VANJA KORAĆ
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,
e-mail: vanja@mi.sanu.ac.rs

ZORAN DAVIDOVAC
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,
e-mail: zorandavidovac@mi.sanu.ac.rs

DRAGAN PRLJA
Institute for Comparative Law,
Terazije 41, Belgrade, Serbia,
e-mail: dprlja@yahoo.com

004.7.056.53:004.491.2
COBISS.SR-ID 228055052

Original research article
Received: April 17th 2016
Accepted: June 20th 2016

RANSOMWARE THREAT TO INFORMATION SYSTEMS

ABSTRACT

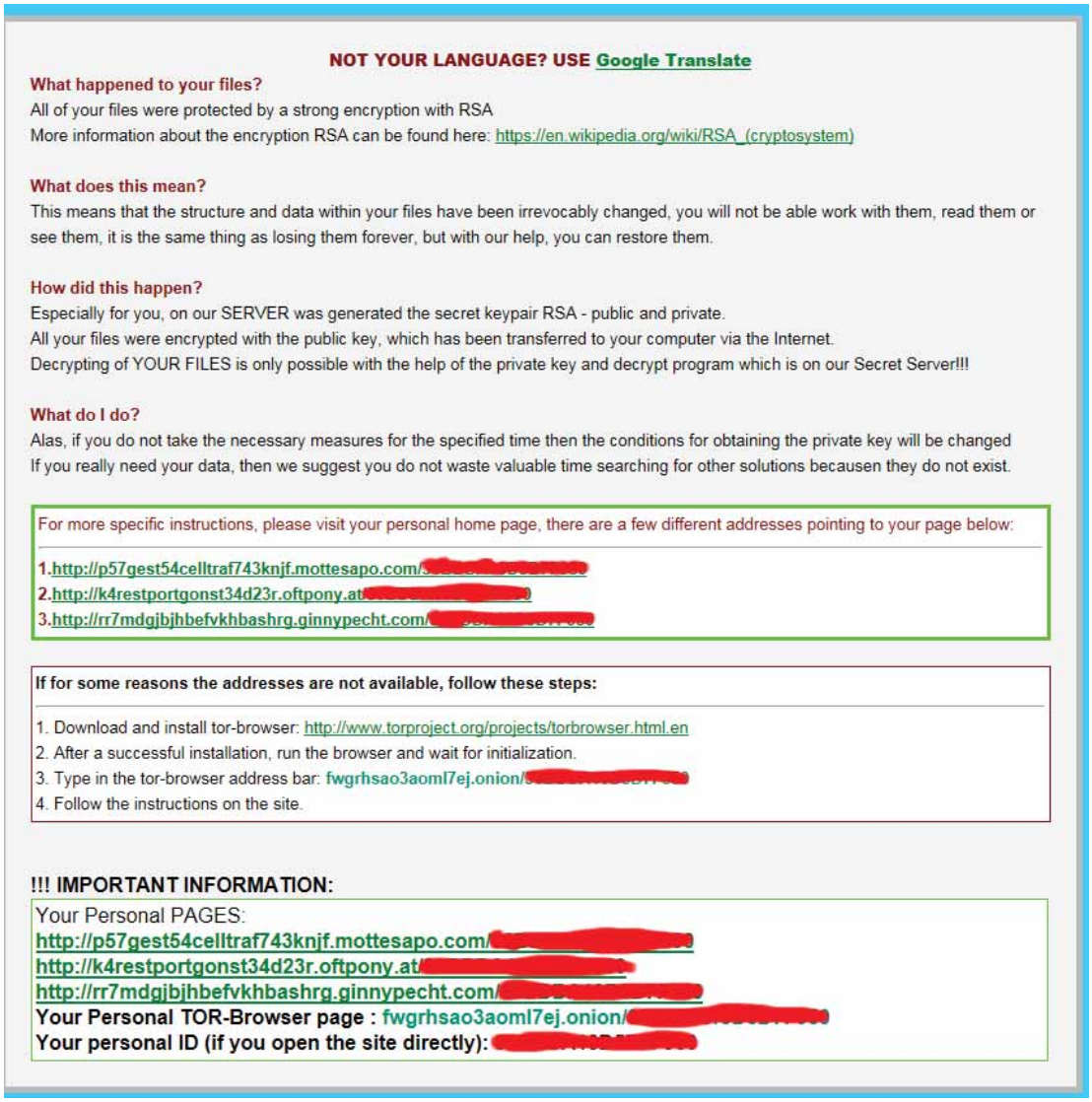
Although a few years ago, it existed as a random threat, crypto ransomware now represents one of the biggest threats in the Internet, endangering data security on operating systems. New technologies, initiating the beginning of mobile communication, the appearance of virtual currenciesand TOR net, formed an environment that enabled ransomware to become even more dangerous. This invasive ransomware, coming in different variations and combinations [Chechik et al. 2016] (Cryptolocker, HydraCrypt, DMA Locker, The Locky, TeslaCrypt 3.0, CryptoWall, The CoinVault, Bitcryptor, TorrentLocker, SynoLocker, Pletoretc.) is now growing, leading to a huge number of infected computers and servers with a Windows environment at providers, organisations, but also in households. In this paper, reliable ways are described to avoid or mitigate the serious damage that can be caused by these malicious threats. Further on, this paper also contains the legal aspects of making and loading malicious crypto ransomware program to a computer.

