SOPHOS
Security made simple.

DIE BESTEN TIPPS ZUM SCHUTZ VOR RANSOMWARE

Unternehmen jeder Größe werden zunehmend durch Ransomware-Angriffe bedroht. Wenn nicht mehr auf wichtige Daten zugegriffen werden kann und dann auch noch eine Lösegeldforderung gestellt wird, ist das Chaos in vielen Unternehmen perfekt und an produktives Arbeiten kaum noch zu denken.

Aber wie läuft ein solcher Angriff normalerweise ab? Und welche Lösungen sollten für eine bestmögliche Abwehr vorhanden sein?

In diesem Whitepaper erklären wir, welche Verfahren zur Übertragung von Ransomware eingesetzt werden, beschäftigen uns mit der Frage, warum Ransomware-Angriffe erfolgreich sind, und geben Ihnen Sicherheitstipps zum Schutz vor Ransomware. Außerdem stellen wir Ihnen eine Reihe von Sicherheitstechnologien vor, die in keiner IT-Umgebung fehlen sollten.

Sophos-Whitepaper Januar 2017

Ransomware – eine kurze Einführung

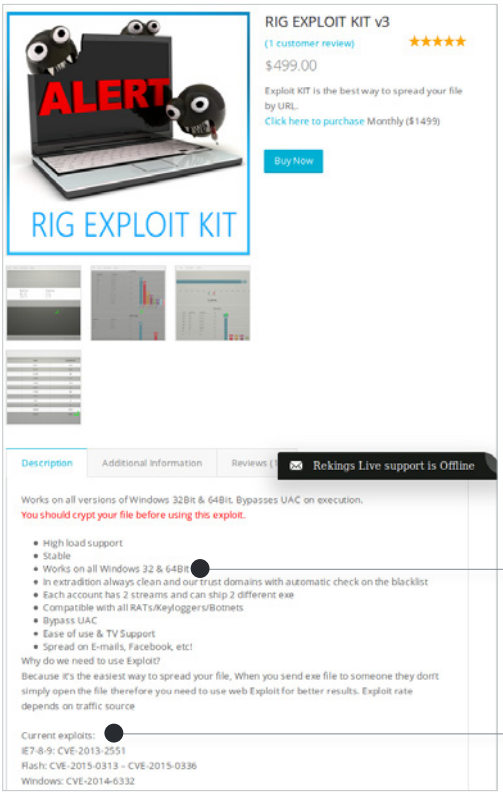
Ransomware ist eine der am meistverbreiteten und gefährlichsten Bedrohungen für Internetbenutzer. 2013 tauchte der berühmt-berüchtigte CryptoLocker auf, und seitdem haben wir es mit einer neuen Ära dateiverschlüsselnder Ransomware-Varianten zu tun, die durch Spam-Mails und Exploit-Kits eingeschleust werden, um von Privatpersonen und Unternehmen Geld zu erpressen.

Die aktuelle Angriffswelle durch Ransomware-Familien hat ihren Ursprung in den Anfangstagen von FakeAV und ist durch die „Locker"-Varianten geprägt – die heutigen Varianten sind auf die Verschlüsselung von Dateien spezialisiert. Alle Kategorien von Schadsoftware haben ein Ziel – von den Opfern durch Social Engineering und direkte Einschüchterung Geld zu erpressen. Die Lösegeldforderungen sind mit jedem erneuten Auftauchen aggressiver geworden.

Warum ist Ransomware so erfolgreich?

Die meisten Unternehmen haben eine Sicherheitssoftware installiert. Warum gelingt es Ransomware trotzdem, auf Systeme zu gelangen?

1. **Raffinierte Angriffstechniken und kontinuierliche Innovation**
   - Sofort einsatzbereite „Malware as a Service (MaaS)"-Programme werden mittlerweile vielerorts angeboten. Mit ihnen ist es ganz einfach, einen Angriff von Anfang bis Ende durchzuführen und aus diesem finanziellen Profit zu schlagen – selbst für weniger technisch versierte Kriminelle. Unten sehen Sie ein zum Kauf angebotenes MaaS-Programm.



