It’s a file infector…
It’s ransomware…
It’s VIRLOCK

Vlad Craciun
Mihail Andronic
Andrei Nacu

Bitdefender

Overview

- Ransomwares and file infectors
- Introducing Virlock
- Reversing Virlock
- Statistics
- Conclusions

Bitdefender

Background

- Most malware on today market, combine all sort of mechanisms to collect/damage user data or to deploy other kinds of malware
- Virlock = Ransomware + Fileinfector
- Damaged files and no PC access?

Ransomwares and file infectors

- Ransomwares
  - Purpose
    - Get money by blocking data or account access
  - Behavior
    - File-lockers
    - Screen-lockers

Ransomwares and file infectors

Screen locker – ICEPOL

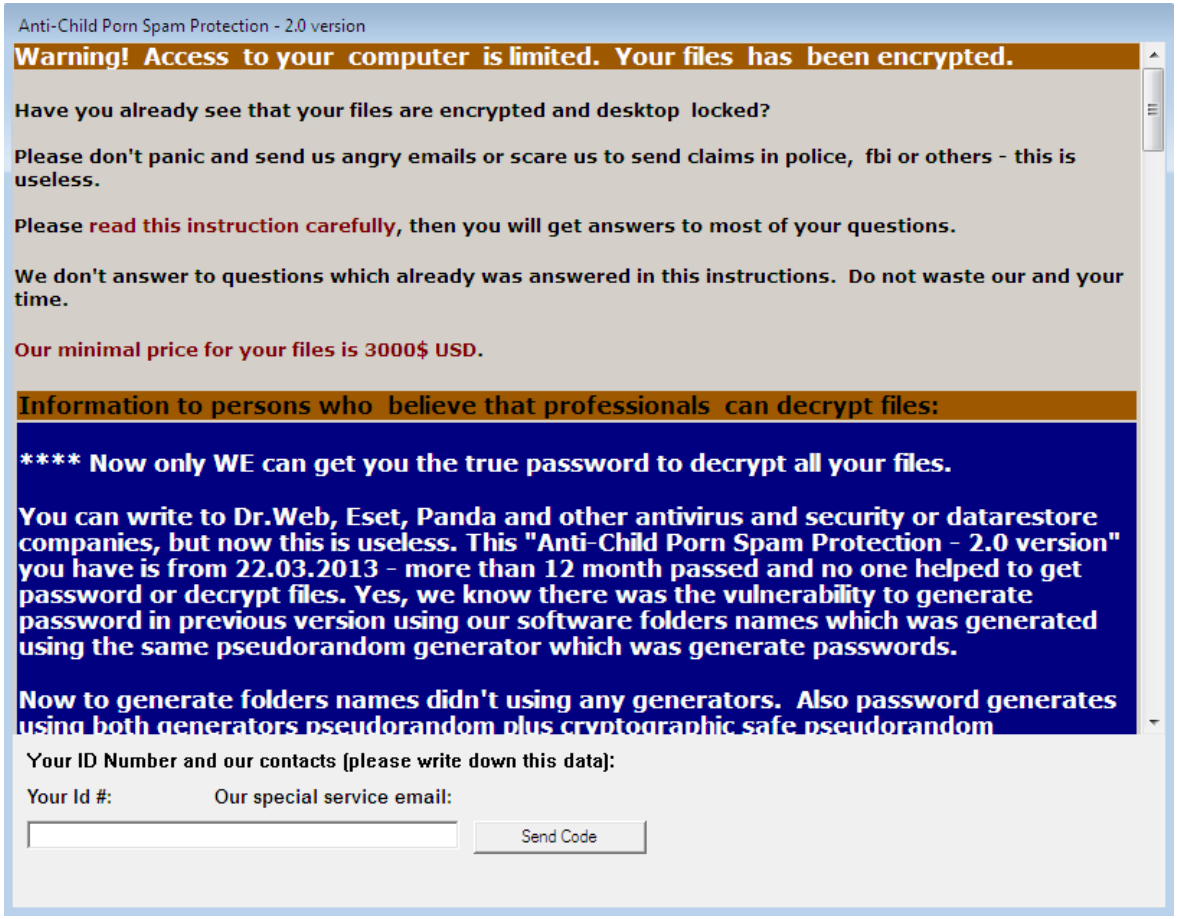
Bitdefender

Ransomwares and file infectors

- File locker – A custom one, similar to Cryptowall

Ransomwares and file infectors

- Both file and screen locker - ACCDFISA



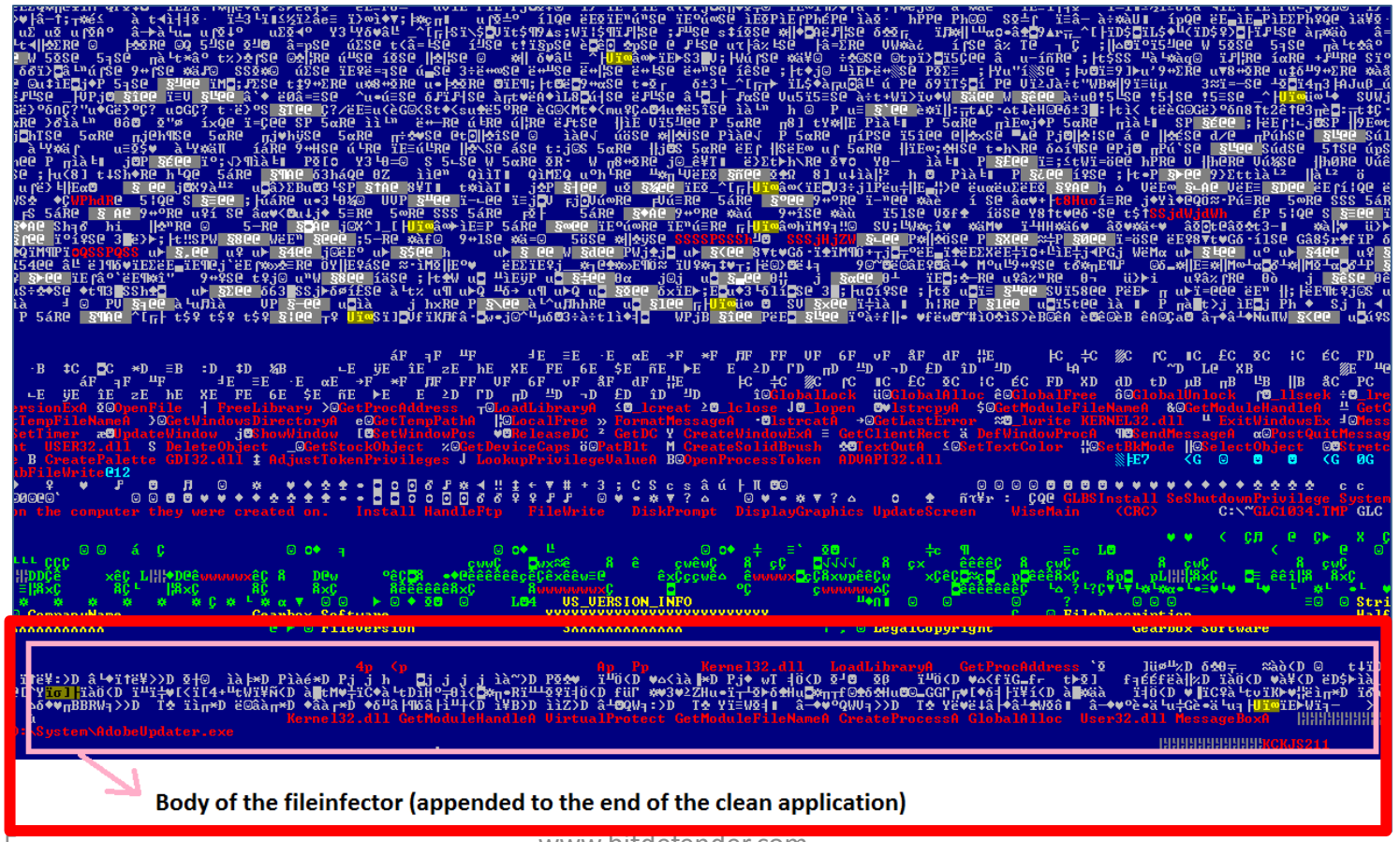
Bitdefender

Ransomwares and file infectors

- File infectors
  - Purpose
    - Delivery and persistence of malware
  - Behavior
    - Alters the legit file by adding the malware payload

