Safeguarding user data with Kaspersky Cryptomalware Countermeasures Subsystem

Cybercriminals are quick to adopt techniques developed by villains in the offline world, including extorting money from victims. One of the most common ransomware attack scenarios sees the user's data encrypted before a ransom demand is delivered. Users place a high value on their data and many of them are willing to pay to get those precious files back. However, paying the ransom is unwise, primarily because it does not guarantee that the corrupted data will be decrypted. At the same time modern cryptomalware uses encryption schemes that – up to now – seem to be unbreakable, so victims face a choice between paying up or losing those files. Of course, reliable internet security software installed on the computer will react to malicious activity but even best antimalware solutions successfully can only detect newly developed cryptomalware after it begins to corrupt data. So from time to time previously unseen malware, which does not appear in any database, is able to encrypt a couple of files before being neutralized. That is why Kaspersky Lab developed its cryptomalware countermeasures subsystem.

Cryptomalware menace

Usually cryptomalware is distributed through spam messages with executable files attached and purporting to be documents, but it can be planted by other means. For example, there are registered cases of cryptomalware installation made by another piece of malware — a Trojan of the ZeuS/Zbot family.

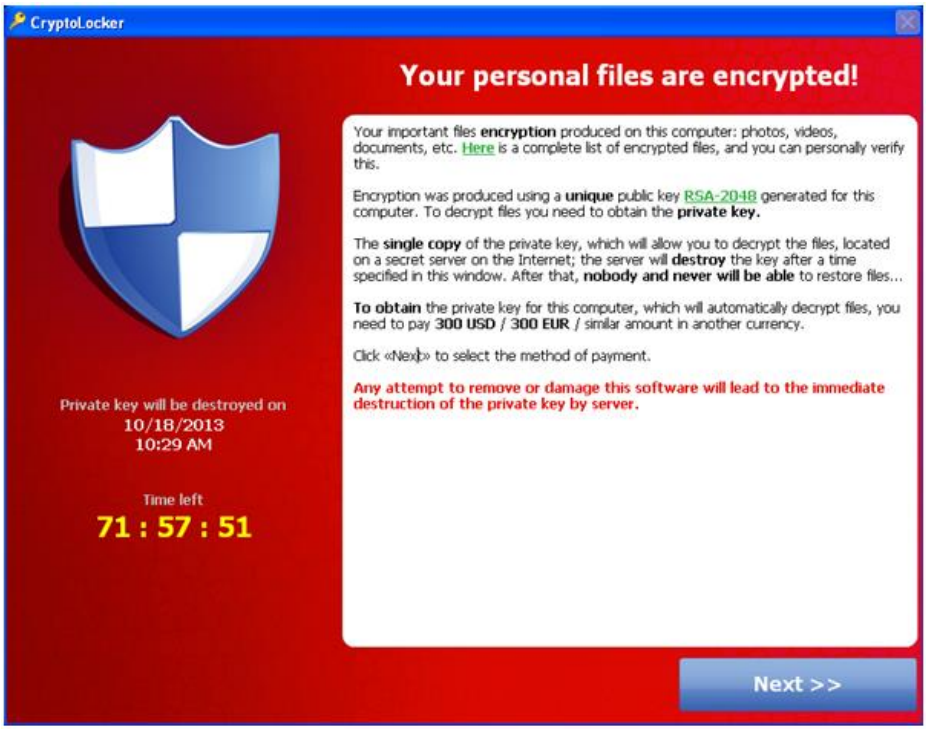
The cryptomalware threat is increasing — Kaspersky Security Network shows that in 2013 about 2.8 million crypto-attacks were registered – that is nine time more than in 2012 – and all the evidence suggests that their number will continue to rise because many people are still willing to pay the ransom. According to a survey, conducted by Interdisciplinary Research Centre in Cyber Security at the University of Kent in February 2014, more than 40% of Cryptolocker victims agreed to pay. Moreover, Dell SecureWorks report shows that the same malware rakes in up to $30 million every 100 days.

Furthermore, the inability to decipher files encrypted by the modern malware spawns an additional threat — false remedy. Desperate users who lose their files search the Internet for any help and sometimes find software that claims to “fix” encrypted data. In the best case, it is a swindle selling a useless ‘solution’; at worst it distributes additional malware.

Evolution of encrypting malware

Criminal methods become more and more sophisticated each year. The first cryptomalware used a symmetric-key algorithm, with the same key for encryption and decryption. Usually, with some help from anti-malware vendors, corrupted information could be successfully deciphered. Then cybercriminals began to implement public-key cryptography algorithms that use two separate keys — public, to encrypt files, and private, which is needed for decryption. One of the first practicable public-key cryptosystems to be used by cybercriminals was called RSA (named after Ron Rivest, Adi Shamir and Leonard Adleman, who first described the algorithm). Back in 2008, Kaspersky Lab's experts managed to crack a 660-bit RSA key used by the GPCode Trojan but soon its authors upgraded key to 1024 bits, making it harder to decrypt.

