Defend Your Data from Ransomware Attacks

Blackmail Software (Ransomware) Solution Brief
We provide all-aspect protection against potential attacks
Ransomware

The topic of “Ransomware” is one of the biggest topics in the IT world. This solution brief contains background information, opinions, and tips for protecting you from dreaded Trojans.

Even TV Sets are Affected

Now it also threatens TVs. A smart TV produced by LG company suddenly stops working. And the screen shows a message stating that the device would only be unlocked if 500 dollars were paid.

This is just one of countless reports about blackmail software (Ransomware). At the moment, no other topic is causing as much attention in IT circles. Companies are the main victims. According to a study by IBM, 70 percent of targeted companies pay the required ransom - half of them more than 10,000 US dollars and 20 percent even over 40,000 US dollars.

On a daily basis, the BSI detects around 380,000 new malicious program variants. There are increasingly more types of blackmail software (Ransomware). As one cannot expect any all-clear signal, companies and institutions should protect themselves.

What is Blackmail Software (Ransomware)?

Blackmail software (Ransomware) is also referred to as encryption or blackmail Trojan. The malicious software (Malware) encrypts files on the computer or smartphone of the victim, and often on connected network drives. The affected data becomes useless. The blackmail software (Ransomware) then shows the victim a blocking screen with the request to transmit a certain sum (often in the form of bitcoins) to the attacker. Only then would the files be decrypted again.

About this solution brief

This solution brief contains background information, opinions and tips for the protection against dreaded blackmail Trojans. It is aimed at IT professionals as well as private users.
10 valuable tips

What should IT administrators and employees consider in order to protect themselves against blackmail software (Ransomware)? Here is a summary of the most important tips.

01 Backups! Backups! Backups!

In spite of all the following measures, no company is ever completely protected against blackmail software (Ransomware). The most important tip is therefore to make regular backups. In addition, the backups should be kept separate from the network. Otherwise, the backups could also be encrypted.

02 Up-to-date

Whether it is the operating system or office applications - the most secure editions are the latest versions. Manufacturers always update their latest software versions first. Updates for older programs are - if at all - usually only provided later. It is therefore recommended to use the latest software versions as much as possible and keep them up-to-date at all times.

03 Unsafe websites

Avoid visiting unsafe websites. But even serious web portals can be infected with malicious software. Particular caution should be paid when visiting blogs - they are the most frequently infected websites. Firewalls with protection mechanisms increase the security of surfing the Web. In particular, content filters can help by blocking contaminated sites. The corresponding databases are constantly updated. In this way, even "newly" infected websites are quickly marked and can no longer be accessed.

04 Take special care with e-mails

Despite spam filters, e-mails from unknown senders will always find their way into your mailbox. In these cases, always be suspicious - and, above all, do not open attachments. And be careful: The tricks of the fraudsters are becoming ever more sophisticated. Be it fictitious and well-made job applications or real-looking mails from financial services providers - a fundamental skepticism is always appropriate when it comes to e-mails.

05 Protection by hardware and software

Among the most effective protection mechanisms are firewalls. Combined with various software solutions, firewalls offer comprehensive protection against blackmail software (Ransomware) and other malicious programs - from gateway to endpoint protection (client). SSL inspection, VPN application intelligence, intrusion detection prevention, single-sign-on and content filters are now common functions of firewalls. In terms of software, anti-virus solutions as well as special anti-ransomware programs are useful. It is important that the programs and firewalls are coordinated so that they do not interfere with one another.
06 Working without admin rights
If possible, do not provide the user profiles of the employees with admin rights. Many programs cannot be installed with normal rights. Similarly, this will prevent various malicious software from being installed.

07 Use of script blockers
We recommend that you install a script blocker for the Web browser. This prevents the execution of malicious code on websites.

08 Raise employees’ awareness
Employees should be reminded of the issue of blackmail software (Ransomware). Correct behavior should also be trained in case of emergencies. For example, case studies can be analyzed. Trainings should be repeated at regular intervals.

09 Be prepared
Plan how to proceed in the worst case scenario. What should one do? Who are the contact persons for the employees? What happens during the time between infection and complete restoration of the systems? A regulated procedure helps to maintain the calm in case of emergencies.

10 In case of an infection
Immediately disconnect the affected computer from all networks. Check if other computers on the network are infected. Then reinstall the system and change all passwords. Now load the backup. It is also advisable to contact the local police stations and file a report. Paying ransom to the blackmailers is not recommended. There is no guarantee that the encrypted data will actually be decrypted.
Malicious software on the Net

The Internet is a blessing and curse at the same time. Its dangers are often not taken seriously. The number of cases involving blackmail software (Ransomware) and other malicious programs, however, are growing rapidly.

Trojans in banking transactions

Just executing a quick money transfer. Hardly anyone is aware of the possibly grave consequences of an infection with malware. But it happens all the time. Newsletters are full of reports about Trojans, with banking Trojans being the dream of criminals and the nightmare of all users. The e-banking Trojan “Tordow” was synonymous with “Super-Trojan” in the context last year.

