TRUST IN GERMAN SICHERHEIT

G DATA TechPaper

Ransomware

G DATA Software AG | Juni 2017

Inhalt

Einleitung

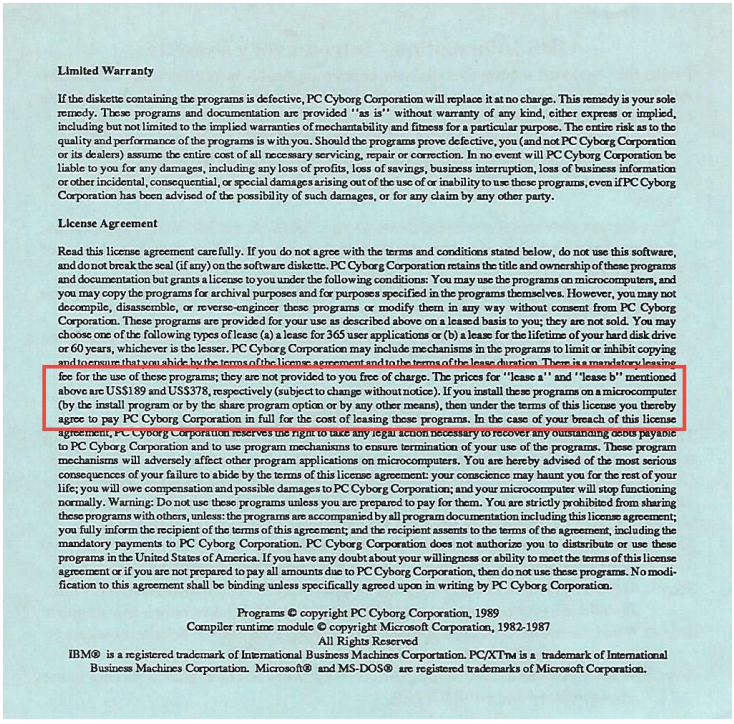
Ransomware ist zu einer der größten Malware-Bedrohungen Zuhause und im Büro geworden. Mit mehr als 4.000 täglichen Ransomware-Angriffen und einer erwarteten Verdopplung für 2017 war das Risiko, persönliche Dateien, Geschäftspläne oder Kundeninformationen zu verlieren, nie größer[1]. In diesem Dokument wird zur Verhinderung von Ransomware-Infektionen erklärt, was Ransomware ist und wie Infektionen verhindert werden.

1. Was ist Ransomware?

Eigentlich ist Ransomware nur eine weitere Form von schädlicher Software, so genannte Malware. Für ihre Opfer unterscheidet sie sich jedoch maßgeblich durch eine wichtige Eigenschaft von anderer Malware. Während reguläre Malware Geräte infiziert, um sie als Teil eines Botnets zu verwenden oder Kreditkarteninformationen zu stehlen, versuchen die Entwickler von Ransomware, den Benutzer direkt zu erpressen, um an Geld zu kommen. Für den Erhalt eines Lösegeldes (engl. „ransom“) sperrt die Ransomware das Gerät oder verschlüsselt sogar die Daten, bis das Opfer zahlt.

1.1. Verlauf

In den letzten Jahren hat Ransomware in vielen hochkarätigen Fällen Schlagzeilen gemacht. Private Benutzer, kleine Unternehmen, große Konzerne – jeder wurde zum Opfer von Ransomware-Angriffen. Es ist jedoch kein neues Phänomen: Die Geschichte von Ransomware lässt sich bis in die späten 1980er zurückverfolgen. Im Winter 1989 wurden über 10.000 mit Ransomware befallene Floppy-Disketten an medizinische Einrichtungen, Forscher und private Haushalte verteilt. Die Disketten enthielten eine Software, die Informationen über AIDS anbot. Stattdessen wurden kriminelle Methoden angewendet, um die Endnutzervereinbarung zu erzwingen. Indem der PC gesperrt und Dateien „verschlüsselt“ wurden, versuchte der Autor eine Zahlung von 189 $ zu erhalten, die an ein Postfach in Panama geschickt werden sollte. Doch die AIDS-Ransomware war eigentlich nicht besonders ausgeklügelt: Dateien und Programme



