Avira

Protection against Ransomware –

FAQ for business customers

www.avira.com

1. What is ransomware?

Ransomware is a type of blackmail malware that encrypts photos, video, music, and other files on a computer or blocks access to the entire system. To access your files or devices again, typically victims need to pay some sort of a ransom or fee.

2. What types of ransomware are there?

Three types of ransomware exist: Encryption ransomware, which scrambles files (making them unusable); lockscreen ransomware, which shows a full-screen image that prevents you from accessing your PC or files; and master-boot-record ransomware, which encrypts the first sector of the partition table on BIOS-based computer systems.

3. What does ransomware do?

Ransomware is typically spread by email or through exploits. In the first instance, the cybercriminal sends a phishing email with an attachment to a specific organization, for example. The unsuspecting user opens this attachment (Word or JavaScript file) as what is written in the email seems deceptively true to the victim. Once the Word document is opened, the user is informed that macros need to be activated to show the content correctly. Enabling macros allows the ransomware to be secretly downloaded onto the computer via a drive-by download by running a script stored in the file.

4. What happens when ransomware infects the computer?

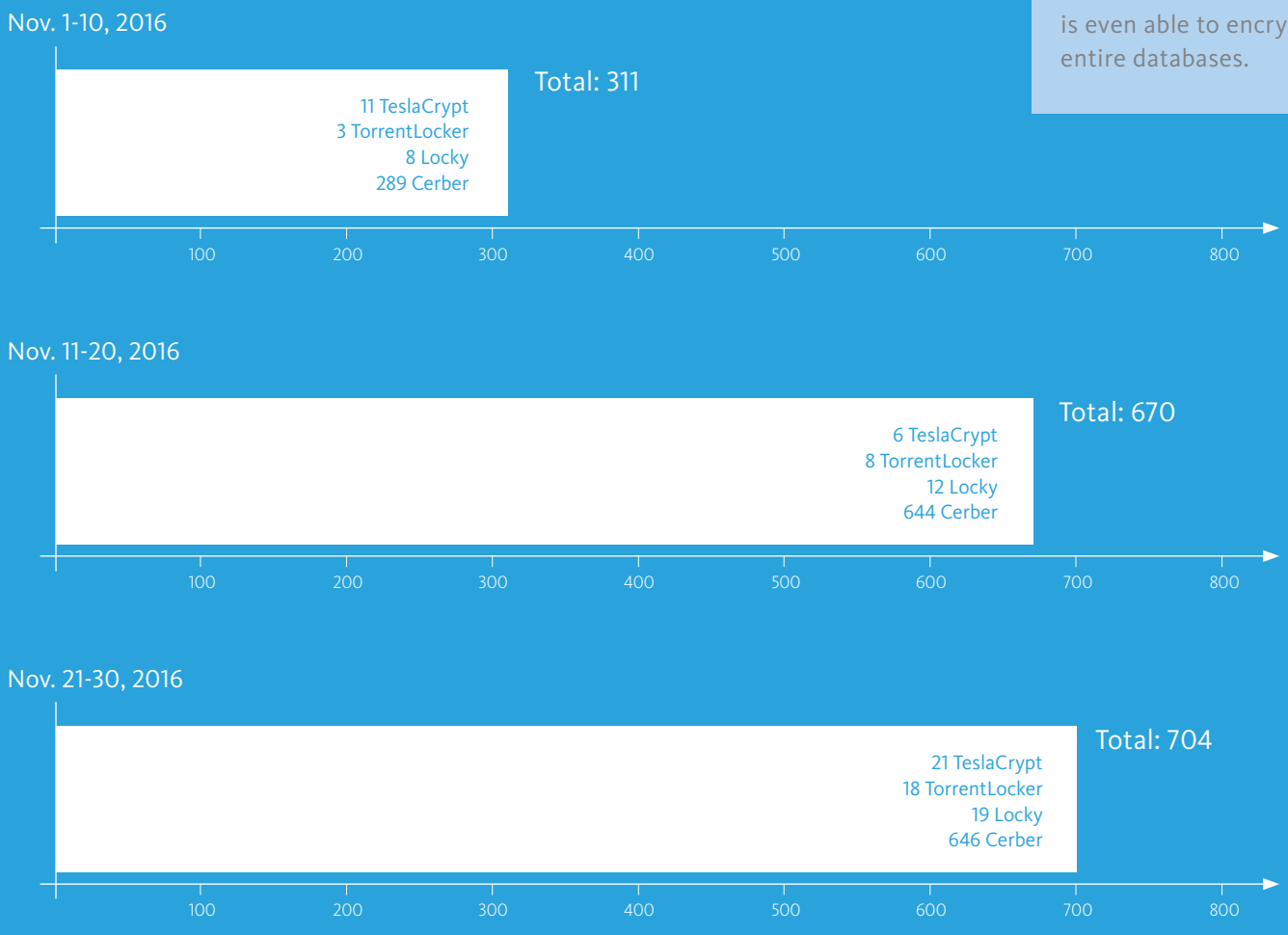
The downloaded crypto-ransomware encrypts all your files, such as photos, videos, and Office documents. It also scrambles data on removable drives and cloud storage services if you are connected to them at the time. Now that all the files have been encrypted using a special file extension, the ransomware demands payment in exchange for unscrambling them. The ransom, which frequently needs to be paid in bitcoins to a special website on the darknet, can amount to many thousands of euros. In the case of screen-locking ransomware, the malware locks the home screen – preventing users from accessing their devices – and similarly demands payment for regaining access such as in the form of purchasing a UKash card or other digital payment method.