Beinhaltet Netzwerk- und Endpoint-Techniken – vom Infizieren einer Website bis zur Bereitstellung eines Endpoint-Payloads und dem Verkauf der Ergebnisse.

Plattformübergreifend und nach der Agile-Methode entwickelt.

Exploits automatisch enthalten.

- Damit der Benutzer die Ransomware installiert, kommen geschickte Social-Engineering-Tricks zum Einsatz. Sie könnten zum Beispiel eine E-Mail erhalten, deren Text in etwa wie folgt lautet:
  „Die Anforderungen meines Unternehmens finden Sie in der Datei anbei. Bitte senden Sie mir ein Angebot."
- Ransomware-Entwickler gehen sehr professionell vor. Hierzu gehört auch, dass sie nach Zahlung des Lösegelds ein funktionierendes Entschlüsselungstool zur Verfügung stellen.

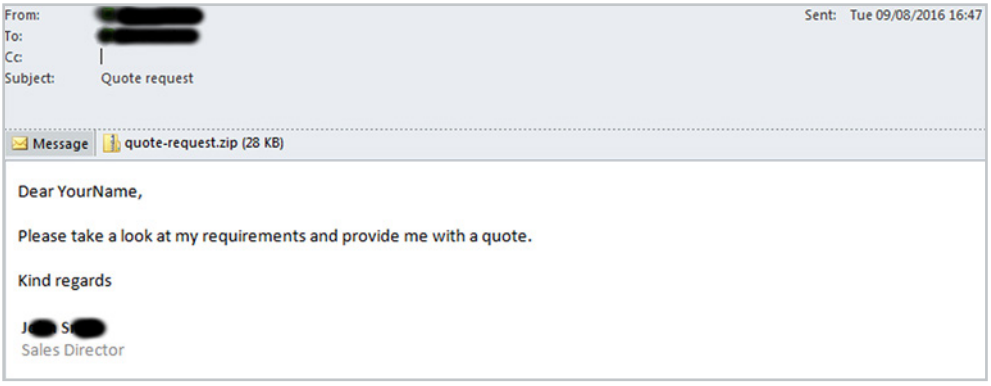
2. **Sicherheitslücken in betroffenen Unternehmen**
   - Unzureichende Back-up-Strategie (keine Echtzeit-Back-ups, Back-ups nicht offline/außerhalb des Büros).
   - Updates/Patches für Betriebssysteme und Anwendungen werden nicht schnell genug installiert.
   - Gefährliche Benutzerrechte (Benutzer arbeiten als Administratoren und/oder haben mehr Dateirechte in Netzlaufwerken als für ihre Aufgaben notwendig).
   - Unzureichende Aufklärung der Benutzer („Welche Dokumente und von wem darf ich öffnen?"
     „Was muss ich tun, wenn ich glaube, dass ein Dokument schädlich ist", „Wie erkenne ich eine Phishing-E-Mail?").
   - Sicherheitssysteme (Virenscanner, Firewalls, IPS, E-Mail-/Web-Gateways) sind nicht vorhanden oder fehlerhaft konfiguriert. Unzureichende Netzwerksegmentierung kann
     ebenfalls hier mitaufgenommen werden (Server und Workstations in demselben Netzwerk).
   - Zu wenig Erfahrung im Bereich IT-Security (.exe-Dateien in E-Mails werden eventuell blockiert, nicht jedoch Office-Makros oder sonstige aktive Inhalte).
   - Widersprüchliche Prioritäten („Wir wissen, dass diese Methode unsicher ist, aber unsere Angestellten müssen ihre Arbeit erledigen können …).
3. **Nicht genügend leistungsstarke Prevention-Technologien**
   - In den meisten Unternehmen ist eine Sicherheitssoftware vorhanden.
   - Ransomware wird kontinuierlich weiterentwickelt, um diese Sicherheitssoftware auszuhebeln und deren Funktionen zu überlisten. Sie löscht sich beispielsweise nach dem Verschlüsseln von Dateien so schnell selbst, dass sie nicht analysiert werden kann.
   - Lösungen müssen speziell zur Abwehr solcher Ransomware-Techniken ausgelegt sein.