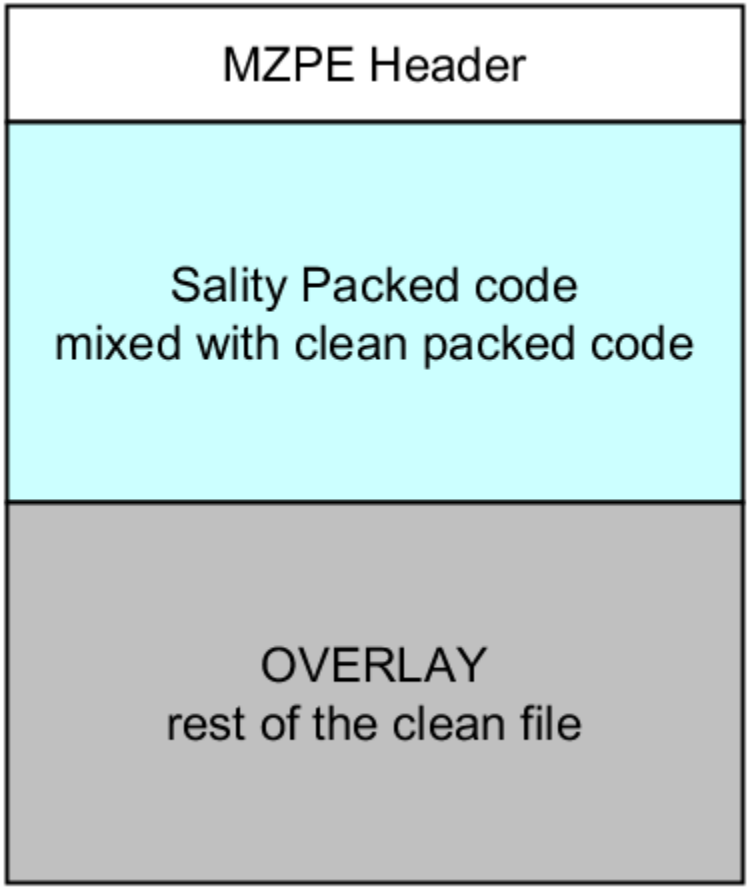
Ransomwares and file infectors

- A simple fileinfector: Pioneer



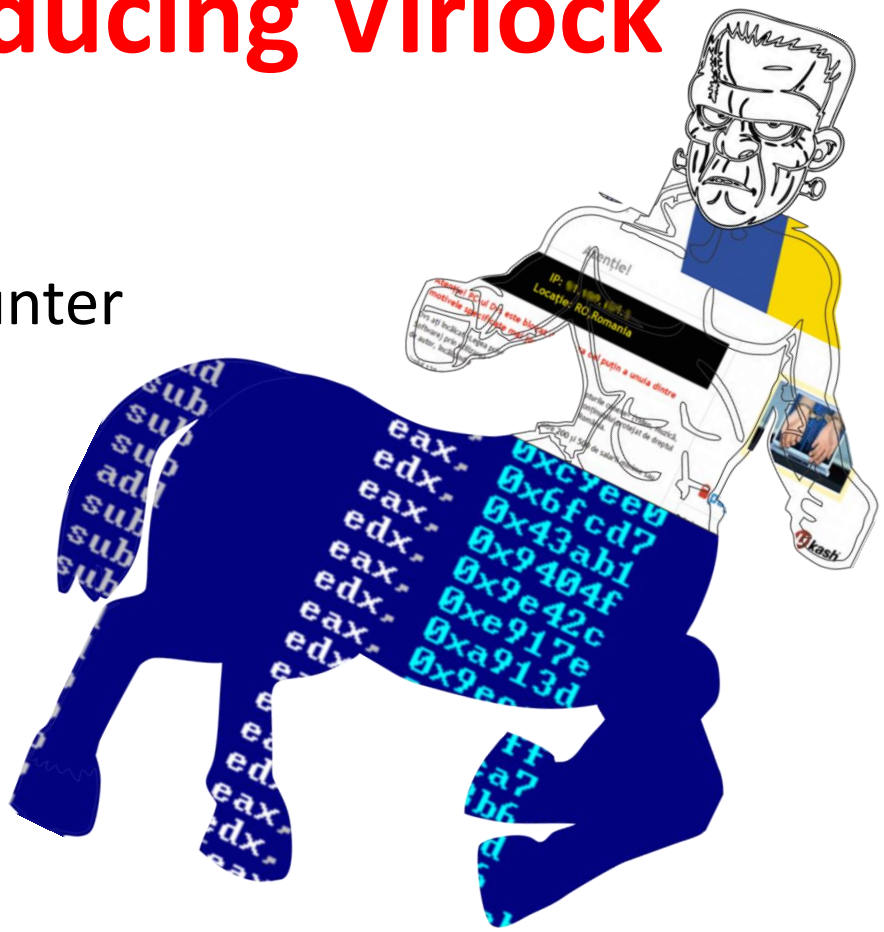
Ransomwares and file infectors

- A more complex one: Sality



Introducing Virlock

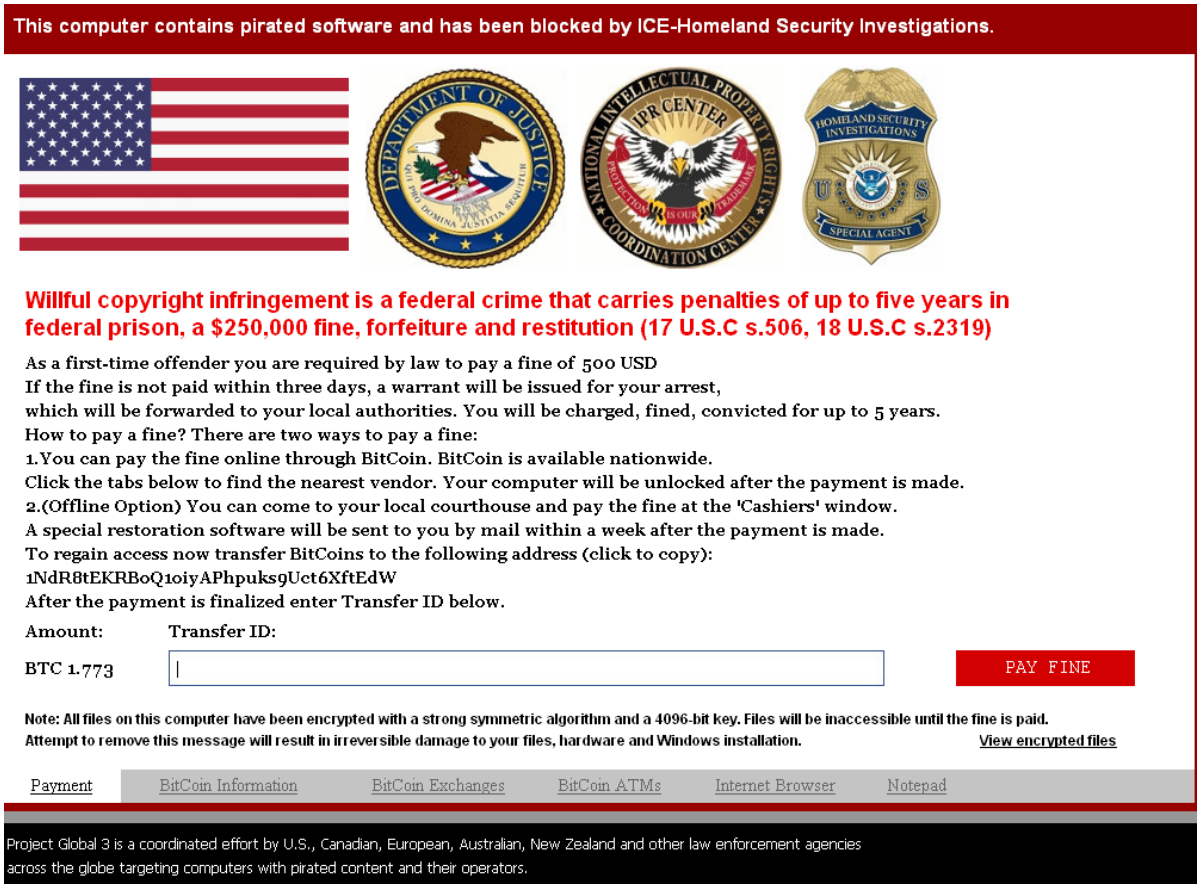
- Virlock
  - hybrid money hunter



- How?
  - Using ransomware screen-locking features
  - Using a well designed infection mechanism

Introducing Virlock

