Security awareness update on

Computer viruses

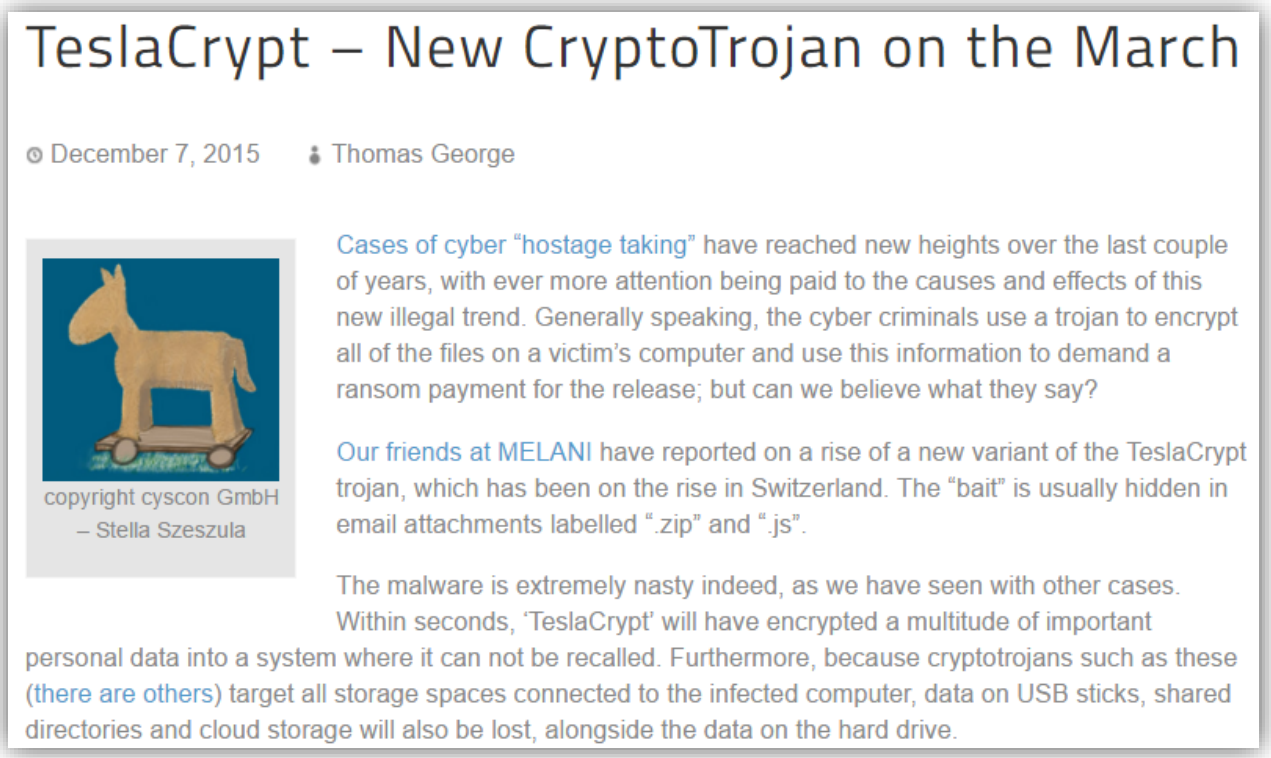
Summary

Computer **viruses** and other forms of **malware (mal**icious soft**ware)** are constantly evolving, much like their biological namesakes, hence the reason for this annual update. This year, it is becoming clearer than ever that – despite our best efforts – we cannot totally prevent virus infections, so we must prepare to deal with incidents. Infections can quickly spread and turn nasty, causing outbreaks similar to human diseases such as bird flu and Zika. We must remain vigilant for possible virus-infected email attachments and apps, plus infectious websites in the hope of avoiding them, and report suspicions about infections as soon as practicable to the Help Desk. There's not a moment to lose.

Current virus concerns

The organization's main concern at the present time is criminal use of computer viruses, specifically bank Trojans and ransomware.

Bank Trojans are secretive programs that intercept and manipulate online bank sessions, draining corporate bank accounts and transferring money via money mules and Bitcoins to untraceable accounts beyond the organization or the authorities' reach. This is major concern for the people in Finance with online access to the corporation's bank accounts. On a smaller scale, bank Trojans will also drain personal bank accounts given the chance, so we all need to take care.



TeslaCrypt – New CryptoTrojan on the March

December 7, 2015 Thomas George

copyright cyscon GmbH – Stella Szeszula

Cases of cyber "hostage taking" have reached new heights over the last couple of years, with ever more attention being paid to the causes and effects of this new illegal trend. Generally speaking, the cyber criminals use a trojan to encrypt all of the files on a victim's computer and use this information to demand a ransom payment for the release; but can we believe what they say?

Our friends at MELANI have reported on a rise of a new variant of the TeslaCrypt trojan, which has been on the rise in Switzerland. The "bait" is usually hidden in email attachments labelled ".zip" and ".js".

The malware is extremely nasty indeed, as we have seen with other cases. Within seconds, 'TeslaCrypt' will have encrypted a multitude of important personal data into a system where it can not be recalled. Furthermore, because cryptotrojans such as these (there are others) target all storage spaces connected to the infected computer, data on USB sticks, shared directories and cloud storage will also be lost, alongside the data on the hard drive.

