ENGENSEC
Educating the Next generation
experts in Cyber Security

Android Ransomware: Turning CryptoLocker into CryptoUnlocker

Alexander Adamov
NioGuard Security Lab
nas.nioguard.com

Demo: Android SimpleLocker

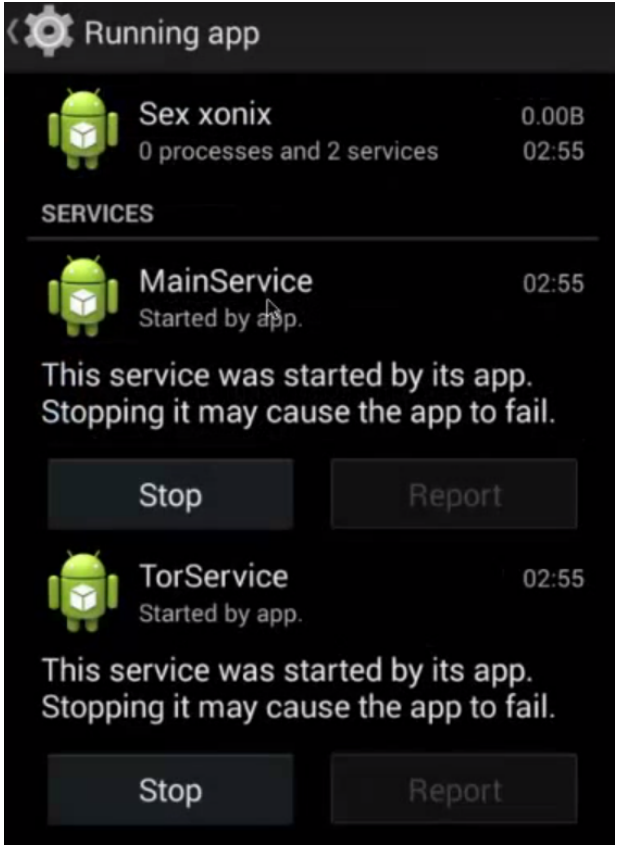
WARNING your phone is locked!
The device is locked for viewing and distribution child pornography , zoophilia and other perversions.

To unlock you need to pay 260 UAH.

1. Locate the nearest payment kiosk.
2. Select MoneXy
3. Enter 380982049193.
4. Make deposit of 260 HRN, and then press pay.

Do not forget to take a receipt!
After payment your device will be unlocked within 24 hours.

In case of no PAYMENT YOU WILL LOSE ALL DATA ON your device!"



Versions

TeslaCrypt - is a family of ransomware encryptors

- Feb 2015 - first detected
- Jul 2015 - TeslaCrypt 2.0.0 discovered by Kaspersky Lab
- Aug 2015 - TeslaCrypt 2.0.5 report
- Sep 2015 - TeslaCrypt 2.1.0 - the latest discovered

Threads

5 threads are running to implement:

- terminating processes (msconfig, regedit, procexp, taskmgr)
- encrypting files
- removing shadow copies of files using vssadmin.exe
- connecting to the Internet

Encrypts files with extensions

.r3d .css .fsh .lvl .p12 .rim .vcf .3fr .csv .gdb .m2 .p7b .rofl .vdf .7z .d3dbsp .gho .m3u .p7c .rtf .vfs0 .accdb .das .hkdb .m4a .pak .rw2 .vpk .ai .dazip .hkx .map .pdd .rwl .vpp_pc .apk .db0 .hplg .mcmeta .**pdf** .sav .vtf .arch00 .dba .hvpl .mdb .pef .sb .w3x .arw .dbf **.ibank** .mdbackup .pem .sid .wb2 .asset .dcr .icxs .mddata .pfx .sidd .wma .avi .der .indd .mdf .pkpass .sidn .wmo .bar .desc .itdb .mef .png .sie .wmv .bay .dmp .itl .menu .ppt .sis .wotreplay .bc6 .dng .itm .mlx .pptm .slm .wpd .bc7 **.doc** .iwd .mov .pptx .snx .wps .big .docm .iwi .mp4 .psd .sql .x3f .bik **.docx** .jpe .mpqge .psk .sr2 .xf .bkf .dwg .jpeg .mrwref .pst .srf .xlk .bkp .dxg .jpg .ncf .ptx .srw .xls .blob .epk .js .nrw .py .sum .xlsb .bsa .eps .kdb .ntl .qdf .svg .xlsm .cas .erf .kdc .odb .qic .syncdb .xlsx .cdr .esm .kf .odc .raf .t12 .xxx .cer .ff .layout .odm .rar .t13 **.zip** .cfr .flv .lbf .odp .raw .tax .ztmp .cr2 .forge .litemod .ods .rb .tor .crt .fos .lrf .odt .re4 **.txt** .crw .fpk .ltx .orf .rgss3a .upk