Limited Warranty

If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of mechantability and fitness for a particular purpose. The entire risk as to the quality and performance of the programs is with you. Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, loss of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

License Agreement

Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement; and the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation does not authorize you to distribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

Programs © copyright PC Cyborg Corporation, 1989
Compiler runtime module © copyright Microsoft Corporation, 1982-1987
All Rights Reserved
IBM® is a registered trademark of International Business Machines Corporation. PC/XT™ is a trademark of International Business Machines Corporation. Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

Abbildung 1: AIDS-Lizenzvereinbarung

[1] Quelle US-amerikanisches Justizministerium, Abteilung für Computerkriminalität und geistiges Eigentum (CCIPS); BBR Services.

konnten mithilfe eines speziell entwickelten Gegenmittels wiederhergestellt werden. Erst 1996 beschrieben Forscher das erste Mal das Konzept der Kryptovirologie, bei der Kryptografie mit öffentlichem Schlüssel offensiv verwendet wird[2]. Danach dauerte es etwa zehn Jahre, bis die erste in Massen verteilte Ransomware mit tatsächlicher Verschlüsselung auftauchte, wie z. B. 2005 der PGPCoder oder 2006 die Ransomware „Archiveus“. Obwohl einige Arten von Ransomware nach wie vor nur den PC sperrten und sich in manchen Fällen als Strafverfolgungsbehörde ausgaben, wurde Ransomware mit Verschlüsselung schnell zur verbreitetsten Art.

1.2. Ransomware in der heutigen Zeit

Mit fortschreitender Forschung in der Kryptografie verbesserten Kriminelle ihre Raffinesse. Obwohl Ransomware, die den PC sperrt, bei Entfernung keinen dauerhaften Schaden anrichtet, bedeuten die zusätzlichen Dateiverschlüsselungsfunktionen, dass selbst bei Entfernung der Ransomware nicht auf die betroffenen Dateien zugegriffen werden kann. Aktuelle Ransomware beruht auf geheimen Schlüsseln, die nur wiederhergestellt werden können, wenn die Kriminellen bei der Implementierung Fehler gemacht haben. Deshalb müssen Ransomware-Infektionen verhindert werden, und Benutzer sowie Administratoren müssen sicherstellen, dass sie ihre Systeme nach einer Ransomware-Infektion wiederherstellen können.

Ende 2013 wurde Cryptolocker zu einer der berüchtigtsten Arten von Ransomware. Seitdem hat es sich zu einer Familie von verwandten Ransomware-Arten entwickelt. Alle diese Arten verschlüsseln die Daten auf der Festplatte des Opfers und schicken den Schlüssel an den Angreifer. Um wieder Zugriff auf Geschäftsdateien oder private Dokumente wie Fotos zu erhalten, müssen die Opfer ein Lösegeld zahlen, um den Entschlüsselungscode zu erhalten. Andere Ransomware (wie Locky, WannaCry oder Spora) unterscheiden sich in ihrer Implementierung, aber das Grundprinzip bleibt gleich. Diese verbesserte Raffinesse von Online-Kriminellen zeigt sich beim Aufwand, den sie nun betreiben, um Ransomware zu erstellen. Obgleich einige Kriminelle nur Dateien verschlüsseln und eine Lösegeldforderung anzeigen, schaffen andere eine komplette Infrastruktur mit Website-Portal, Chat-System und mehreren Zahlungsoptionen einschließlich vollständiger Entschlüsselung, Immunität oder Entfernung.