One of the most recent and most dangerous pieces of cryptomalware, the previously-mentioned Cryptolocker Trojan, also uses a public-key algorithm. After each computer is infected, it connects to the command-and-control server to download the public key, so another key, the private one, is accessible only to Cryptolocker's authors. Usually the victim has no more than 72 hours to pay the ransom before their private key will be deleted forever. It is impossible to decrypt any files without this key. Kaspersky Lab's products successfully detect this Trojan, but if the system is already infected, than nothing can be done with the corrupted files.



Your personal files are encrypted!

Private key will be destroyed on
10/18/2013
10:29 AM

Time left
71 : 57 : 51

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Figure 1. Cryptolocker's ransom demand screen

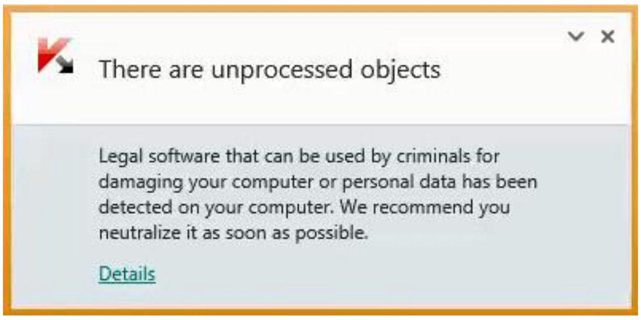
Kaspersky Lab's Cryptomalware Countermeasures Subsystem

At present it is impossible to decipher files encrypted by modern cryptomalware so the only countermeasure that will keep user's data safe is file backup. But general backup, even a regular one, is not enough, because it leaves recently changed files unprotected. That is why Kaspersky Lab developed an alternative countermeasure, based on the System Watcher module.

Kaspersky System Watcher analyses the most relevant system event data, including information on the modification of files. When it registers a suspicious application attempting to open a user's personal files it immediately makes a local protected backup copy of them[1].

[1] *Backed-up files should be no bigger than 10 Mb each*

If the application is then judged to be malicious, Kaspersky System Watcher automatically rollbacks unsolicited changes. Therefore, the user does not need to do anything at all about cryptomalware — there will just be notifications updating the progress of the protection process.

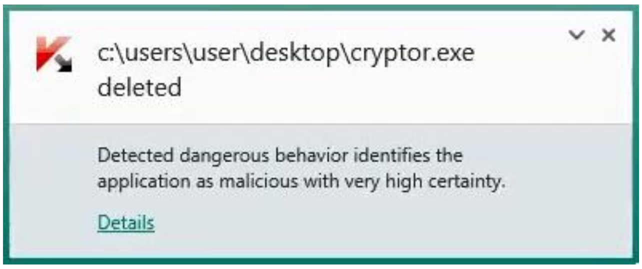


There are unprocessed objects

Legal software that can be used by criminals for damaging your computer or personal data has been detected on your computer. We recommend you neutralize it as soon as possible.

Details

Figure 2. System Watcher finds that an application is making suspicious changes to files and warns the user. At this moment it creates protected backup copies of files and analyses the nature of these changes

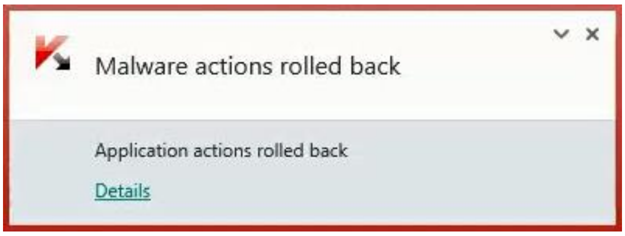


c:\users\user\desktop\cryptor.exe deleted

Detected dangerous behavior identifies the application as malicious with very high certainty.

Details

Figure 3. The application is confirmed as malicious, and file that contains the malware is deleted. Affected files stay encrypted



Malware actions rolled back

Application actions rolled back

Details

Figure 4. System Watcher replaces encrypted files with the backup copies and, when all consequences of the cryptomalware are eliminated, System Watcher reports that all malicious actions were successfully undone

Therefore, even if newly created cryptomalware uses a zero-day vulnerability and manages to avoid all security systems, it will not cause any harm, because any changes it makes will be rolled back automatically. In other words, the cryptomalware countermeasures subsystem keeps user’s data safe and stops the indirect funding of cybercriminals, because paying the ransom will only encourage them to carry on, prompting the creation of more malicious software.

Availability

The Cryptomalware Countermeasures Subsystem is integrated in the System Watcher component, which is part of the following products for home users and business:

For home users

- Kaspersky Internet Security
- Kaspersky Internet Security – Multi-Device (for Windows only)
- Kaspersky Total Security – Multi-Device (for Windows only)
- Kaspersky Anti-Virus

For business

- Kaspersky Endpoint Security for Business
- Kaspersky Small Office Security