Exclusions:

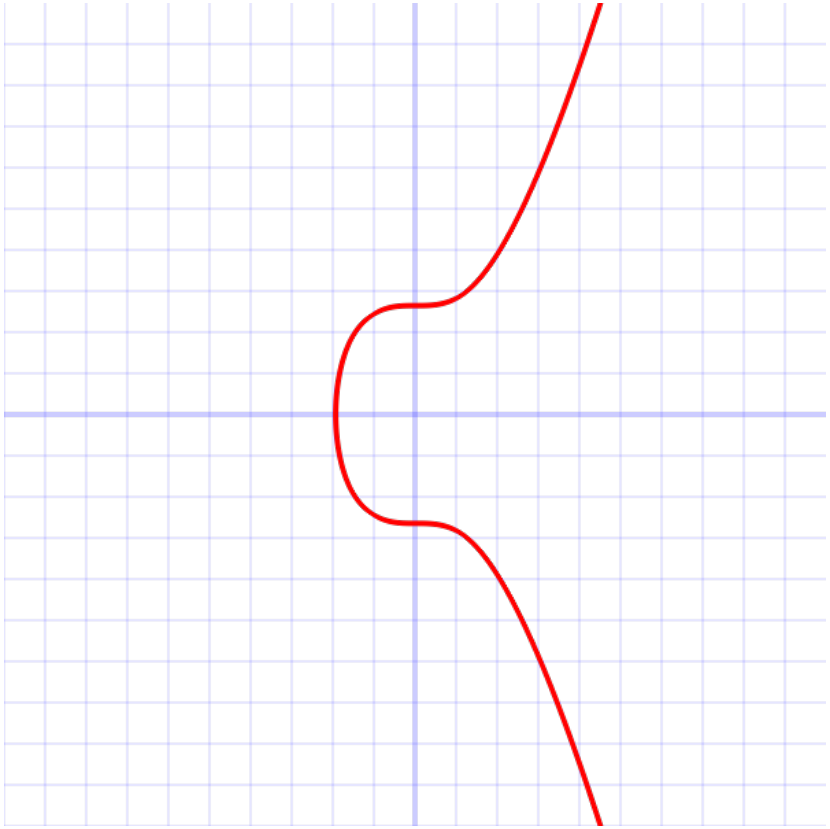
- %Windows%
- %Program Files%
- %Application Data%

Demo: File Encryption

ECDH

https://en.bitcoin.it/wiki/Secp256k1

$y^2 = x^3 + 7$



ECDH Keys

Session	Bitcoin	Attacker
• **session_priv** (aes_key[256]) - generated • **session_btc_pub**[520] = session_btc_priv*G - saved in an encrypted file • **session_ecdh_secret**[1024] =ECDH(master_btc_pub, session_priv) • **session_ecdh_secret_mul**[1024] =session_ecdh_secret* session_priv - saved in enc file	• **master_btc_priv**[256] - sent to C&C -> • **master_btc_pub**[520] = master_btc_priv*G - saved in an encrypted file • **master_ecdh_secret**[1024] =ECDH(master_btc_priv, malware_priv) • **master_ecdh_secret_mul**[1024] =master_ecdh_priv * session_priv) - saved in file and sent to C&C ->	• **malware_priv** • **malware_pub**