KEYWORDS: RANSOMWARE, CRYPTO RANSOMWARE, MALICIOUS PROGRAM, INFORMATION SECURITY, SECURITY THREATS, VIRUS THREATS.

MALICIOUS CRYPTO RANSOMWARE PROGRAM[1]

CryptoLocker, or some of its variants, represents a malicious program, belonging to the crypto file type of ransomware. This type of malicious program, or virus, encrypts documents that are placed on an exposed computer system, by using long keys, for example RSA-2048 or RSA-4096, with the encryption algorithm AES CBC 256-bit. After performing document encryption, a window appears on the operating system offering data decryption, but only after a sum of several Bitcoins, actually around $500, is paid within the

1 The article results from the project: *Viminacium, Roman city and military camp – research of material and non- material culture of inhabitants by using the modern technologies of remote detection, geophysics, GIS, digitalization and 3D visualization* (no 47018), funded by The Ministry of Education, Science and Technological Development of the Republic of Serbia.



NOT YOUR LANGUAGE? USE Google Translate

What happened to your files?
All of your files were protected by a strong encryption with RSA
More information about the encryption RSA can be found here: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our SERVER was generated the secret keypair RSA - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program which is on our Secret Server!!!

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed
If you really need your data, then we suggest you do not waste valuable time searching for other solutions becausen they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1.http://p57gest54celltraf743knjf.mottesapo.com/
2.http://k4restportgonst34d23r.oftpony.at
3.http://rr7mdgjbjhbefvkhbashrg.ginnypecht.com/

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the tor-browser address bar: fwgrhsao3aoml7ej.onion/
4. Follow the instructions on the site.

!!! IMPORTANT INFORMATION:

Your Personal PAGES:
http://p57gest54celltraf743knjf.mottesapo.com/
http://k4restportgonst34d23r.oftpony.at/
http://rr7mdgjbjhbefvkhbashrg.ginnypecht.com/
Your Personal TOR-Browser page : fwgrhsao3aoml7ej.onion/
Your personal ID (if you open the site directly):

Fig. 1 File content of recovery+xxkji.html

following 48, 72 or 96 hours, depending on the ransomware variant. Of course, the longer one waits, the more files will be encrypted and the blackmail sum will increase. After exposing computer systems and encrypting files, in cases of ransomware of the TeslaCrypt type (TeslaCrypt v3, Trojan.Cryptolocker.N), information will appear on the desktop in the form of pop-up windows .txt, .png and .html types (recovery+xxkji.html, recovery+xxkji.png, recovery+xxkji.txt), indicating that computer files have been encrypted. These three files will be positioned on computer systems in each folder in which files have been encrypted. These databases contain information about what happened to users' documents, the ways of purchasing the keys necessary to decode the data, as well as links with payment instructions and hints about decoding the documents. The content of all of the three files is the same and is shown in Fig. 1.