Source: Check-and-Secure blog

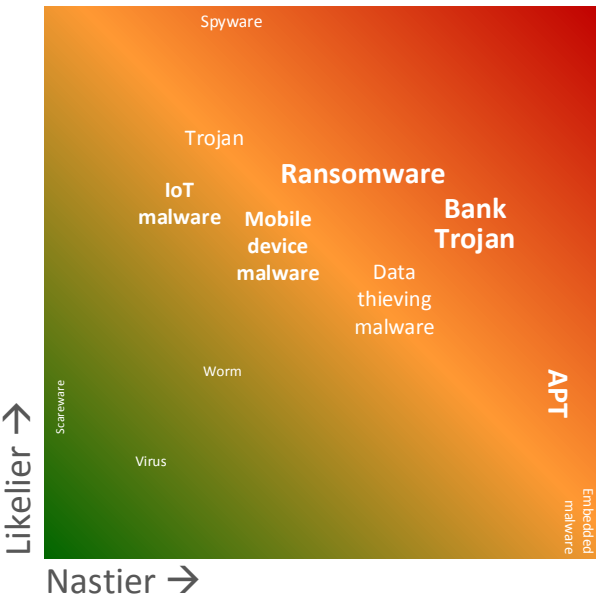
Ransomware programs lock users out of their computer devices, often by encrypting all their data and then demanding a ransom payment for the key needed to decrypt the data. A ransomware infection on the corporate network could lock us out of all our IT systems, totally disrupting the business. According to news reports, the ransom demands, *so far*, have been for just a few hundred or thousand dollars, enough to hurt but not outrageously expensive. The trouble is that nobody likes caving-in to criminals, especially as there is no guarantee that they will provide the unlock key. Paying up also demonstrates weakness, openly inviting further attacks.

Source: Kaspersky

Fortunately, good incident management and response procedures, plus offline backups and technical support from IT and forensics professionals, can reduce the extent and length of disruption caused by viruses … but it's much better to avoid getting infected in the first place!

Emerging virus risks

Besides ransomware and bank Trojans, we're keeping a close eye on other virus risks in the orange and red zone of the colorful risk graphic.



Viruses are an increasing threat to **IoT** (Internet of Things) *things* and **mobile devices** such as laptops, tablet PCs and smartphones. Modern viruses are specifically designed to run on a wide variety of systems including Windows (of course) but also Android, iOS/MacOS and Linux, allowing the same criminal campaigns to work across a larger pool of systems. Criminals can buy custom-made viruses, or rent out entire networks of infected systems on the black market, the hacker/criminal underground.

Data-thieving malware is another growth area. Criminals are stealing personal data to commit identity theft, typically using stolen credit card numbers to make fraudulent purchases. There are persistent rumors about unethical competitors and secret government agencies using viruses to steal commercially valuable information – trade secrets, customer lists, new product designs and so on. It is conceivable that they may also use viruses to disrupt business operations, increasing costs and reducing competitiveness through economic or industrial espionage. The involvement of government intelligence services (spies!) is worrying because of their enormous resources and capabilities.

Keeping viruses under control

Avoidance is best

Be wary of email attachments and links, lost and found USB sticks, dubious apps and websites. Learn to recognize possible phishing emails and other social engineering tricks. Slow down a bit and think about what you are doing. If an email appears unexpectedly, particularly from someone you don't know but maybe from a friend, colleague or relative, resist the temptation to double-click that attachment or click the link until you have had a chance to consider and check with the sender.

Keep your wits about you: be *malaware*

Prevention helps

Keep up-to-date with antivirus software and security patches on all your computing devices. IT Department does this on corporate IT systems but it is *your* responsibility on personally-owned devices (including your home computers, laptops, smartphones, iPads and iPods), especially if they are used for work purposes under BYOD.

Don't meddle with the security software or settings

By the way, make sure that family members and friends who share any of your IT devices know about the malware threat: you don't want to end up with a serious problem because someone *else* using the machine caught an infection!

Rapid response is essential

You *may* be lucky: antivirus software *might* identify and block a virus but if it is something totally new or especially sneaky, antivirus may completely miss it. The first signs of infection might be when important business data goes missing (cybertage), or when the bank or credit card rings you up to ask about unusual charges on your account (identity theft). Contact Help Desk to call out the cavalry.

If you think your system might be infected, call Help Desk urgently

Lastly, keep *offline* backups. **There may be no alternative but to completely wipe and rebuild a badly infected system from scratch.** Any data that is stored on the corporate network is backed up automatically by IT, but *you* are responsible for backing up anything stored on your own devices or on removable media. Cloud backups are better than nothing but ransomware may encrypt or damage cloud backups at the same time it trashes your computer, so we recommend making backups on external hard drives or USB sticks that are normally *disconnected* from the computer and stored somewhere safe – literally in a fire safe if the information is truly valuable.

Further information

Discover more about computer viruses on the intranet *Security Zone*, including scam alerts on bank Trojans, ransomware and more. Contact Help Desk for further assistance. Remember, call them ***straight away*** if you think your desktop, laptop, tablet or smartphone might be infected. Time is of the essence.