G DATA TechPaper

Ransomware

G DATA Software AG | June 2017

Contents

Introduction

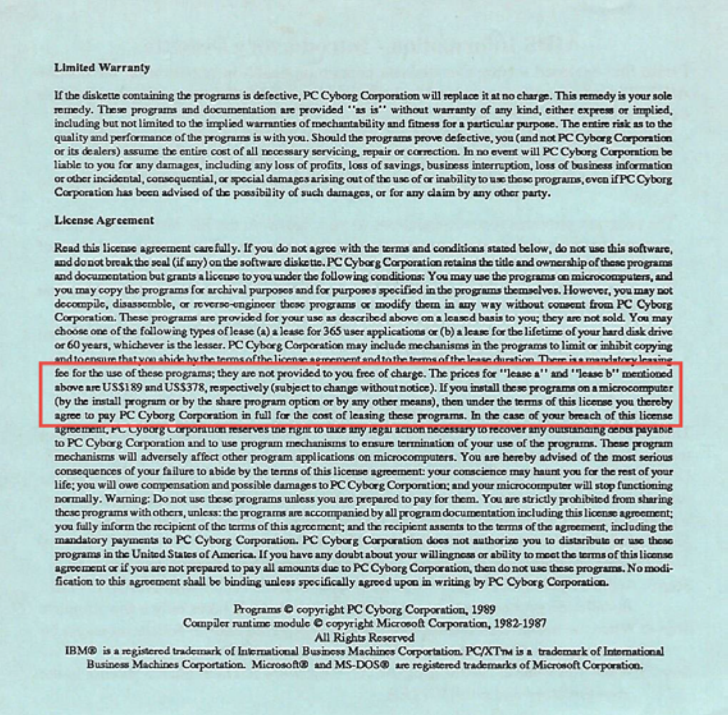
Ransomware has evolved to become one of the biggest malware threats to home and business users alike. With over 4,000 daily ransomware attacks and numbers expected to double in 2017, the risk of losing personal files, business plans or customer information is growing ever larger[1]. To help prevent ransomware infections, this paper will explain what ransomware is and how to prevent ransomware infections.

1. What is ransomware?

Technically, ransomware is just another form of malicious software. To its victims it distinguishes itself from other malware by one crucial property. Whereas regular malware infects devices to use them as part of a botnet or to steal credit card information, ransomware developers try to make money by extorting the user directly. In order to extract a ransom, ransomware locks the device or even encrypts data until the victim pays up.

1.1. History

In recent years, ransomware has made headlines in some high-profile cases. Home users, small business owners, large enterprises – everyone has become victim of ransomware attacks. But it is not a new phenomenon: its history can be traced back to the late eighties. In the winter of 1989, over 10,000 floppies containing ransomware were distributed to medical institutions, researchers as well as private individuals. The floppy contained software offering information about AIDS, as advertised, but it employed criminal methods to enforce its EULA. By locking the PC and "encrypting" files, the author tried to get users to pay $189, to be sent to a post office box in Panama. Technically, the AIDS ransomware was not very sophisticated: files and programs could be restored using a specially developed antidote. Only in 1996 did researchers first describe the concept of cryptovirology: using public-key cryptography offensively[2]. It then took about a decade for the first mass-distributed ransomware with actual encryption to appear, such as PGPCoder in 2005 or Archiveus in 2006. While some types of



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 distaribute 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 Corportation. PC/XT™ is a trademark of International Business Machines Corportation. Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

Figure 1: AIDS License Agreement

[1] Source: United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS); BBR Services.

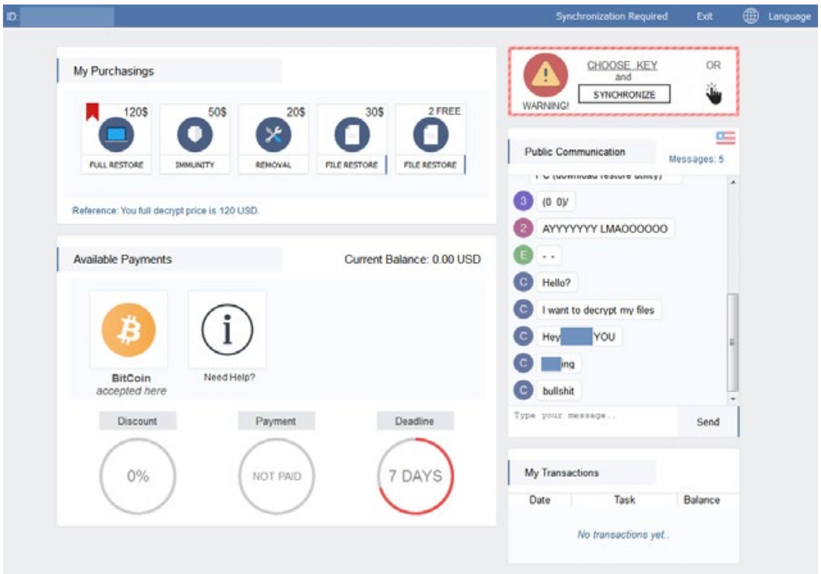
[2] Source: Adam Young and Moti Yung, Cryptovirology: Extortion-Based Security Threats and Countermeasures, IEEE (1996).

ransomware still merely locked the PC, sometimes posing as law enforcement agencies, ransomware with encryption quickly took over as the most widely distributed type.