All of the encoded documents (images, video files and other personal documents) will possess a new extension, depending on the ransomware type (Teslacrypt, depending on its version, adds encrypted extensions .mp3 **.XXX,** .**TTT, .MICRO, .aaa**, .xyz, .zzz; CryptoLocker adds encrypted extension .7z; Locky adds encrypted extension .locky. CryptoWall does not add an extension

Fig. 2 One of the .js exploited versions that appeared between 11th and 22nd March 2016.

whilst DMA Locker does not add extension to the encrypted file, but adds an identifier in the header of the encrypted file **[unique_id][identifier]. locky** [Abrams 2016]). Documents that can be encrypted by malicious ransomware, depending on its type, are as follows [Pilici 2015]: *.mp4, .mp3, .7z, .m4a, .csv, .d3dbsp, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic,*

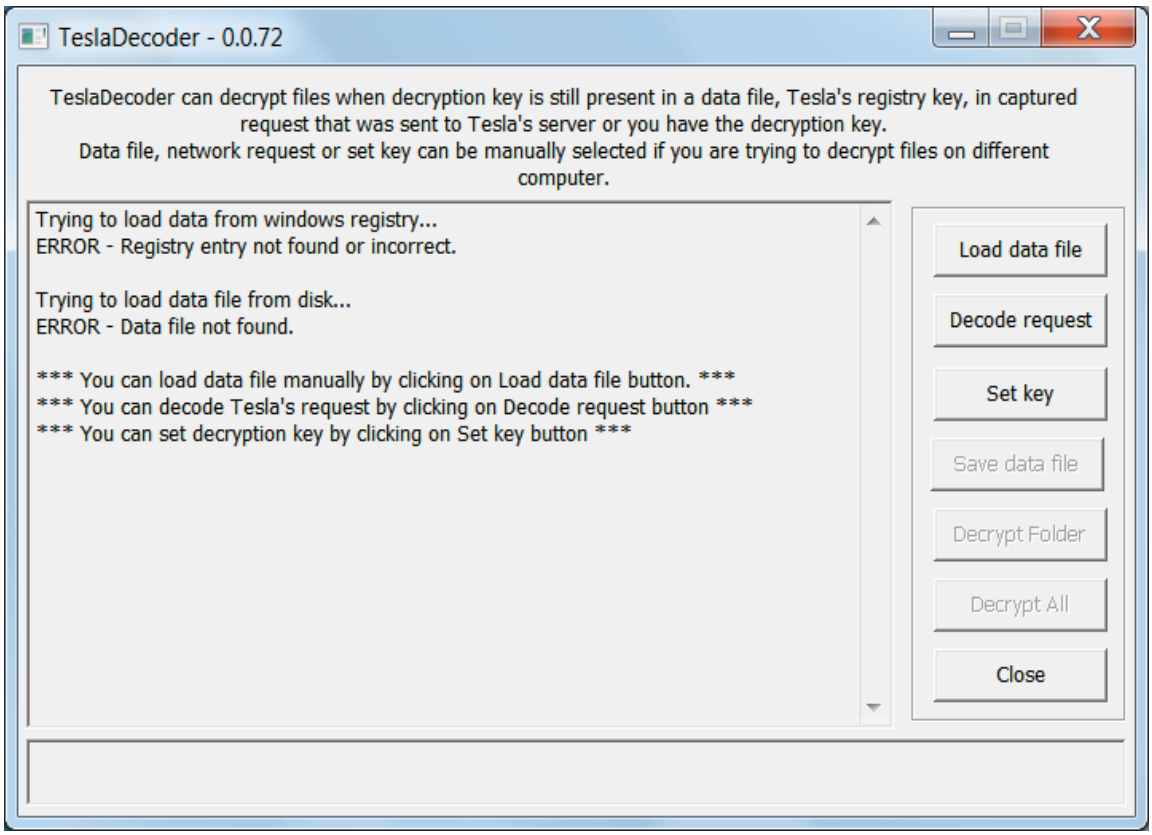
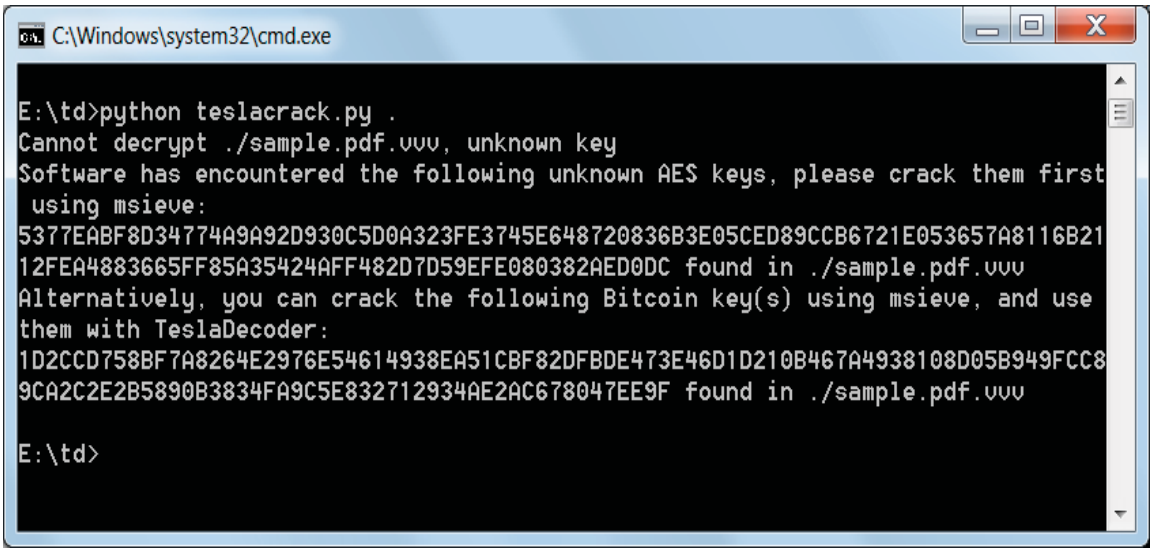