- Screen locking feature similar to ACCDFISA, ICEPOL, etc.



Bitdefender

Introducing Virlock

File infection techniques

- Make files harder to recover
- Increases chances to persist and spread

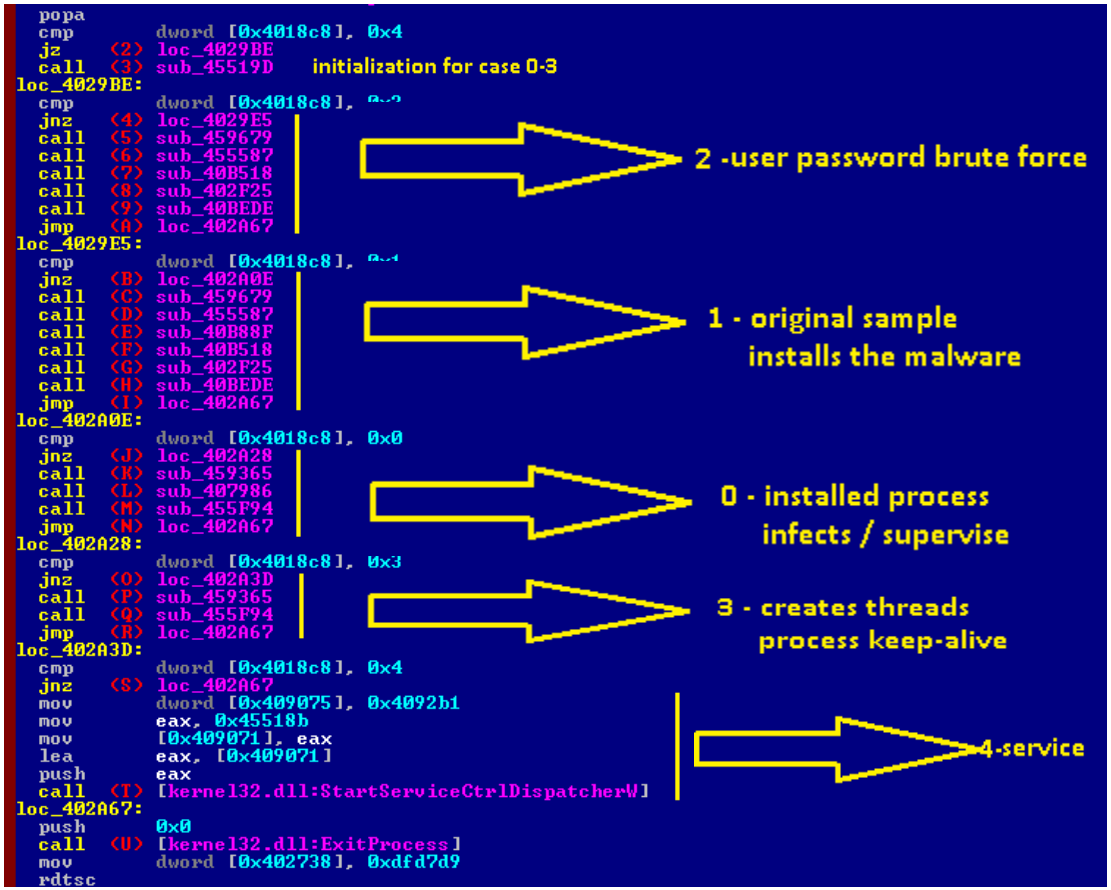
Bitdefender

Reversing Virlock

- Malware installation
- Account password brute-force
- Infected files
- Anti-analysis tricks
- Polymorphic engine
- Different malware versions
- Tricking users

