SIMPLY SECURE

G DATA WHITEPAPER

Ransomware:
A brief summary

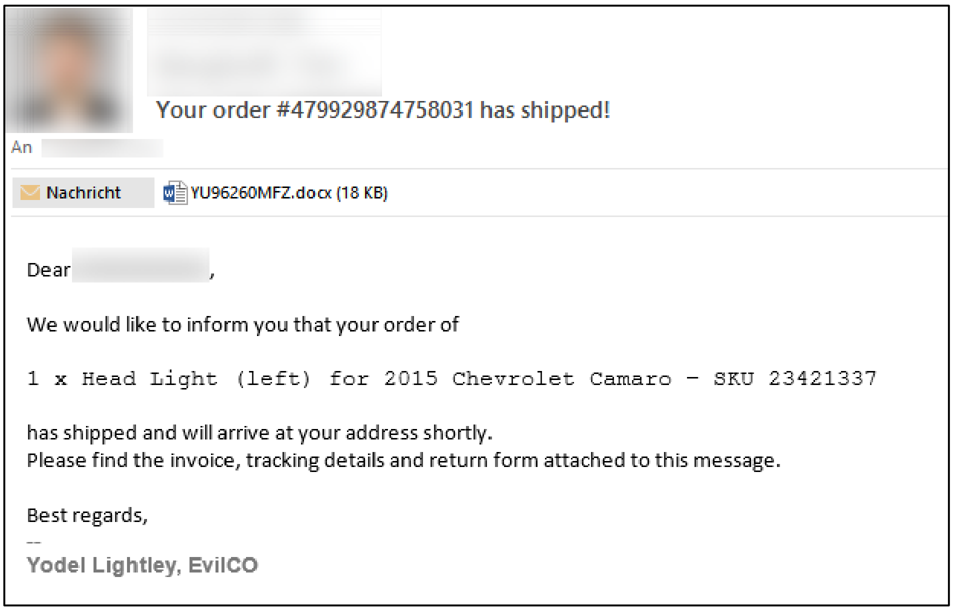
Table of Contents

What is Ransomware?

In short, Ransomware is the electronic equivalent to an individual who takes something from you and demands money to return it to you. In its electronic form, the target is your data or your system. There are two main types of ransomware. One type is called “Crypto Trojans” and the other “Screen lockers”. The latter render the system unusable unless the ransom is paid. Often they pose as warning from a law enforcement agency which suggests that “incriminating material” was found on the system but that criminal prosecution will be foregone if a fine is paid. The most notorious exponent of this type of ransomware is the “FBI Trojan”, also known as Reveton. The former variant, crypto Trojans, targets a victim’s data. This data might consist of pictures, documents, spreadsheets, databases or any other kind of data. Once a PC is infected by the malware, it will encrypt its data. Given the current state of technology, the method used to encrypt the files must be considered uncrackable, even with massive distributed computing power. To the victim the encrypted data is lost, unless the ransom is paid. Payments must then be made either in Bitcoin or some other untraceable method of payment. In theory, an attacker would then hand over the decryption key which allows the victim to recover the files. Should the victim fail to pay the ransom, the decryption key is destroyed, which renders the encrypted data ultimately lost. There are dozens, if not hundreds of different variations of ransomware in circulation which go by the names of Cryptolocker, Cryptowall, VaultCrypt or CTB-Locker. File-encrypting ransomware seems to be increasingly prevalent as of August 2015.

Why does it work so well?

One of the most frequently used techniques for spreading ransomware is called social engineering.
This technique tries to exploit the fact that humans follow certain patterns of behaviour. And those patterns are then used to get a system infected. Humans in general have a tendency to trust one another and to try to help others out – and they usually seek to avoid any problems. A classic example would be an email with what looks like an order confirmation. Typically those emails have an attachment which the victim is expected to open. If a victim receives an email which tells him that his “order has shipped”, and the victim has no memory of having ordered anything (because he or she never has), chances are very high that the attachment is now opened in order to get “further details”.



[redacted]

Your order #479929874758031 has shipped!

An [redacted]

Dear [redacted],

We would like to inform you that your order of

```
1 x Head Light (left) for 2015 Chevrolet Camaro - SKU 23421337
```

has shipped and will arrive at your address shortly.
Please find the invoice, tracking details and return form attached to this message.

Best regards,
--
Yodel Lightley, EvilCO

Figure 1: Sample of a potential cryptolocker email

Another way of contracting ransomware is while surfing the web. If a website has been compromised to serve malware then all it takes to get infected is to visit that website. The victim does not even need to click on anything or actively start a download.