Image BloodDolly TeslaDecoder Source:
(http://www.bleepingcomputer.com/news/security/teslacrypt-decrypted-flaw-in-teslacrypt-allows-victims-to-recover-their-files/)

.bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .map, .wmo, .itm, .sb, .fos, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .js, .css, .rb, .p7c, .p7b, .p12, .pfx, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .cdr, .indd, .ai, .eps, .pdd, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .ppt, .xlk, .xls, .wps, .doc, .odc, .odm, .mid, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .gpg, .aes, .arc, .paq, .tar.bz2, .tbk, .bak, .tar, .tgz, .rar, .zip, .djv, .djvu, .svg, .bmp, .png, .gif, .raw, .cgm, .jpeg, .jpg, .tif, .tiff, .nef, .psd, .cmd, .bat, .class, .jar, .java, .asp, .brd, .sch, .dch, .dip, .vbs, .asm, .pas, .cpp, .php, .ldf, .mdf, .ibd, .myi, .myd, .frm, .odb, .dbf, .mdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .ms11 (security copy), .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wks, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, .hwp, .dotm, .dotx, .docm, .docx, .dot, .max, .xml, .txt, .uot, .pdf, .stw, .sxw, .ott, .odt, .pem, .csr, .crt, .key, wallet.dat, .3g2, .3gp, .c, .gz, .sh,

According to reports by the leading global antivirus companies, most ransomware begins its distribution through phishing attacks, eventually becoming more and more sophisticated, building itself precisely and in a focused manner, in the victim's local language. This malicious program can be found either as an attachment, as an executive file or through a macro virus in a document.