Malware installation

- Setting up the execution environment



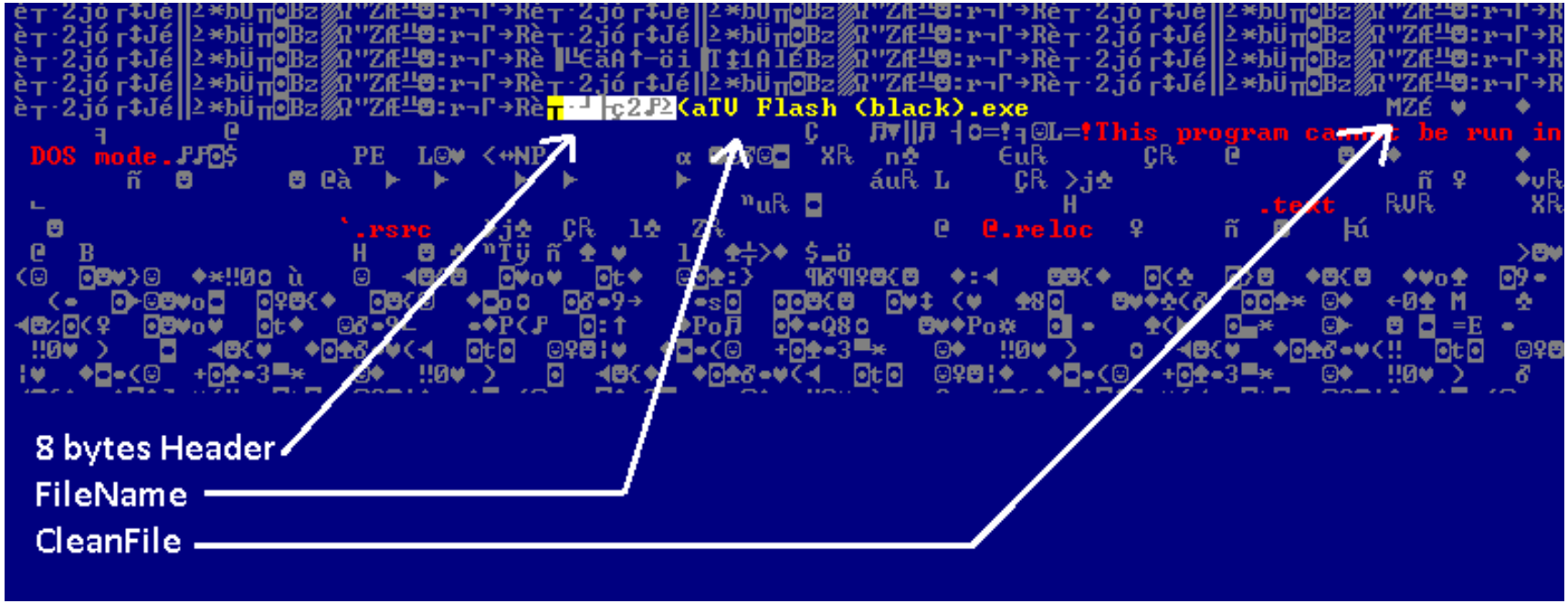
Malware installation

- Executing a fresh infected file

```
  push      dword [0x40170c]
  pop       dword [0x4016f4]
  call  (1) sub_4014A4
  call  (2) sub_40173C
  cmp       dword [0x4016fc], 0x1   Fresh Run of Infection
  jnz   (3) loc_401426
  mov       eax, [0x401704]         Sizeof(Filename)
  add       eax, [0x401708]                 Sizeof(MalwareCode)
  lea       edi, [0x401000]         Absolute address for all operations
  add       edi, [0x401700]          Sizeof(CleanFile)
  add       edi, [0x4016f8]                 Sizeof(DecriptionCode)
  add       edi, 0x8               Sizeof(HeaderStructure)
  mov       ebx, [0x401714]
  mov       [0x4016ec], eax
  mov       [0x4016f0], edi
  mov       [0x4016f4], ebx
  call  (4) sub_4014A4               Decrypt clean file
loc_401426:
  call  (5) sub_401A84
  cmp       dword [0x4016fc], 0x0
  jz    (6) loc_40143D
```

Malware installation

- Getting to the embedded clean file



Account password brute-force

- Malware is trying some kind of dictionary brute force attack in an attempt to gain administrative privileges
- It creates it's own account after that

Bitdefender

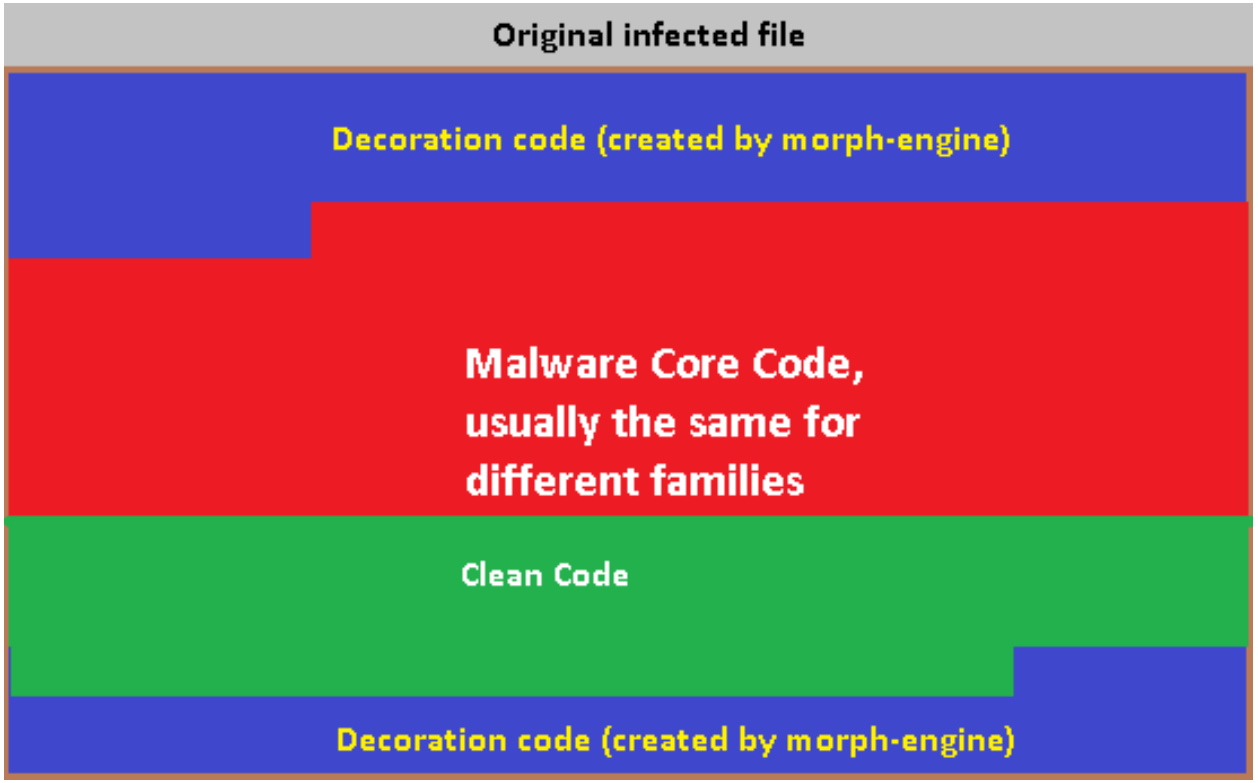
Account password brute-force

- A couple of tried passwords

1qaz@WSX	Password	Passw0rd	orig_Administrator
12345678	P@ssw0rd	p@ssw0rd	operator123
changeme	Password1	Pa$$w0rd	N0th1n9
P@ssword	12345	Abc123	1q2w3e4r5t6y7u8i
Password!	123456789	Qwerty	abcd12345
Passw0rd	1234	Master	Administrator
1q2w3e4r	123456	Password1	Q1w2e3r4
Password01	Admin	welcome	q1w2e3r4t5

Infected files

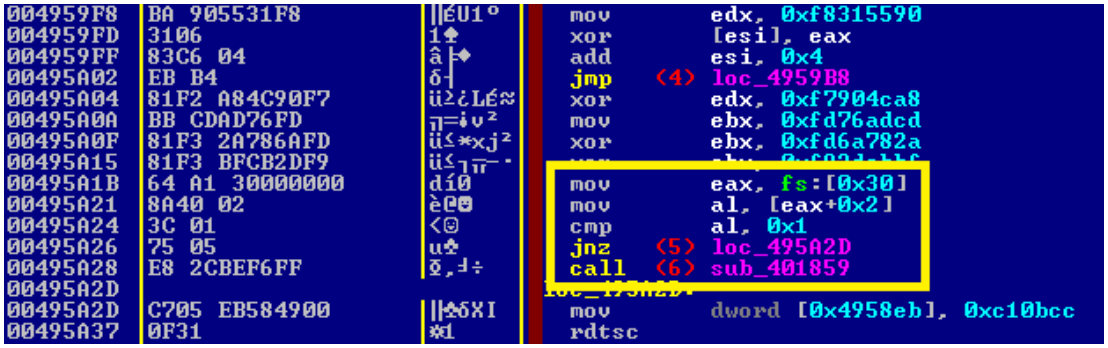
- Clean files are embedded inside the malware
- The path to the clean file is obfuscated
- Similar to Sality