Why do systems get infected so quickly?

Like any malicious software, ransomware makes use of vulnerabilities in software. Those vulnerabilities can be anywhere, but the most commonly exploited ones are in applications which are very widely used. Examples include Microsoft Office products, Adobe Acrobat Reader, Java or the operating system itself. To give you an idea about the speed with which a piece of screen locker ransomware infects a system: from the time an attachment or a website is opened to the point where a victim sees the extortion message on screen it only takes a few milliseconds. File encryptors work equally quickly. During that time, the encryption routine is installed, the installed component contacts its “command center”, generates the encryption key and starts encrypting the files right away. Once the victim sees the ransom note, it is usually too late to stop the files from being encrypted.

Why has Antivirus software such a hard time preventing this?

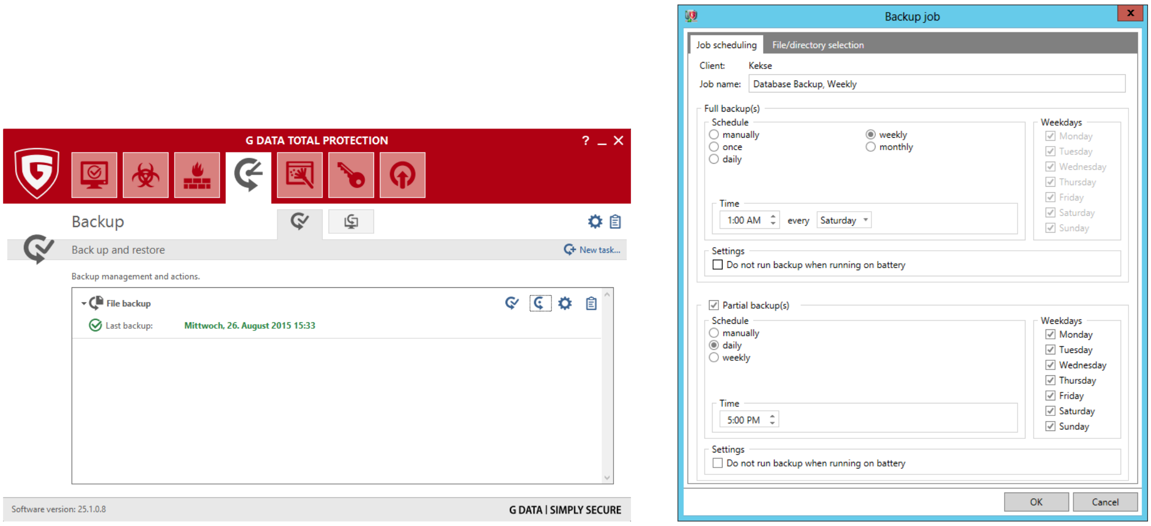
Ransomware has become an issue over the last few months and even years. The year 2013 saw the advent of the original “Cryptolocker” which has since spawned many more variants. This has not gone unnoticed by AV vendors and they ramp up their efforts to stem the flood of ransomware that is after their customers’ systems. There are a lot of weapons in their arsenals, but none of these can entirely prevent an infection by ransomware. Defences are layered: the classic signature-based detection is still the backbone of AV defence but it is not nearly sufficient anymore. For any known email attachment which is detected with a signature, there will be an unnamed number of those which are not detected. More proactive mechanisms are called for, such as behavioural analysis which looks at the activities performed by any given application. G DATA is monitoring actual system routine calls which are being performed by programs running on a system and if the pattern of calls matches that of a malicious piece of software, an alarm is raised. This has increased the effectiveness of ransomware prevention but AV vendors are still a long way away from being able to say “we did it”.
In G DATA’s research facilities, any potential ransomware samples that reach our team of analysts are treated with a higher priority than anything else. That way we can make sure that our signature-based detection is as up-to-date as possible. Additionally, we receive a lot of telemetry data which allows us to optimize the detection rates of both behavioral analysis and ExploitProtection. Currently our researchers are working on more effective defences against this phenomenon.

The question may arise why there is no dedicated anti-ransomware solution. The truth of the matter is, it would be technically possible to build a dedicated anti-ransomware solution which makes sure that the vast majority of ransomware can never infect the system. The problem is that such a solution would have a hard time being accepted by users because it would impact a system’s performance quite heavily, which is not a desirable characteristic for a security solution. The challenge therefore is to minimize the performance footprint and to maximize effectiveness. Rest assured, though: G DATA is not resting about this matter.