Wie läuft ein Ransomware-Angriff ab?

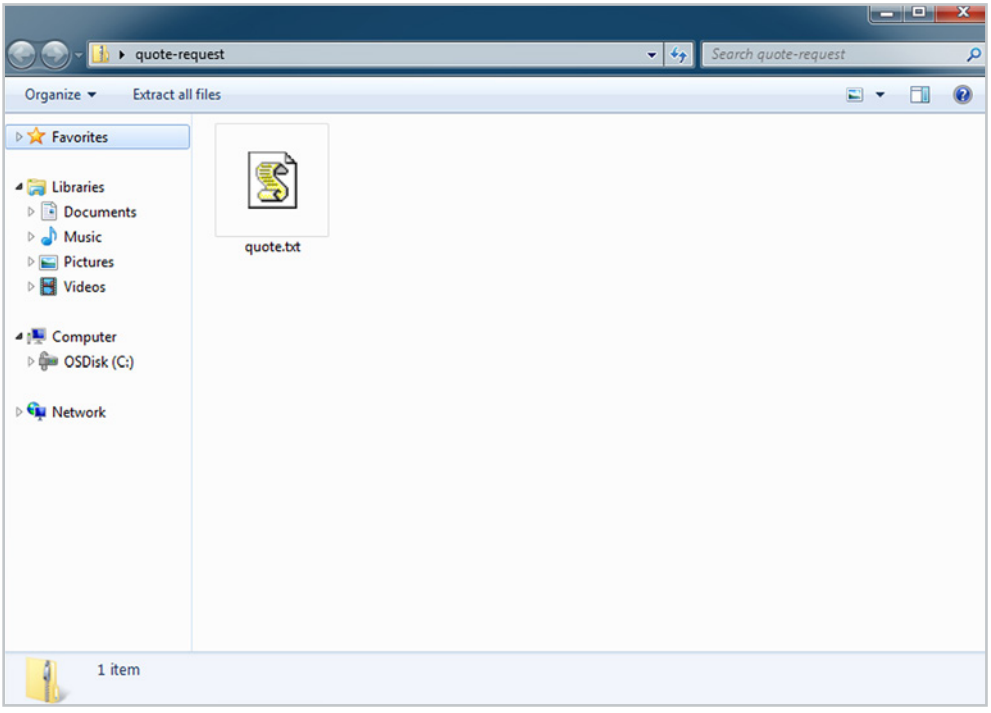
Ransomware-Angriffe beginnen entweder mit einem schädlichen E-Mail-Anhang oder über eine kompromittierte (oft seriöse Mainstream-) Website.

Schad-E-Mails

Kriminelle erstellen heutzutage Schad-E-Mails, die sich von echten E-Mails nicht mehr unterscheiden lassen. Sie sind grammatikalisch korrekt, enthalten keine Rechtschreibfehler und ihr Text ist gezielt auf Sie und Ihr Unternehmen abgestimmt.



Beim Öffnen scheint der ZIP-Ordner eine ganz normale Textdatei zu enthalten.



Wird die Datei jedoch ausgeführt, wird die Ransomware heruntergeladen und auf Ihrem Computer installiert. In diesem Beispiel handelt es sich um eine JavaScript-Datei, die als Textdatei getarnt wurde, aber tatsächlich ein Trojaner ist. Es gibt jedoch noch viele weitere Varianten von Schad-E-Mails, z. B. angehängte Word-Dokumente mit Makros und Verknüpfungsdateien (.lnk).