1.2. Ransomware today

As research on cryptography progressed, criminals kept increasing their sophistication. While ransomware that locks the PC does not leave any permanent damage if removed, the inclusion of file encryption features now means that even if the ransomware is removed, the files can still not be accessed. Current ransomware relies on secret keys that can only be recovered if the criminals made any mistakes in their implementation. Ransomware infections therefore must be prevented and users and administrators must make sure that they can recover their system(s) after a ransomware infection took place.

In late 2013, Cryptolocker established itself as one of the most infamous types of ransomware. It has since developed into a family of related ransomware types. All of them have in common that they encrypt data on the victim's hard drive and send the key to the attacker. To regain access to business files or private documents, such as photos, victims need to pay a ransom in order to receive the decryption key. Other examples of ransomware, such as Locky, WannaCry or Spora, differ in their implementation but the core concept remains the same. The increased sophistication of online criminals can be observed by looking at the effort they now put into building ransomware. Although some criminals just encrypt files and show a ransom note, others build a complete infrastructure, including a website portal, chat system and multiple payment options including full decryption, immunity or removal.



Reference: You full decrypt price is 120 USD.

Current Balance: 0.00 USD

3 (0 0)/

2 AYYYYYYY LMAOOOOOO

E - -

C Hello?

C I want to decrypt my files

C Hey[redacted]YOU

C [redacted]ing

C bullshit

Date	Task	Balance
No transactions yet..		

Figure 2: Spora portal including support chat

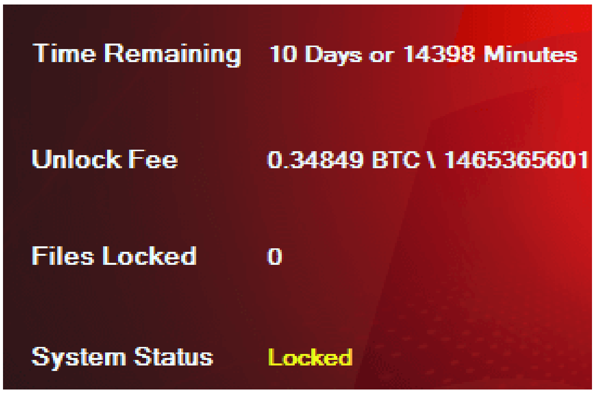
1.3. Distribution and victims

Ransomware is typically distributed like any other type of malware. This includes methods such as:

- Spam with attachment or download link
- Compromised webpage
- Malicious ad network

Even though security professionals and system administrators have been telling end users for years not to click on any suspicious links or attachments, spam remains a major infection vector. Ransomware often hides in macro-enabled text documents, but its executable files can theoretically be included in any vulnerable type of attachment. In addition to spam, compromised webpages are also often used to distribute ransomware. And even websites that have not been attacked themselves may be spreading ransomware if they include code from ad networks that insufficiently audit ads.

Criminals often do not target specific businesses or home users, but instead choose to distribute the ransomware through as many channels as possible. Because its distribution methods cover a large number of possible victims, the risk of being targeted by ransomware is high. It does not matter whether the victim is a business or end user, because both are very likely to pay the ransom if important data have been encrypted. That being said, for some businesses the impact can be larger than for others. For example, hospitals have been heavily affected by ransomware. Likely reasons include the relative age of IT infrastructure, time-critical access to sensitive data and the number of connected devices[3].



Time Remaining 10 Days or 14398 Minutes

Unlock Fee 0.34849 BTC \ 1465365601

Files Locked 0

System Status Locked

Figure 3: Manamecrypt displays a countdown timer to pressure its victims.

Ransomware does not only use the latest technology to maximize its effectivity. Criminals have also implemented behavioral tricks in order to urge users to pay up. As if encrypting important data is not enough, the pressure on victims is increased by displaying a time limit. Many types of ransomware threaten to start deleting files or decryption keys if their demands are not met within a specific amount of time. One family lets users decrypt files for free if they spread the ransomware to other people.

1.4. Business model

The obvious reason for the growth of ransomware distribution is the direct financial gain for online criminals. However, there are multiple factors that enabled that growth in the first place and led to actual business models behind ransomware. Firstly, the rise of alternative currencies has allowed criminals to demand money while remaining anonymous. Many types of ransomware accept payments in Bitcoin, a cryptocurrency that does not require a traditional bank account. Others use payment vouchers or route payments through multiple services in order to hide their identity. Secondly, the technology behind ransomware has become a commodity. Criminals no longer need to develop their own encryption methods – they can make use of ransomware-as-a-service offers that are readily available on underground markets. This means that hardly any investment is required to set up a ransomware business. Finally, ransomware infrastructure is very flexible, complicating efforts by law enforcement officials to locate distribution or payment servers. The chance of getting caught is therefore relatively low. Together, these factors enable a business

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

model that lets criminals quickly set up a ransomware campaign, targeting a large number of users at little cost.