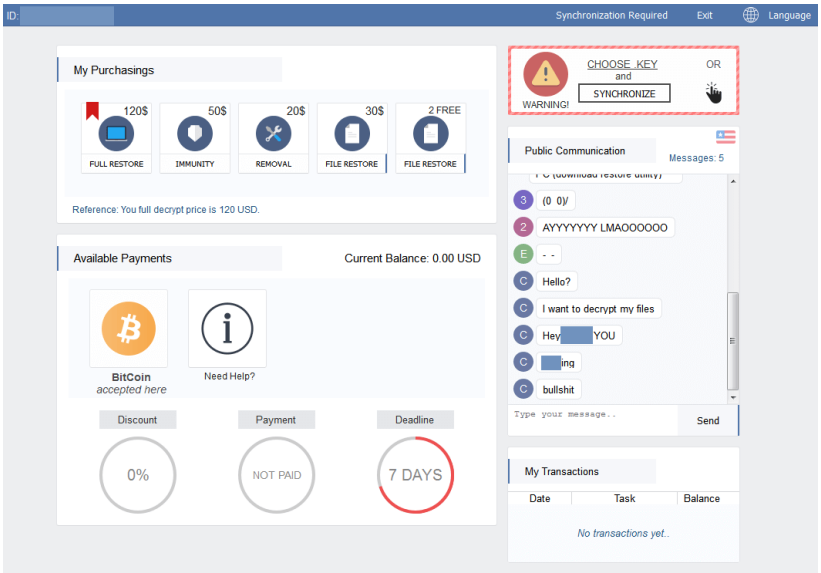


Abbildung 2: Spora-Portal mit Support-Chat

[2] Quelle Adam Young und Moti Yung: *Cryptovirology: Extortion-Based Security Threats and Countermeasures.* IEEE (1996).

1.3. Verteilung und Opfer

Ransomware wird wie jede andere Malware verteilt. Dazu gehören:

- Spam mit Anhang oder einem Download-Link
- Kompromittierte Webseiten
- Schädliche Ad-Netzwerke

Obwohl Sicherheitsexperten und Systemadministratoren seit Jahren Endbenutzer warnen, nicht auf verdächtige Links oder Anhänge zu klicken, bleibt Spam der wichtigste Infektionsvektor. Ransomware versteckt sich oftmals in makrofähigen Textdokumenten, jedoch können die ausführbaren Dateien theoretisch in jedem anfälligen Anhang enthalten sein. Neben Spam werden häufig kompromittierte Webseiten zur Verteilung von Ransomware verwendet. Und selbst Websites, die an sich nicht angegriffen wurden, könnten Ransomware verteilen, wenn sie Code von Ad-Netzwerken enthalten, die Werbeanzeigen unzureichend überprüfen.

Kriminelle zielen nicht auf bestimmte Unternehmen oder Privatbenutzer ab, stattdessen verteilen sie die Ransomware über so viele Kanäle wie möglich. Da die Verteilungsmethoden eine große Anzahl von Opfern betreffen, ist das Risiko, Ransomware zum Opfer zu fallen, sehr hoch. Es ist unwichtig, ob das Opfer ein Unternehmen oder ein Endbenutzer ist, da beide gleichermaßen das Lösegeld zahlen, wenn wichtige Daten verschlüsselt wurden. Im Übrigen könnte die Auswirkung für einige Unternehmen größer sein als für andere. Beispielsweise waren Krankenhäuser stark von Ransomware betroffen. Mögliche Ursachen sind relativ veraltete IT-Infrastrukturen, der zeitkritische Zugriff auf empfindliche Daten und die Anzahl der verbundenen Geräte[3].

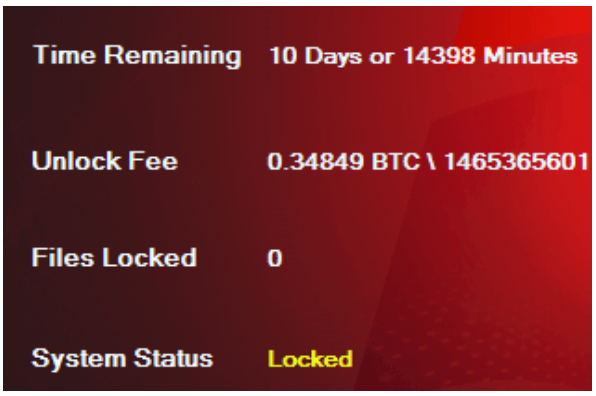


Abbildung 3: Manamecrypt zeigt einen Countdown an, um die Opfer unter Druck zu setzen.