Googulator **TeslaCrack Python Script** Source (http://www.bleepingcomputer.com/news/security/teslacrypt-decrypted-flaw-in-teslacrypt-allows-victims-to-recover-their-files/)

An interesting fact is that if the virus came with the aid of a spam phishing technique, with an attachment as an executive file, the icon appearing to a user on a Windows system is a PDF document [Hassell 2013]. One of the reasons is that in the system, by default, an option "hidden extensions for known file type" is switched on. When, at the end of malicious file name, a malicious attacker adds .pdf (ime.pdf.exe), Windows hides the known .exe extension and the user is deceived into thinking that it is a PDF file from a known sender. This is one of the ways used by encryption ransomware to reach computer systems. The second way it is spread was described by Lawrence Abrams [Abrams 2016]. According to him, this malicious ransomware can be installed on a user's system with the assistance of a malicious macro. For example, an email message containing the "Subject" type:

To: Petar Jovanovic

Subject: Bill number 366

Attachment: name_fajl.doc

Body: Please look at the attachment containing bill to be paid. Detailed specification is contained in the bill.

In other words, the attachment name_file.doc is actually the malicious Word document. When the document is opened, the text will be illegible (although there are variants when the text is legible) and a message will appear on the document, saying that it is necessary to enable a macro in order to make the text legible [Abrams 2016]. Windows will give a warning in the form of Protected View "*Be careful - email attachments can contain viruses. Unless you need to edit, it's safer to stay in Protected View*". The very moment the user enables this malicious macro, the downloading process of the malicious ransomware and the execution from a remote server begins, encrypting those documents with the mentioned extensions.

It should be noted that, in March 2016, an enormous quantity of spam appeared, containing an attachment in java script, with an extension .js. It is specific that until 16th March 2016, none of the known antivirus packages recognised it. The aforementioned .js attachment was of a small size, only 7kb, and appeared to contain only simple text, but it was executed in such a way that the computer would become contaminated [Chechik et al. 2016] [Mendrez 2016].

We should remind ourselves that, on the Internet, there are servers distributing malicious content and, sometimes, it is enough just to click an advertisement for our computer to be contaminated[2].

2 http://www.securitycentral.org.nz/cybersecurity-for-home-internet-users/dealing-with-cryptolocker-ransomware/, accessed on 5th January 2016.

It is worrying that certain encryption ransomware (Locky ransomware) can scan all the local drives, and mapped and unmapped shared net resources, aiming to encrypt documents on them [3] [4]. By encrypting all the documents on the NAS server from a remote server,3 certain ransomware (SynoLocker ransomware) targets NAS (network attached storage) devices and uses the vulnerability of non-updated versions of NAS servers. The trend of accessing and encrypting shared resources with ransomware is expected to continue. This is why extra attention should be paid to licenses when it comes to shared resources, especially those with open shared access, and limit them, in accordance with one's business environment, to the minimum level allowed. Furthermore, there is a danger for data encrypted on a computer to become synchronised with some cloud resources, such as Dropbox and Onedrive, making it possible for data on them to become encrypted.

In addition to, and as a part of, the encryption process, later versions of encryption ransomware also delete the create option and delete all the Shadow Volume copies, as well as copies of the Volume restore on a computer system, in order to prevent the later recovery of a user's documents. To prevent the automatic backup of the Windows volume, they execute the following commands [Cheng 2014]:

-vssadmin.exe Delete Shadows /All /Quiet

Additionally, commands are executed that disable the Windows error recovery startup window:

-bcdedit /set {default} recoveryenabled No

-bcdedit /set {default} bootstatuspolicy ignoreallfailures

In addition, a malicious program will attempt to disable services related to protection, Windows update and information about errors, in order to avoid detection on the system: wscsvc, WinDefend, wuauserv, BITS, ERSvc, WerSvc [Cheng 2014].