2. Protection against ransomware

For many users, the first response to a ransomware infection would be to pay up. After all, paying the ransom means you get your files back, right? Unfortunately, that is not always the case. First of all, there is no guarantee that criminals actually decrypt files once they receive the payment. Because the payments cannot be tracked, there is no way to get a refund if only some files are decrypted (or even none at all). And even if files are decrypted, the ransomware itself remains present on the machine. There is no way to know whether it will re-encrypt files at a later point in time, again demanding a ransom. After all, if criminals know that a specific user decided to pay the ransom once already, the chance that they can earn more money from extorting the same user is larger than if they target random other users. Finally, paying the ransom would just encourage criminals to continue spreading ransomware.

2.1. Anti-ransomware

The best protection against ransomware is to make sure it cannot infect the system in the first place. The use of a security solution with dedicated anti-ransomware functionality is recommended. In addition to standard signature-based detection, security software should be able to detect the specific actions of ransomware, such as file encryption, and block it before it can do any more harm.

2.2. Patches

In addition to ransomware-specific protection, home and business users alike should make sure their operating system as well as all applications are up-to-date. This means regularly checking for patches and installing all applicable ones. For home users, Windows Update should be allowed to automatically install security updates. For business users with multiple endpoints to be managed, a patch management concept with support from patch management software makes sure that administrators know when new patches are available and that they can efficiently and automatically deploy them.

2.3. Backup

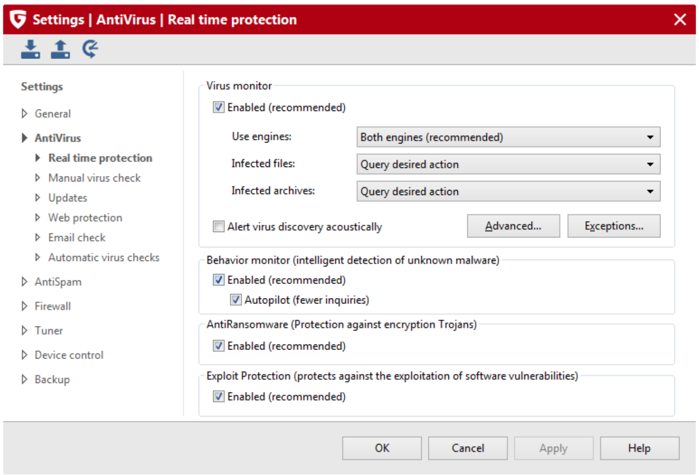
As ransomware relies on the tactic of denying users access to their own files, making sure that those files are safely backed up somewhere else can be very helpful in case of an infection. It is recommended to make backups of all important files regularly. To prevent ransomware from encrypting the original files as well as their backups, the latter should be stored on an external data medium which is not usually connected to the computer. For example, home users could secure their files by saving a backup using a cloud service or on an external hard disk. For network administrators, a centralized backup solution can make sure that important documents from all endpoints are backed up to a central server.

2.4. Awareness

In order to prevent ransomware infections, technical measures should be supplemented by user awareness. For example, when using email, attachments should only be opened if they were sent by a trusted person and if it makes sense from the context that that person would send an attachment. Similarly, links in emails should be treated with suspicion, as many online criminals send spam messages with links that trick people into visiting websites filled with malware.

3. How G DATA protects against ransomware

G DATA solutions offer comprehensive protection against ransomware, both for home and business users. All of our solutions contain a dedicated AntiRansomware module, which helps protect specifically against malware that tries to encrypt files. For business users, this module can be centrally managed using G DATA Administrator. Business users should make sure a comprehensive patch management policy is in place, which can be supported by G DATA Patch Management, an optional module for all G DATA business solutions. To protect important files against data loss of any kind, home users can use G DATA Internet Security or G DATA Total Security to make backups regularly. Our business solutions contain backup functionality as an optional module. More information about G DATA solutions for home users and businesses can be found at www.gdatasoftware.com.



Virus monitor

☑ Enabled (recommended)

Use engines: Both engines (recommended)

Infected files: Query desired action

Infected archives: Query desired action

□ Alert virus discovery acoustically

Behavior monitor (intelligent detection of unknown malware)

☑ Enabled (recommended)

☑ Autopilot (fewer inquiries)

AntiRansomware (Protection against encryption Trojans)

☑ Enabled (recommended)

Exploit Protection (protects against the exploitation of software vulnerabilities)

☑ Enabled (recommended)

Figure 4: AntiRansomware is included in all G DATA solutions