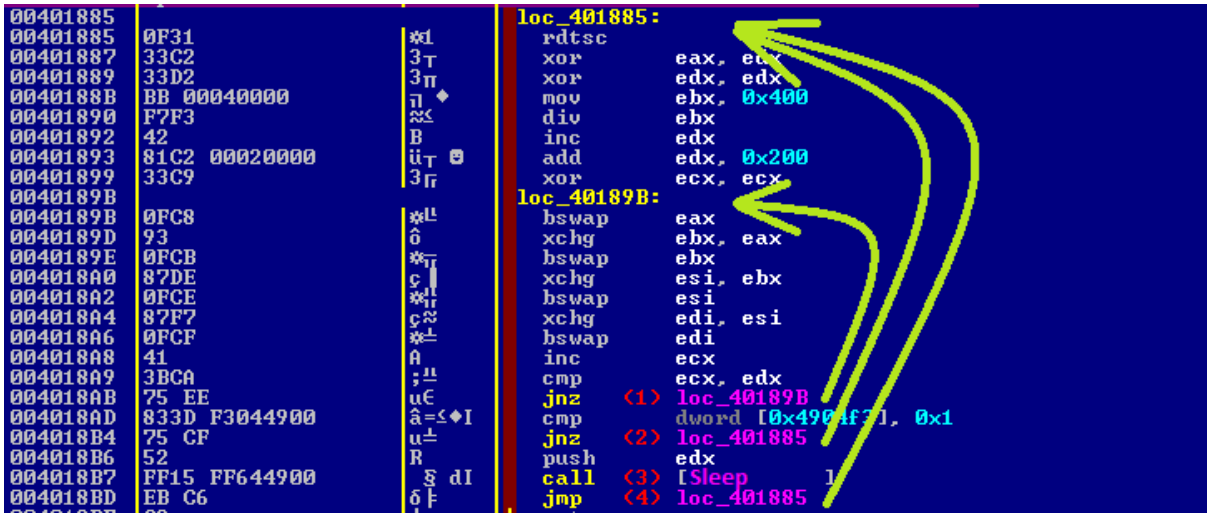


Bitdefender

Anti-analysis tricks

- Detecting the debugger presence

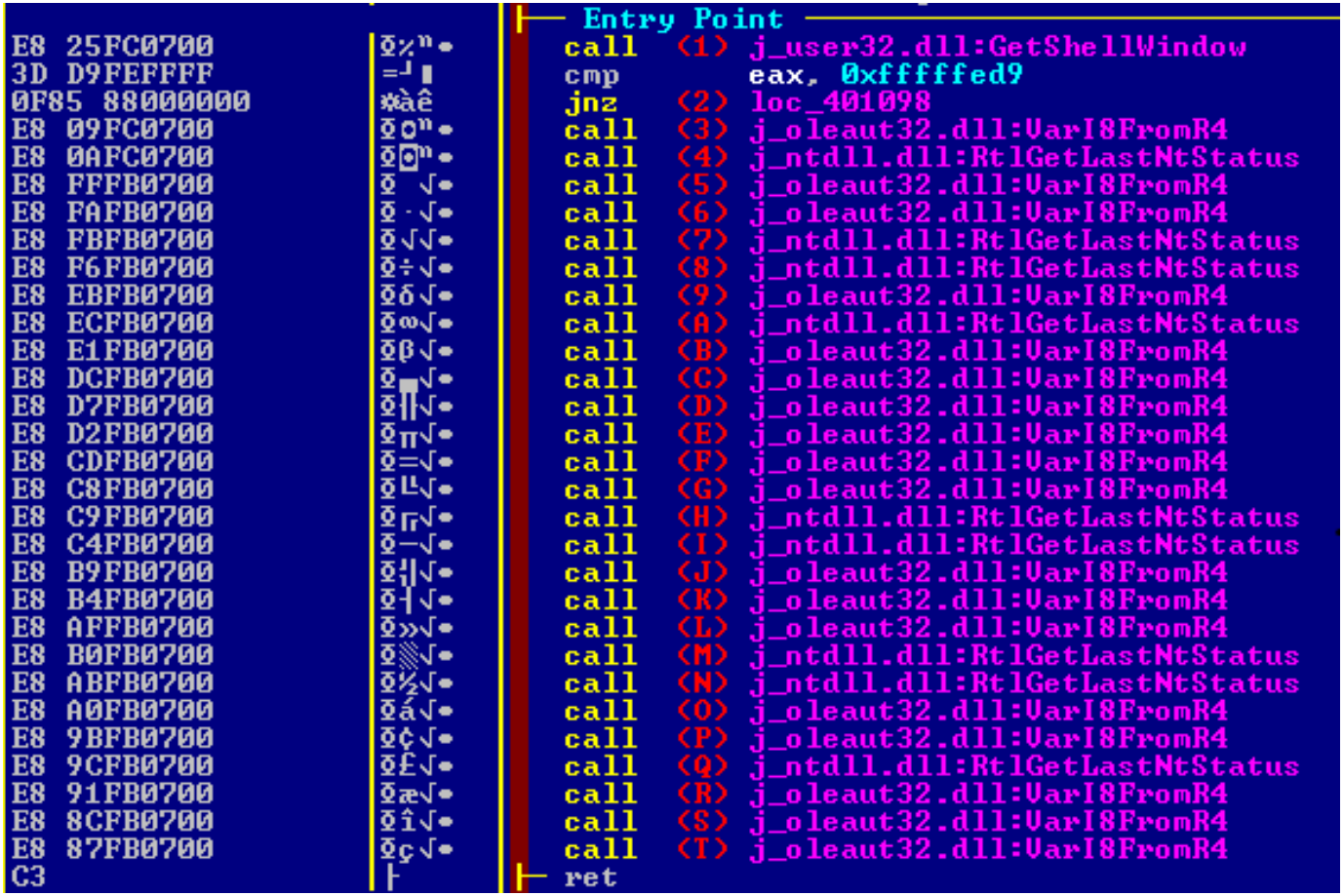




Bitdefender

Anti-analysis tricks

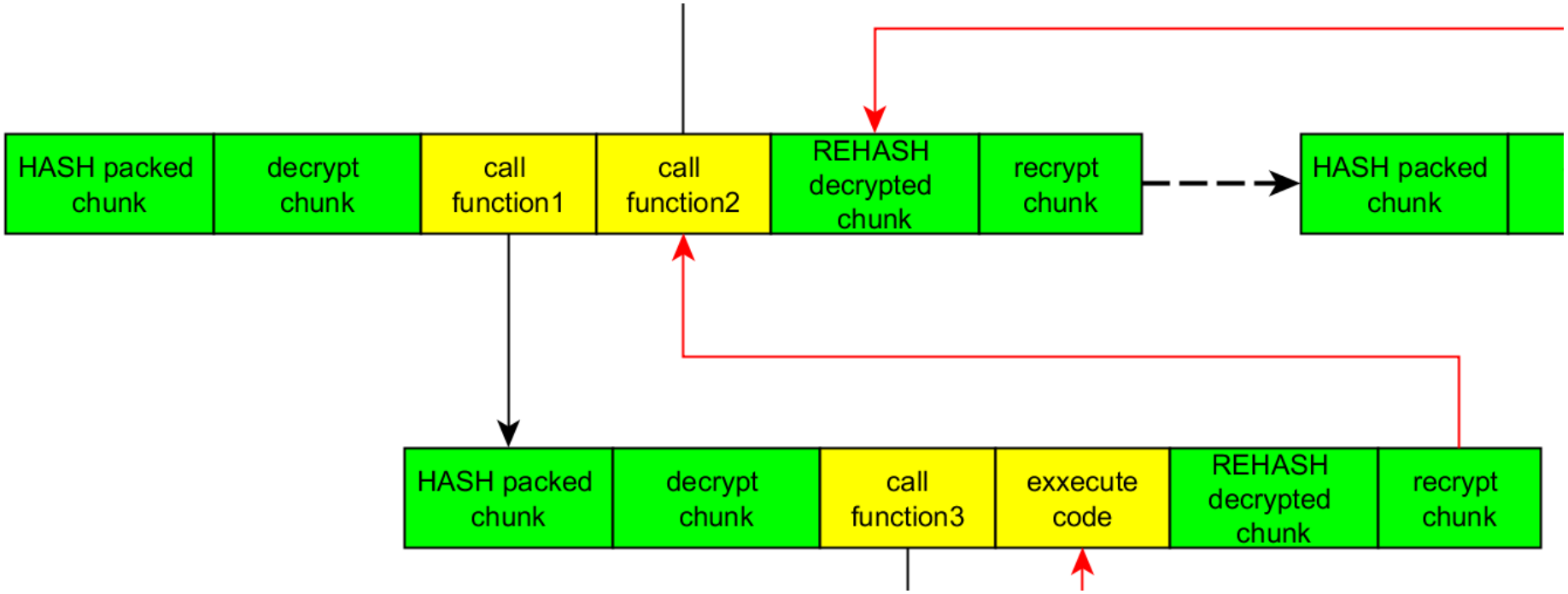
- Anti emulation tricks!