The moral of the story is that no AV solution is going to offer 100% protection from ransomware. Layering of defensive mechanisms is imperative to give the best possible defence.

What measures can I take to increase security?

Since any data which was encrypted by ransomware, is not accessible anymore, the most important safety measure is to maintain a current file backup. Ideally this backup is updated on a daily basis and is logically and physically disconnected from your system. In practise, this means that the medium where your backup is stored is not connected to your computer either via Wifi or through any cables. That way, you will always have a copy of your data which you can use if ransomware strikes or in case of accidental deletion. Businesses are often required by law or industry regulations to have backups in place – home users are well advised to maintain backups of critical data, too. As a home user you may already have all the required mechanisms in place: users of G DATA TotalProtection can already automate all their backups. Business users can also add an optional backup module to their G DATA solution as well – just contact your sales representative.



Back up and restore

Backup management and actions.

File backup

Last backup: Mittwoch, 26. August 2015 15:33

Software version: 25.1.0.8

Client: Kekse

Job name: Database Backup, Weekly

Full backup(s)

Schedule: ○ manually ○ once ○ daily ● weekly ○ monthly

Time: 1:00 AM every Saturday

Weekdays: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Settings: □ Do not run backup when running on battery

☑ Partial backup(s)

Schedule: ○ manually ● daily ○ weekly

Time: 5:00 PM

Weekdays: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Settings: □ Do not run backup when running on battery

Figure 2: Backup configuration in home and corporate user solution

The second and probably most important security measure is to keep all of your applications and the operating system updated. Remember that malicious software in general – not just ransomware – very often can only infect a system by exploiting unpatched vulnerabilities. Installing updates is a tedious process and might not seem very appealing – but there are tools which can automate the process. This is true for home users as well as businesses. G DATA's corporate solutions come with an optional PatchManagement module that can be used to complete all of the required patch management procedures.

Unused applications as well as any unused browser add-ons should be uninstalled – if an application is installed, then it is potentially exploitable, whether it is actively used or not. It should always be remembered that an antivirus software will not be able to stop all attacks against unpatched vulnerabilities in third-party applications. The best protection for unpatched vulnerabilities was, is and always will be, patches and updates.

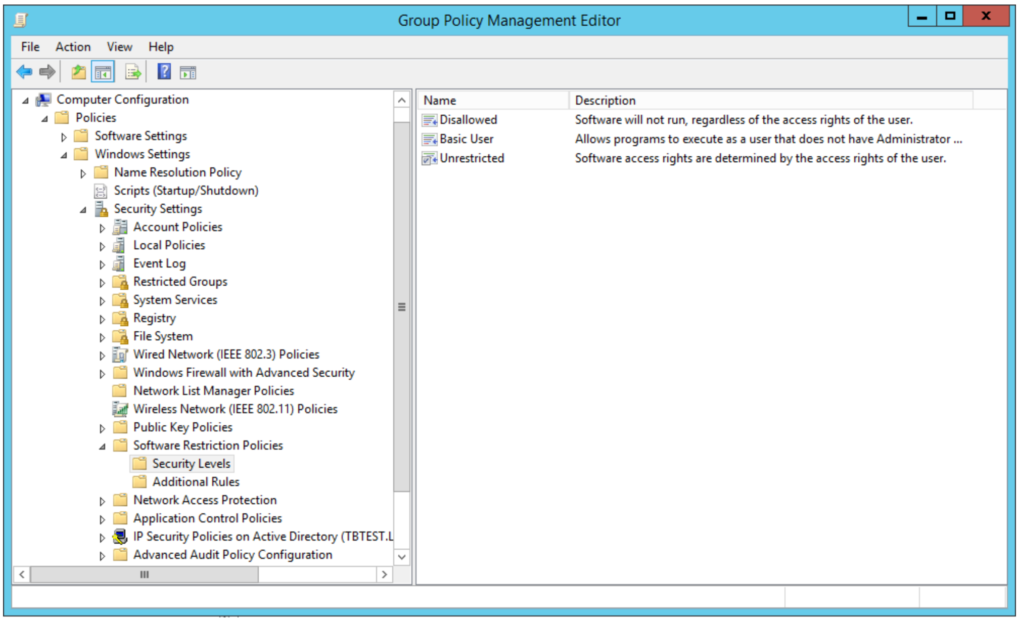
An additional component which helps address potential attack vectors is behaviour monitoring. This feature examines the actions performed by an application. It rates the pattern of actions based on its potential impact: an application which is run in the background and in the context of a different program might not yet raise a red flag, but if said application downloads additional files and/or starts creating startup entries and copy files into system folders, this may well indicate that malware is trying to attack the system. This type of proactive protection is a permanent fixture in most AV programs by now, but on its own it will not be very effective.