Schad-Websites

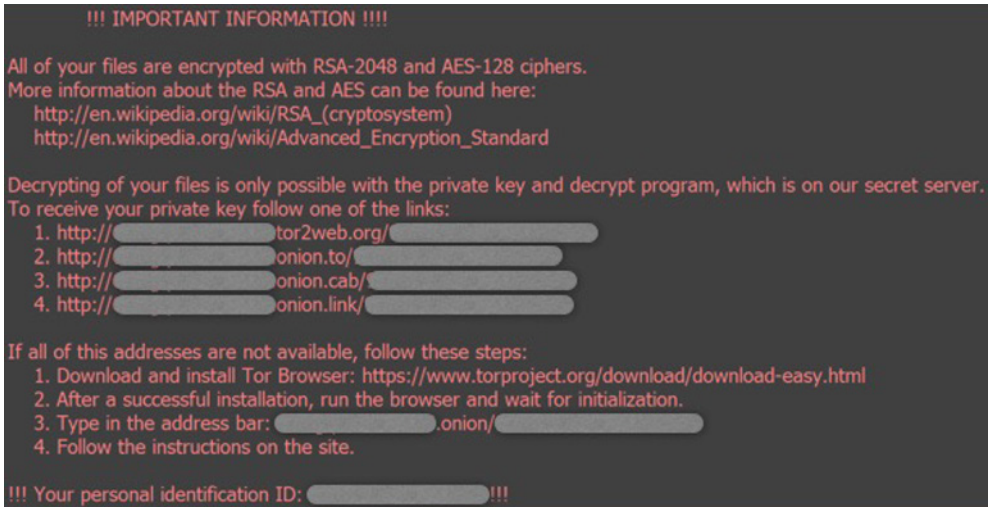
Ein weiterer Infektionsweg ist häufig der Besuch einer seriösen Website, die mit einem Exploit-Kit infiziert wurde. Selbst beliebte Mainstream-Websites können zeitweise kompromittiert sein. Exploit-Kits sind Schwarzmarkt-Tools, mit denen Hacker bekannte und unbekannte Schwachstellen (z. B. Zero-Day-Exploits) ausnutzen.

Sie browsen zur gehackten Website und klicken auf einen harmlos erscheinenden Link, fahren mit der Maus über eine Werbeanzeige oder sehen sich die Seite in vielen Fällen nur an. Das reicht schon, um die Ransomware-Datei auf Ihren Computer herunterzuladen und auszuführen – oft ohne sichtbare Anzeichen, bis es zu spät ist.

Was geschieht als Nächstes?

Nachdem die Ransomware per E-Mail oder über das Internet auf einen Computer gelangt ist, unternimmt sie weitere Schritte:

- Sie nimmt Kontakt zum Command-and-Control-Server des Angreifers auf, sendet Informationen über den infizierten Computer und lädt einen individuellen öffentlichen Schlüssel für diesen herunter.
- Bestimmte Dateitypen (die je nach Art der Ransomware variieren) wie Office-Dokumente, Datenbankdateien, PDFs, CAD-Dokumente, HTML, XML usw. sind auf dem lokalen Computer, auf Wechselmedien und in allen zugänglichen Netzlaufwerken verschlüsselt.
- Automatische Back-ups des Windows-Betriebssystems (Schattenkopien) werden regelmäßig gelöscht, um eine Datenwiederherstellung zu verhindern.
- Auf dem Desktop erscheint eine Nachricht, in der dazu aufgefordert wird, in einem bestimmten Zeitraum ein Lösegeld zu begleichen (meist in Bitcoins).



- Schlussendlich löscht die Ransomware sich selbst und hinterlässt die verschlüsselten Dateien sowie eine Lösegeldforderung.