PREVENTIVE MEASURES

- Turn on DEP (related to the entire system) - *system properties - performance - settings- data execution prevention - turn on*

- Turn on system protection on other drives - *system properties - system protection - only restore previous versions of files*

- Uncheck the option "*hide extensions for known file types*" as follows: *Organise - folder and search options -view - hide extensions for known file types*. This should be done on every account on a computer, since settings refer only to a specific computer user!!!

IN CASE OF RANSOMWARE CONTAMINATION

Instantly switch off the computer system (each minute of work has another encrypted file as a consequence),

Do not attach USB memory sticks or HDD in order to copy data (switch off PC)

It is necessary to immediately inform colleagues and in organisations it is necessary to inform security staff and the systems administrator, colleagues and friends whose addresses are in your address book about the risk, as well as the police authorities responsible for cyber crime[4].

If a user or an organisation possesses a backup on cd/dvd/blueray/cloud, or, for example, a corporate backup, the data is protected. If there is no backup, the options are as follows:

Attach disc to a Linux work station and make a backup image of discs and files.

Attempt to clean the system with a live version of an antivirus program, eg. Endpoint Symantec protection SERT, using another computer, eg. Linux computer (forensic work station) and use antivirus software. However, there is no guarantee that the computer will be 100% cleaned and the

3 http://www.mcafee.com/us/resources/solution-briefs/sb-quarterly-threat-q1-2015-2.pdf, accessed on 16th February 2016.

4 http://www.securitycentral.org.nz/cybersecurity-for-home-internet-users/dealing-with-cryptolocker-ransomware/, accessed on 5th January 2016.

virus itself fully recognised!

Only after that, attempt to save the data. First try with Shadow explorer and try to recover previous file versions (this action has been useful with some types of ransomware).

Rescued data should be saved to cd/dvd/blueray

The contaminated computer should be re-installed, update the OS, install the latest antivirus and scan the saved cd/dvd/blueray disc.

Experts can recover some data by using the "undelete recovery" function, to recover deleted files, since after file encryption, the originals are deleted. This is a long process and is performed on a computer with a Linux OS or a Mac OS x, since the data is extracted directly from a disc or an image backup disc with specialist programs.

When it comes to Mail servers, it should be forbidden to send executable files. With Linux, for example, this can be performed with procmail, using the following lines:

```
LOGFILE=/var/log/procmail.log
:0
* < 256000
* ! ^Content-Type: text/plain
{
        :0B
        * ^(Content-(Type|Disposition):.*|[
]*(file)?)name=("[^"]*|[^  ]*)\.(bat|cmd|com|exe|-
js|pif|scr)
#3#  /dev/null
        /var/spool/mail/EXE
}
```

At the moment, older versions of TeslaCrypt, possessing a weak point enabling data to be recovered, i.e. decrypted, possess different extensions: .ECC, .EZZ, .EXX, .XYZ, .ZZZ, .AAA, .ABC, .CCC, and .VVV. Later versions, without the aforementioned weak point, can not be decrypted, but they can be recognised by their extensions .xxx, .ttt, .micro and .mp3. For TeslaCrypt 2.0, there are tools that can provide an encryption key, eg. BloodDolly[5] and Googulator scripts6 [Abrams 2016]. In cases when data is encrypted with a later version of TeslaCrypta, perform backup of the data (encrypted) and wait for tools with more up-to-date solutions.

LEGAL ASPECTS OF MAKING AND LOADING A MALICIOUS ENCRYPTION RANSOMWARE PROGRAM

Making and loading malicious programs belongs to the category of unlawful actions against computers and computer systems, actually against confidence, integrity and data and system accessibility. Such crimes are sanctioned according to national laws and their coordination with international legal acts. The most important legal act in Europe, which is coordinated with national laws, is the Council of Europe's Convention on Cybercrime, of 2001. This Convention demands national laws forbidding *illegal access* to information contained on a PC or computer system, aimed at collecting, altering or destroying them. Furthermore, it demands prosecution for *altering data* on a PC, in the sense of partial or complete damage, deletion, the alteration of content, compression or any other method of changing the original data. At first sight, such an act may appear similar to *illegal access*, but it needs to be understood as a complementary act.