5. What is the current threat level?

Ransomware attacks will continue as this business model is like a modern-day gold rush for cybercriminals, with many victims willing to pay – often tacitly. Cybercriminals are continuously developing this lucrative business model. This means that nowadays not only Windows programs (Portable Executable) are used, but script languages – VBS, JavaScript, PowerShell – are increasingly also utilized to make malware classification more difficult. Ransomware is now also on Android devices: Users cannot use their smartphone until they buy back their data via text message payment. Mac users are affected by the KeRanger ransomware, among others. Other well-known types include Petya, FBI Ransomware, and Locky, which have already infected millions of Windows computers.

Ransomware – a persistent threat

Volume of selected encryption Trojans
in November 2016 | Source: ransomwaretracker.abuse.ch



Cerber

The Cerber family is one of the most dangerous types of ransomware, which typically spreads in the form of email attachments. The latest version is even able to encrypt entire databases.

6. Which security technologies does Avira employ to fight ransomware?

A multi-layered security strategy is needed to minimize and mitigate the risk factors associated with ransomware. To achieve this aim Avira has developed efficient technologies to detect and fight malicious software in real time. We employ state-of-the-art technology such as machine learning/ artificial intelligence, reputation, behavior-based detection, and real-time analyses to classify unknown files. And our customers always have access to the most current data thanks to our cloud service. In the future, systems supported by artificial intelligence will play a major part in analyzing and classifying previously unknown malicious software.

Avira recommends the following actions to protect yourself against blackmailing Trojans:

1.

Always keep security software and applications up-to-date.

Do not put off updates and patches.

Segment the company network.

2.

Regularly train employees by informing them about current threats (such as ransomware) and their particularities as well as regular backups, the more often, the better.

3.

These backups must be stored separately or offline from the network infrastructure – a backup encrypted by a crypto Trojan is of no use to anyone.

7. What IT security strategy do companies need to have in place to be protected against attacks?

IT security should be an integral component of the corporate strategy for every company to be prepared for cyber attacks – no matter whether it is a small office with a few employees, an SMB, or a corporation. This is the only way to avoid data espionage and losses, and the resulting reputational damage. In general, companies should install security software that offers real-time protection against malicious software, such as with the help of cloud technology. In addition, artificial intelligence technology allows for quick detection of files that are still unknown as being malicious software. To do so, however, companies have to equip their IT security systems correspondingly and guarantee unrestricted operation of these technologies.

4.

Restricted user rights: Each employee should only have the access and user permissions that he/she actually requires.

Whitelisting: Only authorized software may be run.

5.

Create bring your own device (BYOD) rules: Secure the company network against "outside" devices (such as private laptops, smartphones, and other data carriers such as USB sticks).

6.

Use a form of browser protection or a secure browser to block harmful websites and phishing sites automatically.

About Avira

Avira, a family-owned company which enjoys above-average growth, was founded in 1986 by the IT security pioneer Tjark Auerbach in Tettnang. It is one of the most important regional employers in the Lake Constance area.
For three decades, Avira has provided its customers with security solutions, developed by Avira itself, for protection against Internet threats, malware attacks, harmful programs, and data theft. More than 100 million users, particularly micro and small businesses as well as home users, rely on Avira's software and value its reliability, performance, and usability.
Avira ranks second among the world's leading antivirus software manufacturers. The company, headed by Travis Witteveen, operates its own virus laboratories and continuously demonstrates its enthusiasm for innovation and its capabilities by developing next-generation security technologies. These include real-time protection through cloud-based malware detection and the "Online Essentials" Web Console.
Avira works closely with the Federal Office for Information Security (BSI) and is a founding member of the "IT-Security made in Germany" initiative.
Avira's experience and top-rated products and services help people move freely and safely in our digital world.
Security in the real world is another important concern for Avira. Established by the company's founder, the Auerbach Foundation supports charitable and social projects, and has already sponsored more than 300 projects in the areas of education and schooling, children, youth and family, assistance for senior citizens and people with disabilities, as well as arts and culture.

Errors excepted. Subject to technical changes. As at: December 2016

Avira

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany
Phone: +49 (0) 7542-500 0

PROTECTING PEOPLE
IN THE CONNECTED WORLD

www.avira.com