Neun Sicherheitsmaßnahmen, die Sie am besten gleich ergreifen sollten

Um vor Ransomware geschützt zu bleiben, benötigen Sie nicht nur die neuesten Sicherheitslösungen. Auch IT Security Best Practices wie regelmäßige Mitarbeiterschulungen sind unerlässlich. Befolgen Sie unbedingt die folgenden neun Best Practices:

1. **Fertigen Sie regelmäßig Back-ups an und verwahren Sie diese offline und außerhalb des Büros**

Ransomware ist nur eine Gefahr von vielen: Ihre Daten können auf diverse andere Arten abhanden kommen: z. B. durch Feuer, Hochwasser, Diebstahl, Beschädigung eines Laptops oder versehentliches Löschen. Verschlüsseln Sie Ihre Back-ups, damit Ihre Daten auch dann sicher bleiben, wenn Ihr Back-up-Gerät in die falschen Hände gerät.

2. **Aktivieren Sie Dateierweiterungen**

Dateierweiterungen sind in Windows standardmäßig deaktiviert und nur über die Dateiminiaturansicht ersichtlich. Bei aktivierten Dateierweiterungen können Sie Dateitypen, die normalerweise nicht an Sie und Ihre Benutzer gesendet werden (z. B. JavaScript), einfach erkennen.

3. **Öffnen Sie JavaScript (.JS)-Dateien in Notepad**

Wenn Sie eine JavaScript-Datei in Notepad öffnen, können keine Schad-Skripte ausgeführt werden und Sie können den Inhalt der Datei überprüfen.

4. **Aktivieren Sie keine Makros in Dokumentanhängen, die Sie per E-Mail erhalten**

Microsoft hat die automatische Ausführung von Makros schon vor Jahren aus Sicherheitsgründen deaktiviert. Viele Infektionen funktionieren nur, wenn Sie Makros aktivieren. Aktivieren Sie also keine Makros!

5. **Vorsicht bei Attachments, die Ihnen unaufgefordert zugesendet werden**

Cyberkriminelle machen sich das Dilemma zunutze, dass Sie erst dann mit Sicherheit sagen können, ob ein Dokument seriös ist, nachdem Sie es geöffnet haben. Lassen Sie im Zweifel lieber die Finger von einem Attachment, das Ihnen verdächtig erscheint.

6. **Beschränken Sie Ihre Anmelderechte auf das Nötigste**

Bleiben Sie nur so lange wie wirklich nötig mit Administratorrechten angemeldet und vermeiden Sie in diesem Zeitraum Surfen, das Öffnen von Dokumenten und andere reguläre Arbeitsschritte.

7. **Ziehen Sie die Installation von Microsoft Office Viewern in Betracht**

Mit diesen Viewer-Anwendungen können Sie sich den Inhalt von Dokumenten anzeigen lassen, ohne sie in Word oder Excel zu öffnen. Die Viewer-Software unterstützt keine Makros. Es besteht also keine Gefahr, Makros versehentlich zu aktivieren.

8. **Installieren Sie Patches zeitig und regelmäßig**

Malware, die nicht über ein Dokument eingeschleust wird, ist meist auf Sicherheits-Bugs in beliebten Anwendungen wie Microsoft Office, Browsern oder Flash angewiesen. Je eher Sie Patches installieren, desto weniger Schwachstellen können ausgenutzt werden.

9. **Halten Sie die Sicherheitsfunktionen in Ihren Geschäftsanwendungen aktuell**

In Office 2016 gibt es beispielsweise nun das Steuerelement „Ausführung von Makros in Office-Dateien aus dem Internet blockieren", mit dem Sie sich vor externen Schadinhalten schützen und Makros intern weiterhin nutzen können.