In G DATA's B2B solutions, the behaviour monitoring component is located in the "Client Settings" tab; home users will find it in the G DATA SecurityCenter. To maximize security it should be enabled at all times.

It is the combination of user education, signature-based protection, preventive such as regular backups, minimizing risks from exploitable software through regular updates as well as mechanisms like behaviour monitoring which is most effective against malware in general.

Having a good antivirus solution will not only mitigate the impact from ransomware but from other malicious software as well. It may not be perfect and not the answer to all questions but having an antivirus solution is still preferable over not having any malware protection at all.

In a business environment, implementing certain group policies in Active Directory will also help minimize the attack surface.
One viable and effective, albeit very restrictive solution involves blocking all applications which are not run from one of the "Program Files" folders, using what is called "Software Restriction Policy"[1]. To achieve this, a new group policy must be created in `gpmc.msc`.
The corresponding option is located under *Computer Configuration / Policies / Windows Settings / Security Settings / Software Restriction Policies*. The default is "*Unrestricted*". Setting the default to "*Disallowed*" will result in software not being able to run unless it is started from C:\Program Files (x86). Under "*Additional Rules*", exceptions can be maintained. This will address one common trait of many ransomwares: they run out of TEMP folders, %appData% or the Recycle Bin folder. Note that this approach is not necessarily applicable in all network scenarios (e.g. Workgroups); some third party applications may also require different configurations and settings.


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (TBTEST.L
Advanced Audit Policy Configuration

Name	Description
Disallowed	Software will not run, regardless of the access rights of the user.
Basic User	Allows programs to execute as a user that does not have Administrator ...
Unrestricted	Software access rights are determined by the access rights of the user.

Figure 3: Software restriction in Group Policy Editor

[1] For detailed information on software restriction policies, see https://technet.microsoft.com/en-us/library/cc786941(v=ws.10).aspx

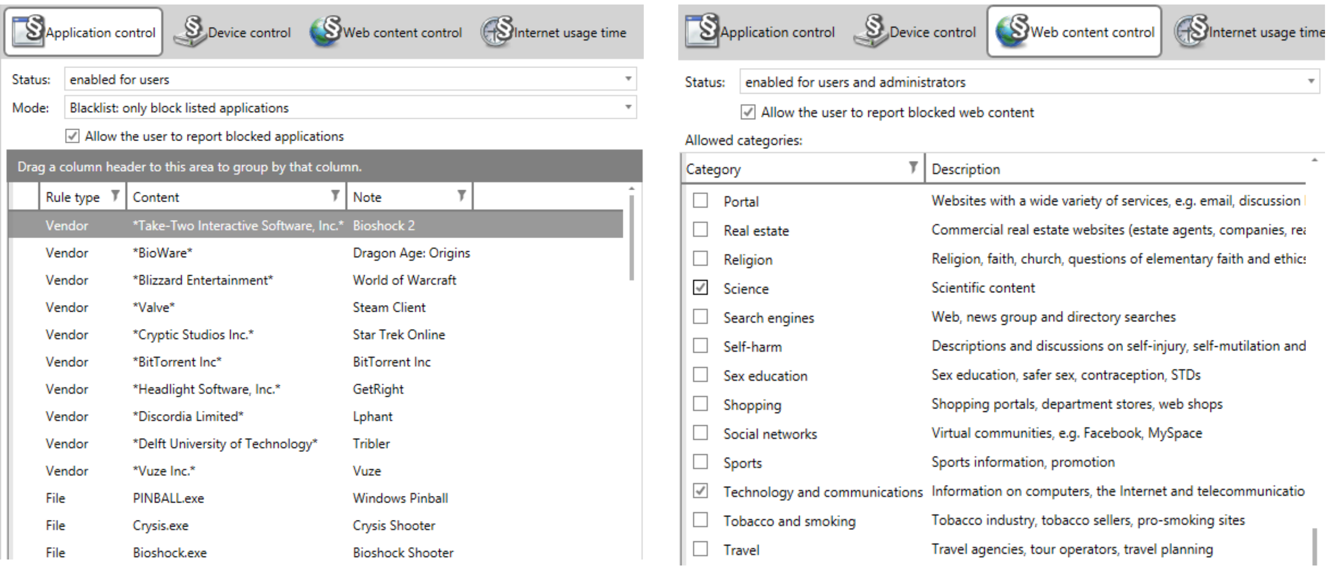
Restricting write permissions for shared folders is an option that should be considered; the handling of email attachments should also be looked at carefully. For example, unless business operations absolutely demand *.zip or *.exe attachments, those should be blocked. This is possible in G DATA's MailSecurity Gateway – additionally, all of G DATA's solutions have a cloud-based component called "OutbreakShield" which will not allow emails to pass through which are known to carry an attachment associated with crypto-malware.