E-Banking Trojan “Tordow”

Once Tordow had successfully established itself, the Trojan could, for example, copy calls, copy bank information and reload and install additional malware. There was also the risk that the malware could read access data, including passwords, for online services from mobile web browsers. This is just one example of the enormous damage potential that users are exposed to.

Great variety of malicious programs

Apart from Trojans, which can spy on a computer and forward sensitive data to third parties, there are various other forms of malicious programs. Recently, there have been many media reports about blackmail software (Ransomware). These are also called Encryption Trojanians and can be found in a number of different varieties - the common denominator being extortion.

Thus, data is encrypted on the computer and also on the network drives of the victim - and only decrypted when a ransom payment is made. At least, this is what the attackers promise. Experts advise against transferring money in such cases. Rather, they advise making regular backups, which should be kept separate from the computer and the network.

Reasonably-priced firewalls with integrated threat defense system

To simply accept the above-mentioned dangers is, however, not a viable alternative. Both private individuals and companies of all sizes can now opt for affordable solutions offering reliable protection against blackmail software (Ransomware) and other malicious programs.

For all the damage ransomware can cause, you are not defenseless in the fight against these online bandits. Several security options exist to protect personal and enterprise systems from being compromised. Unified Security Gateways, or USGs, provide comprehensive protection against potential ransomware attacks through features like anti-spam to block phishing emails, content filtering to prevent access to suspicious links, anti-virus to protect users from malware-infected files, and Intrusion Detection and Prevention (IDP) to detect and stop intruders from gaining control of your system.

Anti-Spam blocks unwanted Email

Anti-Spam is the first line of defense in protecting one’s system from ransomware by filtering out suspicious content with reputation-based email protection. Potentially harmful messages can be blocked before the recipient ever has a chance to open them. Real-time protection is augmented with automated sharing and updating to continuously monitor and report activity.
Content filters secure Web connections
As with anti-spam, content filtering cuts ransomware attacks off at their source. If a user accidently clicks a suspicious link, the URL is checked against a database of malicious sites. Databases are continuously updated to stay one step ahead of the cyber thieves. Zyxel USG and ZyWALL products also offer SSL inspection to combat encrypted web traffic.

Anti-Virus stops malware-infected files
Anti-Virus provides a third line of protection by thoroughly scanning incoming files for worms, Trojan horses, and malware with protocols such as SMTP and POP3.

IDP monitors network behaviors
Intrusion Protection and Prevention service is like having your own personal security guard who is constantly on patrol for abnormal behavior on your network. Zyxel IDP vigilantly watches for suspicious connection attempts and backdoor programs.
Gloomy prospects

The omnipresent topic of blackmail software (Ransomware) has become a serious problem. Experts Marc Henauer and Andreas Wisler are painting a gloomy picture.

A terrifying number of infections

5000 infections per hour - and this alone in Germany. Blackmail software (Ransomware) is on the rise. Marc Henauer, Section Head of MELANI (Melde- und Analysestelle Informationssicherung/Reporting and Analysis Center for Information Security) explains the situation.

New players

The ever growing importance of IT for business processes also leads to increased opportunities for fraud, espionage and blackmail, explains Henauer. Today, new actors appear in the role of bad guys - organized crime and even states have discovered the benefits of blackmail software (Ransomware). In addition to commercial motifs, the accumulation of know-how and also political purposes are increasingly used as reasons for the use of blackmail software. Events like the National Ransomware Awareness Day, which MELANI organized last May 19, 2016, shows how seriously the Federal Government takes the problem.

Coffee machines and cars

Andreas Wisler confirms the severity of the problem. The CEO of the company goSecurity GmbH knows about various real-life examples of cyberattacks. Hacked coffee machines, paralyzed hospitals, and even a Tesla car that could not be started. With increasing electronic networking, devices very different from ordinary computers or smartphones are becoming popular attack targets.

Even small companies are affected

Wisler pointed out that the cases of blackmail software (ransomware) infections are no longer only restricted to major companies. Even small businesses and even one-man companies are increasingly under attack. In 2015, SMEs were the most attacked companies at a rate of 43 percent. The common opinion of many SME bosses that only large companies are in danger of falling victim to Ransomware is definitely wrong.

Harmful blogs

The most dangerous websites containing malicious software are not sites with pornographic content. Most malicious programs are spread via blogs. Online shops are also popular hunting grounds for criminals.