Bitdefender

Anti-analysis tricks

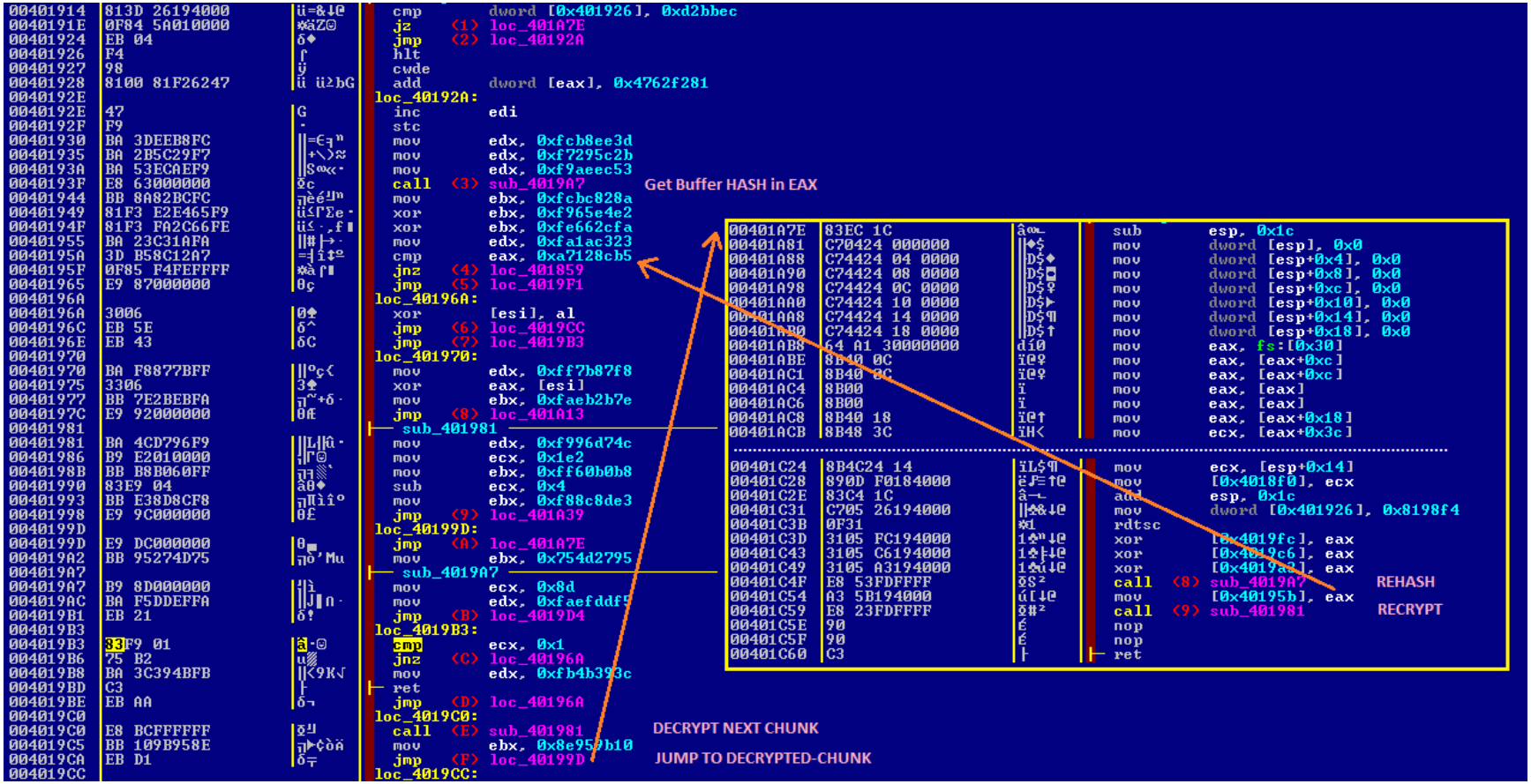
- Decrypt → Execute → Re-Encrypt



Bitdefender

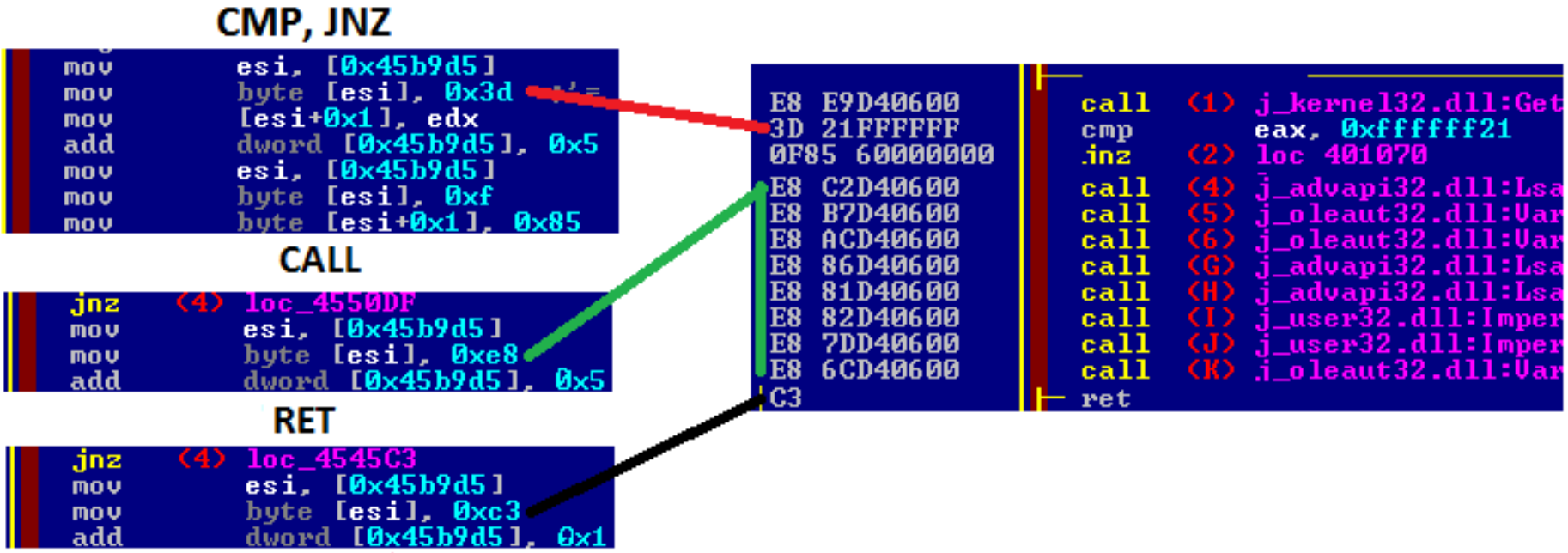
Anti-analysis tricks

- Decrypt → Execute → Re-Encrypt



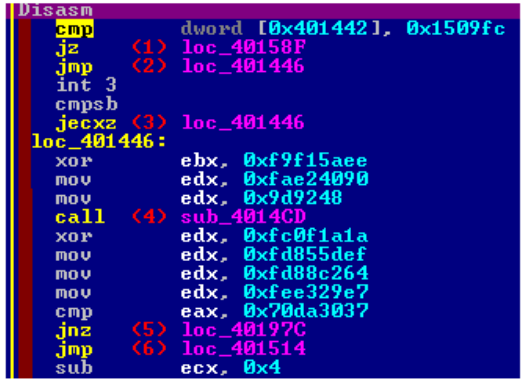
Polymorphic engine

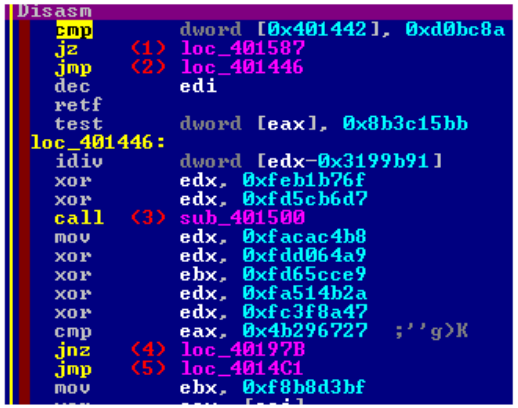
- Basic reshape technique

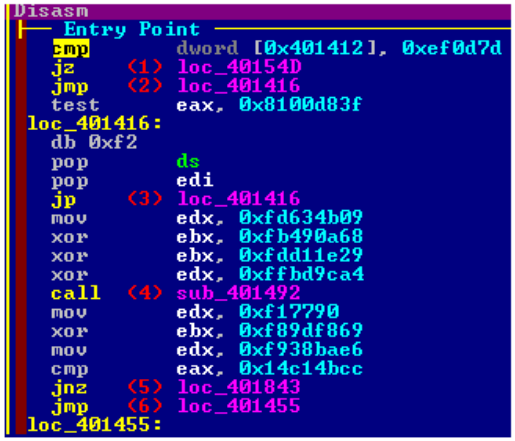


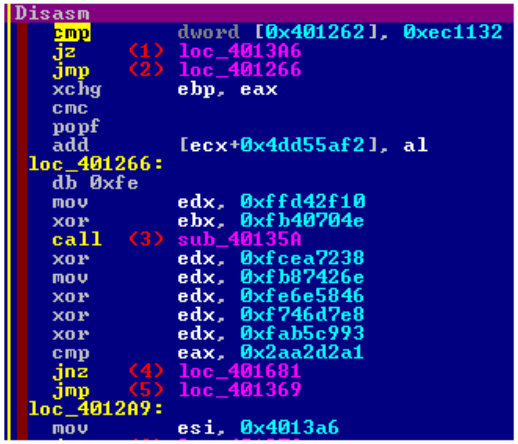
Different malware versions

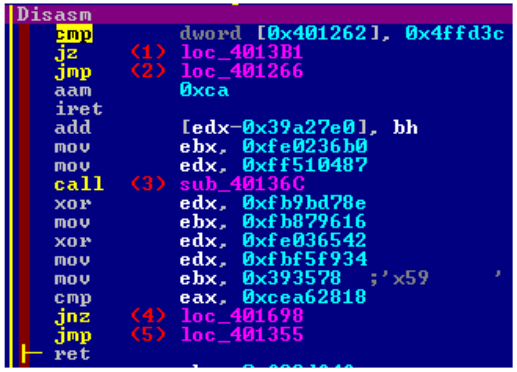
- [Hash encrypted code, compare hash] - template











Bitdefender

Different malware versions

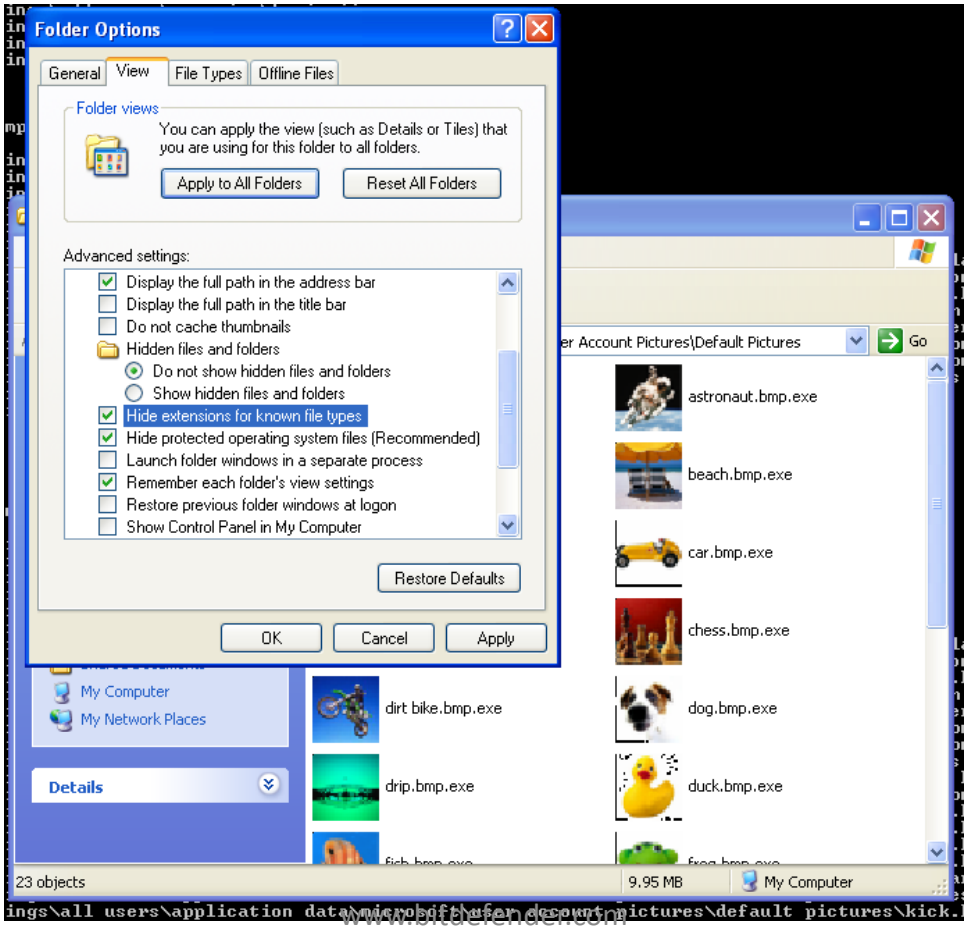
- Similar code within 2 different families

```
CALL v2.00401735
CALL v2.00401A66
CMP DWORD PTR DS:[401A26],1
JNZ SHORT v2.00401677
MOV EAX,DWORD PTR DS:[401A2E]
ADD EAX,DWORD PTR DS:[401A32]
LEA EDI,DWORD PTR DS:[401400]
ADD EDI,DWORD PTR DS:[401A2A]
ADD EDI,DWORD PTR DS:[401A22]
ADD EDI,8
MOV EBX,DWORD PTR DS:[401A3E]
```

```
CALL v1.00401741
CALL v1.00401A63
CMP DWORD PTR DS:[401A23],1
JNZ SHORT v1.0040167D
MOV EAX,DWORD PTR DS:[401A2B]
ADD EAX,DWORD PTR DS:[401A2F]
LEA EDI,DWORD PTR DS:[401400]
ADD EDI,DWORD PTR DS:[401A27]
ADD EDI,DWORD PTR DS:[401A1F]
ADD EDI,8
MOV EBX,DWORD PTR DS:[401A3B]
```