Ransomware verwendet nicht nur die neueste Technologie zur Maximierung ihrer Effektivität. Kriminelle wenden auch verhaltensbezogene Tricks an, um Benutzer zur Zahlung zu drängen. Als wenn die Verschlüsselung von wichtigen Daten nicht genug wäre, wird der Druck auf Opfer erhöht, indem eine zeitliche Begrenzung angezeigt wird. Viele Arten von Ransomware drohen, mit dem Löschen von Dateien oder Entschlüsselungscodes zu beginnen, wenn die Forderungen nicht innerhalb eines bestimmten Zeitraums erfüllt werden. Bei einer Art von Ransomware können Benutzer Dateien kostenlos entschlüsseln, wenn sie die Ransomware an andere Leute weiterleiten.

[3] Quelle: https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

1.4. Geschäftsmodell

Der offensichtliche Grund für die zunehmende Verteilung von Ransomware ist der direkte finanzielle Gewinn für Online-Kriminelle. Es gibt jedoch mehrere Faktoren, die diese Zunahme erst möglich machen und zu einem tatsächlichen Geschäftsmodell hinter Ransomware geführt haben. Zunächst können Kriminelle durch das Aufkommen alternativer Währungen Geld fordern, während sie anonym bleiben. Viele Arten von Ransomware akzeptieren Bitcoin-Zahlungen, eine Krypto-Währung, die kein traditionelles Bankkonto erfordert. Andere nutzen Zahlungsbelege oder leiten Zahlungen über mehrere Dienste weiter, um ihre Identität zu verschleiern. Des Weiteren ist die Technologie hinter Ransomware zu einer Ware geworden. Kriminelle müssen nicht mehr ihre eigenen Verschlüsselungsmethoden entwickeln; sie können angebotene Ransomware nutzen, die einsatzbereit auf Schwarzmärkten erhältlich ist. Das bedeutet, dass nur wenig investiert werden muss, um ein Ransomware-Geschäft einzurichten. Letztlich ist die Ransomware-Infrastruktur sehr flexibel, was die Bemühungen von Strafverfolgungsbehörden auf der Suche nach Verteilungs- und Zahlungsservern erschwert. Die Wahrscheinlichkeit, erwischt zu werden, ist somit relativ gering. Diese Faktoren schaffen zusammen ein Geschäftsmodell, mit dem Kriminelle schnell eine Ransomware-Kampagne einrichten und mit geringen Kosten eine Vielzahl von Benutzern angreifen können.

2. Schutz gegen Ransomware

Für viele Benutzer ist die erste Antwort auf eine Ransomware-Infektion die Zahlung des Lösegeldes. Denn die Zahlung des Lösegeldes bedeutet doch, dass man seine Dateien zurückbekommt, oder? Leider ist das nicht immer der Fall. Zunächst gibt es keine Garantie, dass Kriminelle tatsächlich die Dateien entschlüsseln, nachdem sie die Zahlung erhalten haben. Da die Zahlungen nicht verfolgt werden können, gibt es keine Möglichkeit, eine Erstattung zu erhalten, wenn nur einige (oder auch keine) Dateien entschlüsselt werden. Und selbst, wenn Dateien entschlüsselt werden, verbleibt die Ransomware auf dem Computer. Man kann nicht wissen, ob Dateien zu einem späteren Zeitpunkt wieder verschlüsselt werden und erneut ein Lösegeld gefordert wird. Schließlich ist für Kriminelle die Wahrscheinlichkeit größer, dass ein bestimmter Benutzer, der bereits einmal das Lösegeld gezahlt hat, dies auch ein zweites Mal tut, wenn er ihn erneut erpresst, anstatt zufällig andere Benutzer anzugreifen. Letztlich führt die Zahlung des Lösegeldes nur dazu, dass sich Kriminelle bestätigt fühlen und die Verteilung von Ransomware fortsetzen.

2.1. Anti-Ransomware

Der beste Schutz gegen Ransomware ist sicherzustellen, dass das System erst gar nicht infiziert werden kann. Dafür wird die Verwendung einer Sicherheitslösung mit dedizierter Anti-Ransomware empfohlen. Neben der standardmäßigen signaturbasierten Erkennung muss Sicherheitssoftware in der Lage sein, bestimmte Ransomware-Aktionen wie Dateiverschlüsselung zu erkennen und sie zu blockieren, bevor sie Schaden anrichten können.