In accordance with the Convention on Cybercrime, a definition of illegal computer actions was introduced into Serbian law with the Criminal Law of 20057, Chapter 27, as "crimes against computer data" (paragraphs 298–304a). High technology crime in the sense of this law includes performing illegal actions by using computers, computer networks, computer data, as well as their products in

5 http://download.bleepingcomputer.com/BloodDolly/TeslaDecoder.zip

6 https://github.com/Googulator/TeslaCrack

7 Krivični zakonik, „Sl. glasnik RS", nr. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012 and 104/2013.

material or electronic form, as objects or means of performing illegal actions. In the Criminal Law, the term *computer virus* is defined as a computer program or any similar set of orders entered into a computer or computer network, intended to multiply itself and influence other programs or data on a PC or computer network by adding the program or set of orders to one or more computer programs or data. According to the definition of a malicious program, paragraph 300 of the Criminal Law of Serbia sees it as a special act of *making and loading computer viruses.* A person who makes a computer virus, with the aim of loading it onto a computer or computer network, will be punished with a fine or imprisonment of up to six months. A person who loads a computer virus onto a computer or computer network, and causes damage therein, will be punished with a fine or imprisonment of up to two years. Devices and means used to commit this illegal act will be confiscated.

According to Serbian Criminal Law, in making and loading a malicious encryption ransomware program, an illegal act of *damaging computer data and programs* has been committed (paragraph 298 of the Criminal Law). An unauthorised person who deliberately deletes, alters, damages, hides or in any other way makes computer data or a program useless, will be punished with a fine or imprisonment of up to one year. If the caused damage exceeds RSD 450,000, the criminal will be imprisoned for between three months and three years. If the caused damage exceeds RSD 1,500,000, the criminal will be imprisoned for between three months and five years. Devices and means used to commit this illegal act, if owned by the executor, will be confiscated.

According to the Council of Europe's Convention on Cybercrime, and according to national law, making and entering a malicious encryption ransomware program definitely constitute illegal actions with the accompanying fines and prison terms.

CONCLUSION

At the moment, there is no way to obtain a private key for encoding data without buying it. Although there are antivirus houses that can find an encoding method, such encoders are not universal and are efficient only with targeted ransomware[8]. Since ransomware copies the original file with a coded version, with later versions it even deletes Volume Shadow copies, the only reliable way to recover documents is recovery from a backup. Apart from the aforementioned preventive measures, the best way to protect against ransomware is the implementation of an antivirus system based on endpoint protection[9] (Symantec endpoint protection[10], Sophos Enduser Protection Bundles[11], Kaspersky Endpoint Security[12], McAfee Complete Data Protection13 and others), keeping it updated and installing the latest security patches on a system [Davidovac and Korać 2011]. Proactive protection in the form of making regular backup copies of the most important data onto a device (or network backup location) which is attached only during the backup process will reduce damage to a minimum. The cheapest backup is the use of cd/dvd/blueray or cloud storage (Dropbox, Google drive and others), with the condition that there is no synchronisation (not ascribed as an access letter), while the data upload itself should be done only via a web interface. Backup to USB memory sticks or USB HDD is not advisable, given that these are RW media (it is possible to write data to USB memory sticks or USB HDD).

8 https://noransom.kaspersky.com/

9 Endpoint protection represents a united protection, including antivirus and spyware protection, protection on a network level by recognising malicious traffic and blocking it with its own firewall.