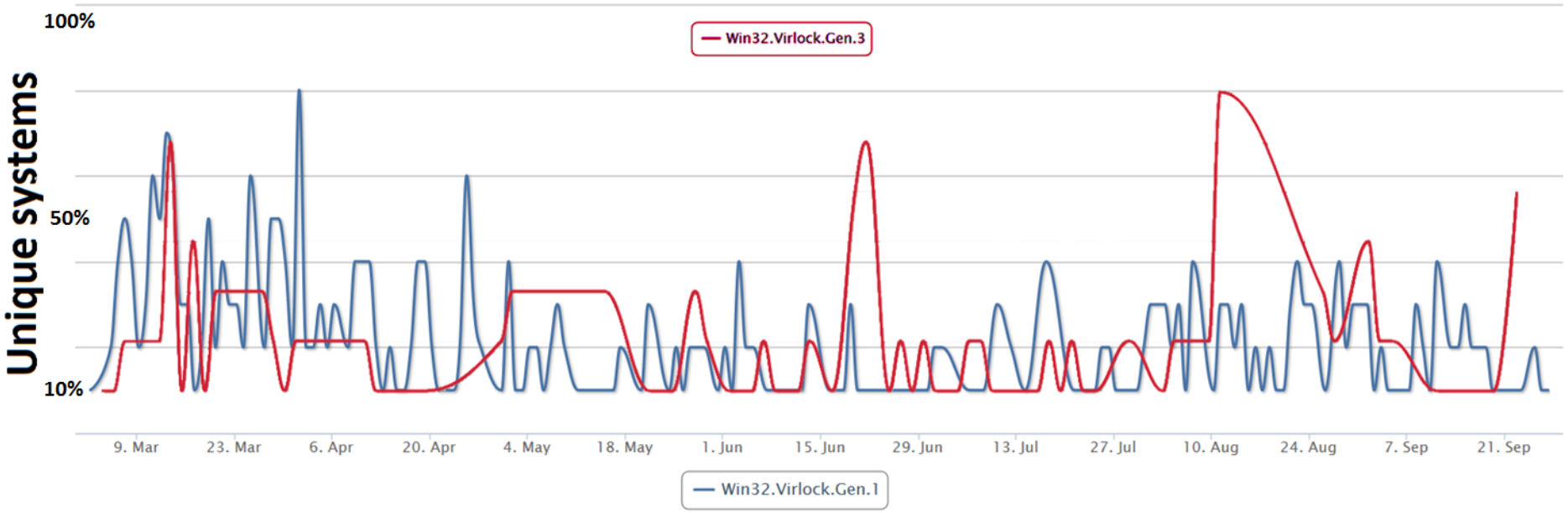
Tricking users

- Why does my pictures have an exe extension?



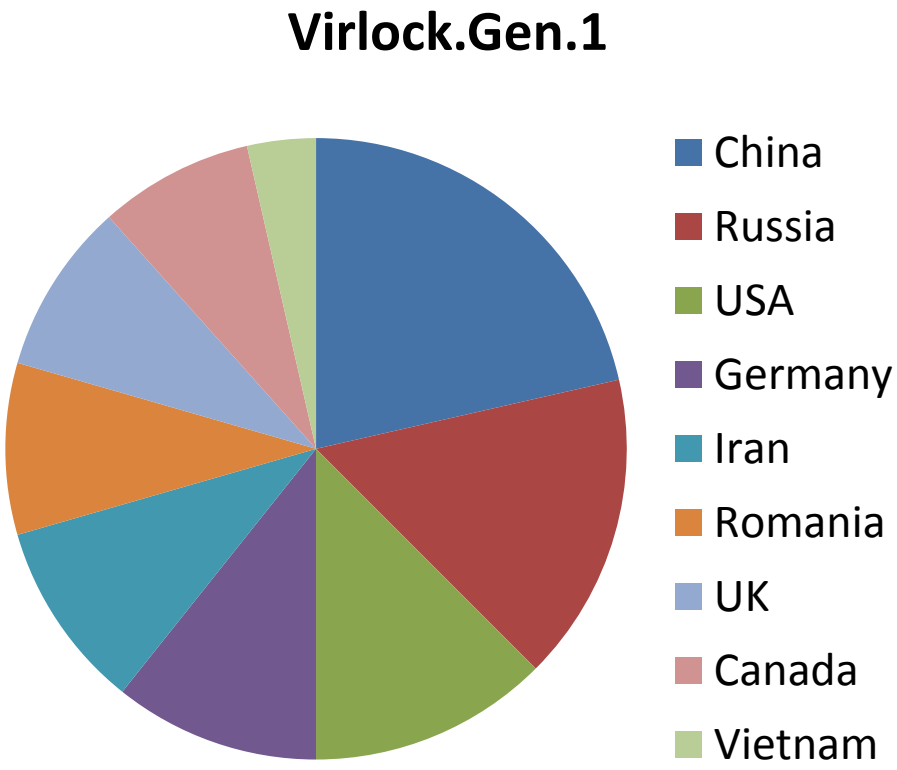
Statistics

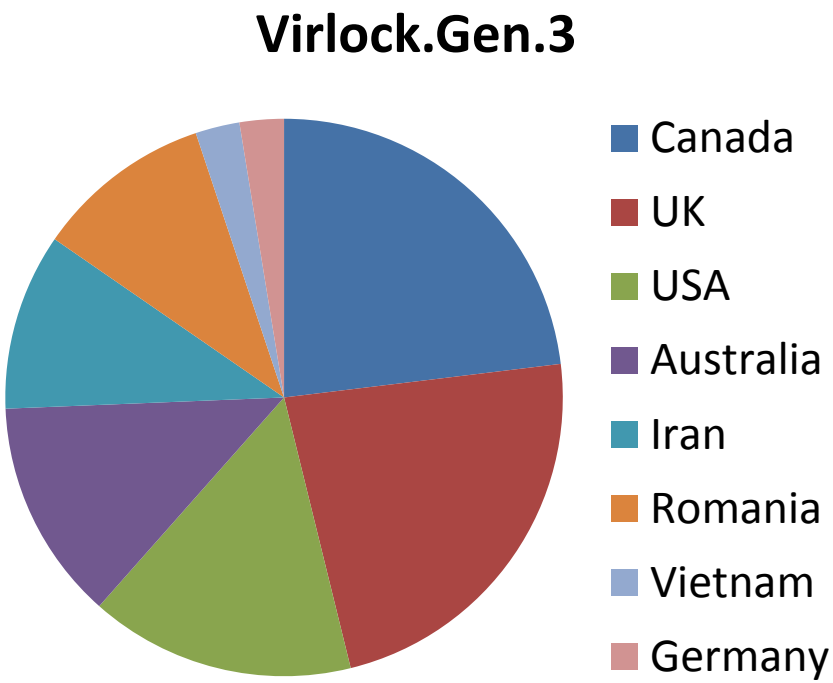
- Spreading of Win32.Virlock.Gen.1/3 until September 2015



Statistics

- Infected systems by Win32.Virlock.Gen.1/3





Statistics

- Areas with an increased number of affected files

Country	Gen.1	Gen.2	Gen.3	Gen.4	Gen.5
Canada	17.9%	0.07%	42.6%	0.07%	-
Vietnam	5.6%	-	0.27%	-	0.03%
Iran	6.2%	0.02%	1.9%	0.45%	-
France	2.11%	-	-	0.36%	-
Netherlands	2.04%	-	-	-	-
United Kingdom	1.96%	-	2.22%	-	-

Bitdefender

Conclusions

- We face new generations of file infectors
- Most of them include compiler technologies , multi stage unpacking and anti-analysis tricks to block analysis be it static or dynamic
- Virlock is among the first malwares to combine ransomware and file infection technologies
- All these changes provides us with a clear picture of even more hybrid malware technologies, working together to persist longer

?