2.2. Patches

Neben einem spezifischen Ransomware-Schutz sollten Privathaushalte und Unternehmen sicherstellen, dass ihr Betriebssystem und alle Anwendungen auf dem neuesten Stand sind. Das bedeutet, dass regelmäßig auf Patches geprüft werden muss und alle zutreffenden Patches installiert werden müssen. In Privathaushalten muss unter Windows Update die automatische Installation von Sicherheitsupdates aktiviert sein. Bei geschäftlichen Benutzern mit mehreren zu verwaltenden Endpunkten muss ein Patch-Management-Konzept mit der Unterstützung einer Patch-Management-Software sicherstellen, dass Administratoren wissen, wann neue Patches verfügbar sind, und dass sie sie effizient und automatisch bereitstellen können.

2.3. Datensicherung

Da Ransomware auf der Verweigerung des Zugriffs auf eigene Dateien beruht, kann es bei einer Infektion sehr hilfreich sein, immer eine Sicherung dieser Dateien zu haben. Es wird empfohlen, regelmäßig Sicherungen aller wichtigen Dateien zu erstellen. Zur Verhinderung, dass Ransomware Originaldateien und ihre Sicherungen verschlüsselt, müssen sich die Sicherungen auf einem externen Speichermedium befinden, das in der Regel nicht mit dem Computer verbunden ist. Private Benutzer könnten ihre Dateien beispielsweise durch Sicherung mithilfe eines Cloud-Dienstes oder einer externen Festplatte schützen. Für Netzwerkadministratoren könnte eine zentrale Sicherungslösung dabei helfen, wichtige Dokumente von allen Endpunkten auf einem zentralen Server zu sichern.

2.4. Bewusstsein

Zur Verhinderung von Ransomware-Infektionen müssen technische Maßnahmen durch die Aufklärung der Benutzer ergänzt werden. Bei der Nutzung von E-Mails sollten beispielsweise Anhänge nur geöffnet werden, wenn die E-Mail von einer vertrauenswürdigen Person stammt und wenn es sich durch den Kontext ergibt, dass die Person einen Anhang schickt. Gleichermaßen müssen Links in E-Mails mit Vorsicht genutzt werden, da viele Online-Kriminelle ihre Spam-Nachrichten mit Links verschicken, die auf eine mit Malware gefüllte Website weiterleiten.

3. So schützt G DATA gegen Ransomware

Lösungen von G DATA bieten einen umfassenden Schutz gegen Ransomware, sowohl für private als auch geschäftliche Benutzer. Alle unsere Lösungen enthalten ein dediziertes AntiRansomware-Modul, das besonders gegen Malware schützt, die versucht, Dateien zu verschlüsseln. Für geschäftliche Benutzer kann dieses Modul zentral mithilfe von G DATA Administrator verwaltet werden. Geschäftliche Benutzer müssen sicherstellen, dass eine umfassende Patch-Management-Richtlinie in Kraft ist, die durch

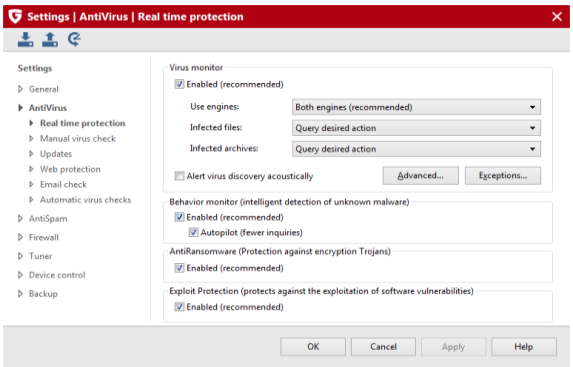


Abbildung 4: AntiRansomware ist in jeder G DATA Lösung enthalten.

G DATA Patch Management unterstützt werden kann. Dabei handelt es sich um ein optionales Modul für alle G DATA Geschäftslösungen. Für den Schutz von wichtigen Dateien vor jeglichem Datenverlust können private Benutzer G DATA Internet Security oder G DATA Total Security für regelmäßige Datensicherungen verwenden. Unsere Geschäftslösungen enthalten Sicherungsfunktionen als optionales Modul. Weitere Informationen über Lösungen von G DATA für private und geschäftliche Benutzer finden Sie unter www.gdata.de.