Mit diesen Schutztechnologien bleiben Sie vor Ransomware geschützt

Um Ransomware zuverlässig abwehren zu können, müssen Sie für *jede* Phase eines Angriffs effektive Abwehrmaßnahmen ergreifen. Beginnen Sie auf Ihren Endpoints mit unserer einmaligen CryptoGuard-Technologie in Sophos Intercept X, die Ransomware stoppt, bevor es zu spät ist. CryptoGuard ist auf Ihren Endpoints und Servern aktiv und erkennt und stoppt Dateiverschlüsselungen durch Ransomware. Es ergänzt Ihre bestehende Sicherheit und blockiert Prozesse, die versuchen, unbefugte Änderungen an Ihren Daten vorzunehmen.

E-Mail-Bedrohungen stoppen

Die beste Waffe gegen Schad-E-Mails ist Ihr E-Mail-Gateway. Anti-Spam-Technologien stoppen Ransomware-E-Mails. Antivirus scannt auf E-Mail-Bedrohungen und blockiert diese. Durch das Blockieren von E-Mails mit Makro-Attachments können Sie einer weiteren weitverbreiteten Ransomware-Technik vorbeugen. Die Time-of-Click-Technologie verhindert, dass Sie und Ihre Benutzer zu infizierten Websites navigieren – auch wenn diese noch unbedenklich waren, als sie in Ihren Posteingang gelangten.

Web-Bedrohungen stoppen

Web-Bedrohungen werden von der Firewall und dem Web-Gateway neutralisiert. Eine URL-Filterung blockiert Ransomware-hostende Websites sowie deren Command-and-Control-Server. Mittels Durchsetzung strenger Kontrollen können Sie zudem dafür sorgen, dass mit Ransomware in Verbindung stehende Dateien gar nicht erst heruntergeladen werden.

Cloud Sandboxing sowohl auf E-Mail- und Web-Gateway-Ebene blockiert komplexe Zero-Day-Bedrohungen wie Ransomware. Diese Technologie können Sie sich als Ihr eigenes privates Malware-Labor vorstellen, in dem verdächtige Dateien ausgeführt werden, um ihr Verhalten zu analysieren.

Server schützen

Server Whitelisting und Lockdown sorgen dafür, dass Ihre Server sicher bleiben – zugelassene Anwendungen werden auf eine Whitelist gesetzt und Änderungen und Updates nur eingeschränkt erlaubt. Alle anderen Versuche, Änderungen vorzunehmen, werden automatisch blockiert. Ransomware wird daher bereits gestoppt, bevor sie aktiv werden kann. Malicious Traffic Detection verhindert, dass Ransomware Command-and-Control-Server kontaktiert und seinen Payload herunterlädt.

Security Heartbeat

Ihre Sicherheitsprodukte sind für sich genommen zwar durchaus leistungsfähig, sollten für eine optimale Leistung jedoch zusammenarbeiten können. Wenn Sie Ihren Endpoints und Ihrer Firewall ermöglichen, Sicherheitsinformationen auszutauschen und proaktiv auf Bedrohungen zu reagieren, erhalten Sie besseren Schutz vor komplexen Bedrohungen als je zuvor.

Befolgen Sie beim Einsatz Ihrer Sophos-Lösungen unsere Best Practices:
www.sophos.com/kb/120797

Kostenlose Testversion unter
www.sophos.de/free-trials

Mehr als 100 Millionen Anwender in 150 Ländern vertrauen auf Sophos. Wir bieten den besten Schutz vor komplexen IT-Bedrohungen und Datenverlusten. Unsere umfassenden Sicherheitslösungen sind einfach bereitzustellen, zu bedienen und zu verwalten. Dabei bieten sie die branchenweit niedrigste Total Cost of Ownership. Das Angebot von Sophos umfasst preisgekrönte Verschlüsselungslösungen, Sicherheitslösungen für Endpoints, Netzwerke, mobile Geräte, Server, E-Mails und Web. Dazu kommt Unterstützung aus den SophosLabs, unserem weltweiten Netzwerk eigener Analysezentren. Weitere Informationen unter www.sophos.de.

Sales DACH (Deutschland, Österreich, Schweiz):
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2016-09-08 WP-DE (RP)