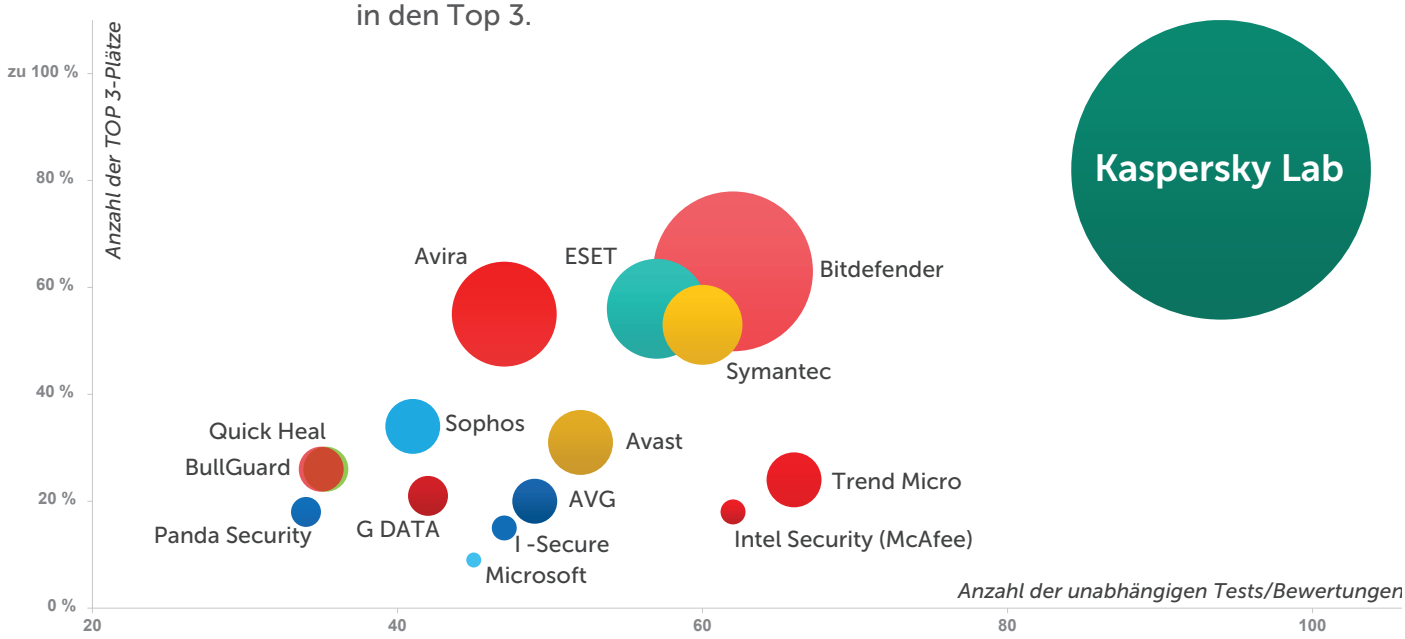
Das Verschlüsseln von Verzeichnissen auf einigen Servern kann durchaus Teil der normalen Sicherheitsstrategie eines Unternehmens sein. Bei Kaspersky Security for Windows Server **kann der Administrator Ausnahmen** für Verzeichnisse festlegen, in denen Verschlüsselungsvorgänge planmäßig stattfinden sollen.

# Alle Hebel in Bewegung setzen – Schutz vor Ransomware mit Kaspersky Lab

Da sich die Bedrohungslandschaft ständig weiterentwickelt, hat es sich Kaspersky Lab zur Aufgabe gemacht, mit jeder neuen Generation von Malware Schritt zu halten und mehrstufige Sicherheitskonzepte zum Schutz unserer Kunden bereitzustellen. Wir sind in der Lage, die Bedrohung durch Ransomware sowohl auf Workstations (Kaspersky-Aktivitätsmonitor) als auch auf Servern (Anti-Ransomware-Technologie in Kaspersky Security for Windows Server) zu entschärfen.

Kaspersky Lab erneuert laufend sein Arsenal von Schutztechnologien, die auf unserer umfassenden Sicherheitsexpertise beruhen. Hinzu kommt, dass die von uns behauptete Leistungsfähigkeit unserer Lösungen immer wieder durch unabhängige Testergebnisse und das Urteil von Branchenanalysten (TOP3) bestätigt wird.

2015 haben die Produkte von Kaspersky Lab an 94 unabhängigen Tests und Bewertungen teilgenommen. Unsere Produkte waren 60 Mal auf Platz 1 und 77 Mal in den Top 3.




Vollständige Angaben zur TOP3-Metrik finden Sie hier [www.kaspersky.com/top3](www.kaspersky.com/top3)