Sobering conclusion

The general rule is: Chances of becoming victims of blackmail software (Ransomware) are higher than ever before. For individuals, one-man businesses, SMEs and even large companies, this growing threat means above all one thing: Be cautious when using the Internet, protect yourself as well as possible, and be prepared for the worst case scenario. Tips for this can be found on the fourth page of this solution brief.
Security services

Anti-Virus
- Integrate Kaspersky’s leading technology SafeStream II gateway
- Anti-virus including viruses, Trojans, worms, spyware and rogue ware
- Fast stream-based scanning provides real-time protection with no file size limitation
- High detection rate without sacrificing performance
- Cloud-optimized database supported

Anti-Spam
- Transparent mail interception via SMTP and POP3 protocols
- Zero-hour virus outbreak protection
- Sender-based IP reputation filter
- Blacklist and whitelist support

Application Patrol
- Granular control over the most important applications
- Identifies and controls application behavior
- Application bandwidth management
- Supports user authentication
- Real-time statistics and reports

Content Filtering 2.0
- Dynamic, cloud-based URL filtering database
- Bandwidth regulation by filtering
- SafeSearch support for social networking content constraints
- IPv6 GeoIP Blocking covers management of billions of IOT and mobile devices
- GeoIP maps and tracks IP addresses from the cloud into real geographical locations

Intrusion Detection and Prevention
- Routing and transparent (bridge) mode
- Detects and alerts you of suspicious or malicious activity
- Customizable protection profile
- Customized signatures supported

Product/Service Compatibility List

ZyWALL Security Appliances and Services

<table>
<thead>
<tr>
<th>Product/Service Compatibility List</th>
<th>USG1900/1100</th>
<th>USG310/210/110</th>
<th>USG60/60W</th>
<th>USG40/40W</th>
<th>ZyWALL 1100/310/110</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTM Package</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Ant-Virus, IDP and Application Patrol, Content Filtering 2.0, Anti-Spam)</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
<td>1 year</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
</tr>
<tr>
<td>IDP and Application Patrol</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
</tr>
<tr>
<td>Content Filtering 2.0</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
</tr>
<tr>
<td>Anti-Spam</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
<td>1 year/2 years</td>
</tr>
</tbody>
</table>
Interview with the training leader

The experienced Zyxel Training Course Leader Patrick Hirscher answers the most important interview questions on the subject of blackmail software (Ransomware) and offers useful first-hand tips.

Q: How do you judge the threat posed by blackmail software (Ransomware)?

The threat is very severe, ever growing, and still difficult to assess. There is one point, however, everyone agrees on with regard to the topic of blackmail software (Ransomware): Unfortunately, we currently do not have a simple comprehensive solution for all problems in this area. Obviously, the IT industry is aware of this, and this gives hope for a swift solution. But for the time being, we have to cope with the current situation and keep the available solutions as safe as possible.

Q: How can blackmail software (Ransomware) be blocked already in incoming mail?

As a first instance, one certainly needs an anti-spam solution with an integrated virus scanner. However, Ransomware attacks are becoming increasingly sophisticated and are, unfortunately, often not recognized by anti-spam solutions despite the latest sandbox-security technology. At Zyxel, all emails with suspicious attachments are blocked and quarantined. However, this leads to negative consequences: The quarantining is manually executed by an IT employee who checks the mail for its trustworthiness and then releases it to the addressee. This implementation entails great effort, but is very effective in light of the current threat situation. In addition, dedicated mailboxes are used for public mail accounts, which deal with many general and potentially dangerous e-mails. The logged-in user works with very restricted rights on the file server. In case of a Ransomware attack, the damage would be limited and under control.

Q: How can systems become as immune as possible against blackmail software (Ransomware)?

An absolute must is to continually upgrade operating systems and applications. In this area, we are uncompromisingly committed to “speed”. As soon as new updates are made available by manufacturers, we implement them as quickly as possible. This is no longer done only over the following weekend, but even during ordinary workdays. In principle, we are convinced of this need, but are currently doing our best to create a reliable report, which shows that all clients have the latest version.

Q: How can one increase awareness of blackmail software (Ransomware) among users?

The assessment of the trustworthiness of a specific case has gone wrong even in our own company. A very well-forged application was forwarded as an e-mail via three instances. One person finally opened the application file infected with blackmail software (Ransomware). And this, despite a macro program warning on the part of the Word software. Fortunately, the virus scanner installed on the client was able to prevent even worse effects. Following this incident, we conducted an internal security training course, obligatory for all employees, in which we disclosed and analyzed the case in order to learn from it. I am convinced that the time spent on this activity has made a significant contribution to the correct handling of information from different sources (mail, browser, etc.). In the future we will carry out further internal awareness training courses.
Q: What should be taken into account when securing data with backups?

In the case of successful crypto attacks, only the existing backups provide required data. We have ensured that the saved data is separated from the corporate network after each successful backup.

Q: What other measures are planned for Zyxel?

- Use of FW ZLD4.25 within the ZyWALL USG Series (with GeoIP and SafeSearch)
- Uninstalling of various SW packages on the clients (only providing SW, which are required)
- Revision of the internal IT guidelines
- Adaptation of the authorization structures on the file server

Q: What other tips can you give IT managers?

IT departments can make a major contribution to ensuring the security of company by operating various systems, which are well maintained and regularly checked for correct functioning. The known cases of loss or damage show, however, that different human behavior could have prevented a lot of the negative effects. It is therefore constructive to train employees on a regular basis and to provide them with specific information about new hazards. Moreover, one should take the necessary time to create widespread awareness - it’s worth it!