**Names for keys conform to Securelist.com article*
** G - is a generator (base point) on secp256k1*

File Encryption Key

- AES-256-CBC
- key expansion to: 1920 bits
- encryption blocks: 128 bits

C&C domains

http://josemanuelegea.es/wp-content/themes/the-newswire/misc.php

http://bostonhygiene.com/wp-content/plugins/quick-setup/misc.php

http://arborvictoria.com/wp-content/plugins/dropdown-menu-widget/misc.php

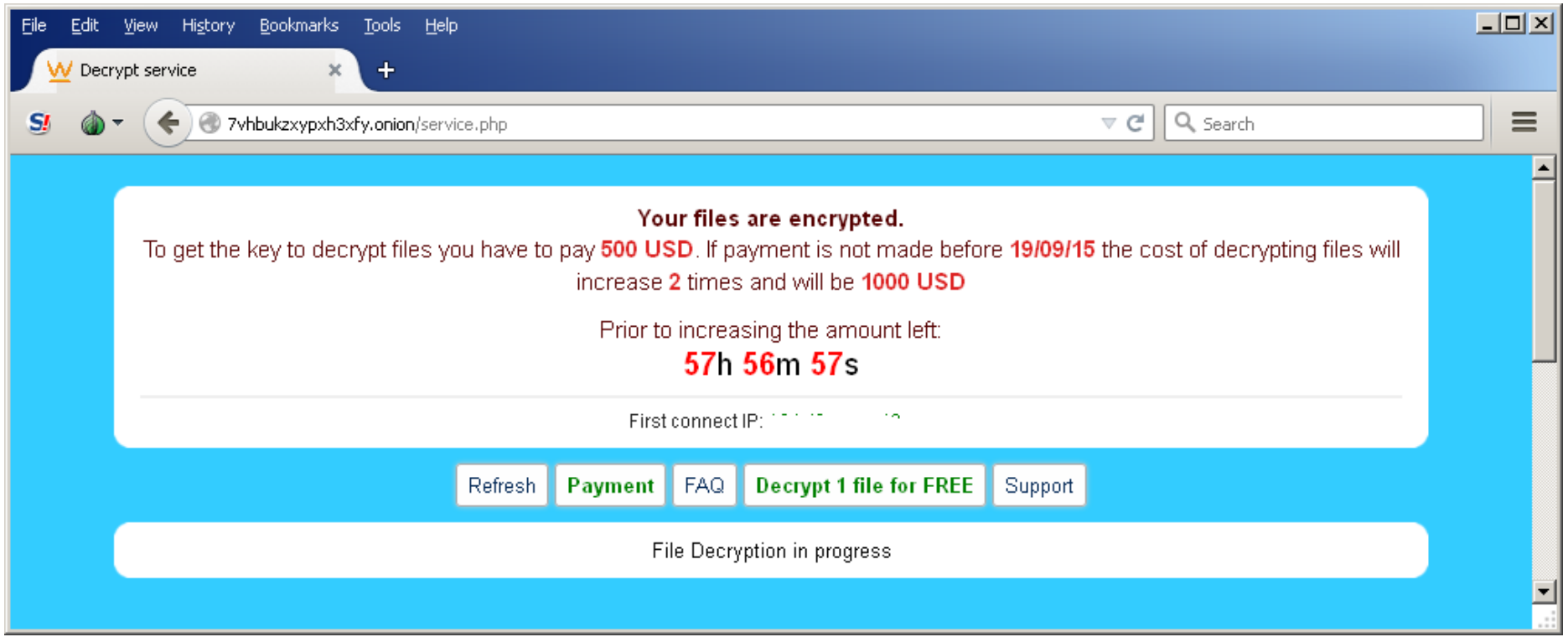
http://myconsulting.es/wp-content/plugins/post-notification/misc.php

http://prettybaked.pl/wp-content/plugins/share-buttons-wp/misc.php

Cracked URL

?
Sub=Crypted&key=AB5BCBA43DAEDE8DE7FF27BFD7B7B13A903C65117A012A64F5687C23DADB8D68&dh=31014602AAD8BDF6297C6FD6B0876A1C2685C1C9F6443D913DB93A300F7C0CB6442CA9B487984A40F2EBF191E6881AD3389A43FA9C057FD128ECC220F2F1BA2E&addr=1ESpfMvFNuR8E726bZZFnv4qrkE2LL5wY8&size=116&version=2.1.0&OS=2600&ID=39&gate=josemanuelegea.es&ip=194.47.155.162&inst_id=9F883CBCD898366B

Decryption Service



Demo: Cracking “Ping” Message

Questions?

Watch more about Android SimpleLocker on Youtube:
https://www.youtube.com/watch?v=dFXqMFsgutg
https://www.youtube.com/watch?v=0CfWXDaNA_0

Read more about TeslaCrypt 2.1 in the NioGuard Blog:
http://nioguard.blogspot.com/

Email: ada@nioguard.com