In addition to this, users must be made aware on a regular basis to be wary of any emails they receive, especially if the email meets at least two out of three criteria:

- comes from an unknown sender
- is written with an undertone of urgency, with a suggestion or threat of negative consequences
- contains a call for action (e.g. "See attached document for more information" or "Click here to reactivate your account").

In order to minimize the impact of malicious software in general, password policies which require a certain level of complexity must be enforced. Third party software as well as hardware solutions are available on the market to assist in this task, such as password managing applications. Since malicious software often runs with the permissions of the user who is currently logged on, administrator permissions should be used only when required.

On top, G DATA's PolicyManager offers network administrators a way to whitelist only those applications, storage devices and websites which are relevant for business operations.



Status: enabled for users

Mode: Blacklist: only block listed applications

☑ Allow the user to report blocked applications

Rule type	Content	Note
Vendor	*Take-Two Interactive Software, Inc.*	Bioshock 2
Vendor	*BioWare*	Dragon Age: Origins
Vendor	*Blizzard Entertainment*	World of Warcraft
Vendor	*Valve*	Steam Client
Vendor	*Cryptic Studios Inc.*	Star Trek Online
Vendor	*BitTorrent Inc*	BitTorrent Inc
Vendor	*Headlight Software, Inc.*	GetRight
Vendor	*Discordia Limited*	Lphant
Vendor	*Delft University of Technology*	Tribler
Vendor	*Vuze Inc.*	Vuze
File	PINBALL.exe	Windows Pinball
File	Crysis.exe	Crysis Shooter
File	Bioshock.exe	Bioshock Shooter

Status: enabled for users and administrators

☑ Allow the user to report blocked web content

Allowed categories:

Category	Description
□ Portal	Websites with a wide variety of services, e.g. email, discussion
□ Real estate	Commercial real estate websites (estate agents, companies, re
□ Religion	Religion, faith, church, questions of elementary faith and ethic
☑ Science	Scientific content
□ Search engines	Web, news group and directory searches
□ Self-harm	Descriptions and discussions on self-injury, self-mutilation and
□ Sex education	Sex education, safer sex, contraception, STDs
□ Shopping	Shopping portals, department stores, web shops
□ Social networks	Virtual communities, e.g. Facebook, MySpace
□ Sports	Sports information, promotion
☑ Technology and communications	Information on computers, the Internet and telecommunicatio
□ Tobacco and smoking	Tobacco industry, tobacco sellers, pro-smoking sites
□ Travel	Travel agencies, tour operators, travel planning

Figure 4: Application & web content control in G DATA PolicyManager

My network has been hit with ransomware. What do I do now?

The first and most important thing is not to panic. This can worsen the impact of what is happening and lead to complications further down the line. Here is a list of things to do in case a system was affected by ransomware.

a) First of all, **do NOT pay the ransom**!
Even if enough money is available, a ransom should never be paid. There is no way of ensuring that you will be able to recover any or all of your data – the attacker may all of a sudden demand more money or just fail to deliver on his "promise".
Also, the money raised with those ransoms will contribute to more organized crime.

b) **Disconnect the system** from the rest of the network **immediately.**
The reason for this measure is that some variants of ransomware infect & encrypt network drives and shared folders as well.

c) The infected system should from now on be considered compromised and not trustworthy anymore. **Restore data from a backup** and consider rebuilding the system.

d) If the system was hit with a screen locker that demands money to give you back controls, **go to our website.** The "Tools" section at http://www.gdata.de/downloads holds the link to a removal tool which is capable of removing some types of screen-locking ransomware.

The above list is not exhaustive – additional steps may be required for individual production environments or the practical application might look different. Whichever steps are taken in the event of a ransomware infection, those should become part of an organization's Business Continuity Plan which is reviewed and updated regularly and to which the IT department can refer. This will help prevent unnecessary downtime and to ensure a consistent response every time the plan needs to be put into action.