10 https://www.symantec.com/products/threat-protection/endpoint-family/endpoint-protection

11 https://www.sophos.com/en-us/products/enduser-protection-suites.aspx

12 http://www.kaspersky.com/business-security/endpoint-select

13 http://www.mcafee.com/us/products/complete-data-protection-advanced.aspx

BIBLIOGRAPHY

Hassell J.
Cryptolocker: How to avoid getting infected and what to do if you are, Computerworld, October 2013.
http://www.computerworld.com/article/2485214/microsoft-windows/cryptolocker-how-to-avoid-getting-infected-and-what-to-do-if-you-are.html, 25.10.2013

Pilici S.
Remove CryptoLocker virus (Files Encrypted Ransomware), MalwareTips, June 2015.
https://malwaretips.com/blogs/remove-cryptolocker-virus/, 17.6.2015

Abrams L.
The Locky Ransomware Encrypts Local Files and Unmapped Network Shares, Bleeping Computer, February 2016.
http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/ 16.02.2016

Abrams L.
DMA Locker Ransomware targets Unmapped Network Shares, Bleeping Computer, February 2016.
http://www.bleepingcomputer.com/news/security/dma-locker-ransomware-targets-unmapped-network-shares/ 08.02.2016

Mimoso M.
Android Ransomware First to Encrypt Data on Mobile, Threatpost,
https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535/ 9.6.2014.

Cheng B.
CryptoWall – Another Ransomware Menace, Security Research by Fortinet Inc.,
https://blog.fortinet.com/post/cryptowall-another-ransomware-menace, August 05, 2014.

Abrams L.
TeslaCrypt Decrypted: Flaw in TeslaCrypt allows Victim's to Recover their Files, Bleeping Computer,
http://www.bleepingcomputer.com/news/security/teslacrypt-decrypted-flaw-in-teslacrypt-allows-victims-to-recover-their-files/ January 20, 2016

Chechik D., Kenin S. and Kogan R.
Angler Takes Malvertising to New Heights, Spiderlabs Research, March 14, 2016.
https://www.trustwave.com/Resources/SpiderLabs-Blog/Angler-Takes-Malvertising-to-New-Heights/

Mendrez R.
Massive Volume of Ransomware Downloaders being Spammed, Spiderlabs Research, March 9, 2016.
https://www.trustwave.com/Resources/SpiderLabs-Blog/Massive-Volume-of-Ransomware-Downloaders-being-Spammed/

Davidovac Z. and Korać V.
Vulnerability management and patching it systems, Arheologija i prirodne nauke, br. 6, str. 129-144, UDK 007:004.056.5 005.21:004.49, ISSN 1452-7448, Beograd, 2011.

McAfee Defeat Ransomware: Ensure Your Data Is Not Taken Hostage, Solution Brief, Intel Corporation or McAfee, Inc., February 2016.
http://www.mcafee.com/us/resources/solution-briefs/sb-quarterly-threat-q1-2015-2.pdf

REZIME
RANSOMWARE PRETNJA INFORMACIONIM SISTEMIMA

KLJUČNE REČI: RANSOMWARE, ENKRIPTUJUĆI RANSOMWARE, MALICIOZNI PROGRAM, INFORMACIONA BEZBEDNOST, BEZBEDNOSNE PRETNJE, VIRUSNA PRETNJA.

Iako je pre par godina postojao kao sporadična pretnja, enkriptujući ransomware je trenutno jedna od najvećih pretnji na Internetu koja donosi veliku opasnost za bezbednost podataka na računarskim sistemima. Nove tehnologije koje su inicirale prelazak na mobilnu komunikaciju, pojavu virtuelnih valuta i pojavu TOR mreže, oblikovale su okruženje da ransomware bude još opasniji. Ovaj invazivni ransomware koji dolazi u različitim varijantama i kombinacijama [Chechik et al. 2016] (Cryptolocker, HydraCrypt, DMA Locker, The Locky, TeslaCrypt 3.0, CryptoWall, The CoinVault, Bitcryptor, TorrentLocker, SynoLocker, Pletor i dr.) trenutno beleži porast, što za posledicu ima veliki broj zaraženih računara i servera sa Windows okruženjem kako kod provajdera, organizacijama, tako i onih u kućnom okruženju. U samom radu su opisani pouzdani načini da se izbegnu ili da se ublaže, vrlo ozbiljne štete koje ove zlonamerne pretnje mogu da izazovu. Takođe, ovim radom su obuhvaćeni i pravni aspekti pravljenja i unošenja zlonamernog enkriptujućeg programa ransomware na računar.