

**It's a file infector...**  
**It's ransomware...**  
**It's VIRLOCK**

Vlad Craciun  
Mihail Andronic  
Andrei Nacu



```
01010111010010100001001001010111001101000110110111
0110101010001100110110110100101011001001101000110101
101001010110010011010001101110110010101100001010000
110010001100100100100001101001100100110011001000111
011000110100100100000110010011100000110100011101100010
10100110100100110010001000100100100100100100100100100
111001011010010010010010010010010010010010010010010010
1110110010010010010010010010010010010010010010010010010
021001100100100100100100100100100100100100100100100100
1001101010010010010010010010010010010010010010010010010
011010010010010010010010010010010010010010010010010010
011010010010010010010010010010010010010010010010010010
001000110010010010010010010010010010010010010010010010
0010010010010010010010010010010010010010010010010010010
110101010101000010001001001001001001001001001001001010
11000010010101001001001001001001001001001001001001010
1100110001010011001000000100000010101000110110001110011
0110010001101000011010010010010010010010010010010010011
0110010001101000011010010010010010010010010010010010011
00110101000011010010010010010010010010010010010010010011
110010101000011010010010010010010010010010010010010010011
0101001000000100010010010010010010010010010010010010010011
000110100010010010010010010010010010010010010010010010011
110010101000011010010010010010010010010010010010010010011
0101001000010010010010010010010010010010010010010010010011
01010000000100010010010010010010010010010010010010010010011
0001010101110010110010010010010010010010010010010010010011
0000101101011100000110010010010010010010010010010010010011
11010001000010010010010010010010010010010010010010010010011
```

**Bitdefender**

# Overview

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

# 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



Poliția  
Română



Atenție!

IP: 91.199.101.3  
Locație: RO, Romania

**Atenție! PC-ul Dvs este blocat din cauza cel puțin a unuia dintre motivele specificate mai jos.**

Dvs ați încălcat «Legea privind drepturile de autor și drepturile conexe» (Video, Muzică, Software) prin utilizarea sau distribuția neautorizată a conținutului protejat de dreptul de autor, încălcând astfel Articolul 128 din Codul Penal al României.

Articolul 128 din Codul Penal prevede o amendă între 200 și 500 de salarii minime sau privarea de libertate de la 2 până la 8 ani.



 paysafe card  Ukash

# Ransomwares and file infectors

- File locker – A custom one, similar to Cryptowall



# Ransomwares and file infectors

- Both file and screen locker - ACCDFISA



Anti-Child Porn Spam Protection - 2.0 version

**Warning! Access to your computer is limited. Your files has been encrypted.**

Have you already see that your files are encrypted and desktop locked?

Please don't panic and send us angry emails or scare us to send claims in police, fbi or others - this is useless.

Please **read this instruction carefully**, then you will get answers to most of your questions.

We don't answer to questions which already was answered in this instructions. Do not waste our and your time.

**Our minimal price for your files is 3000\$ USD.**

**Information to persons who believe that professionals can decrypt files:**

**\*\*\*\* Now only WE can get you the true password to decrypt all your files.**

**You can write to Dr.Web, Eset, Panda and other antivirus and security or datastore companies, but now this is useless. This "Anti-Child Porn Spam Protection - 2.0 version" you have is from 22.03.2013 - more than 12 month passed and no one helped to get password or decrypt files. Yes, we know there was the vulnerability to generate password in previous version using our software folders names which was generated using the same pseudorandom generator which was generate passwords.**

**Now to generate folders names didn't using any generators. Also password generates using both generators pseudorandom plus cryptographic safe pseudorandom**

Your ID Number and our contacts (please write down this data):

Your Id #:  Our special service email:

# Ransomwares and file infectors

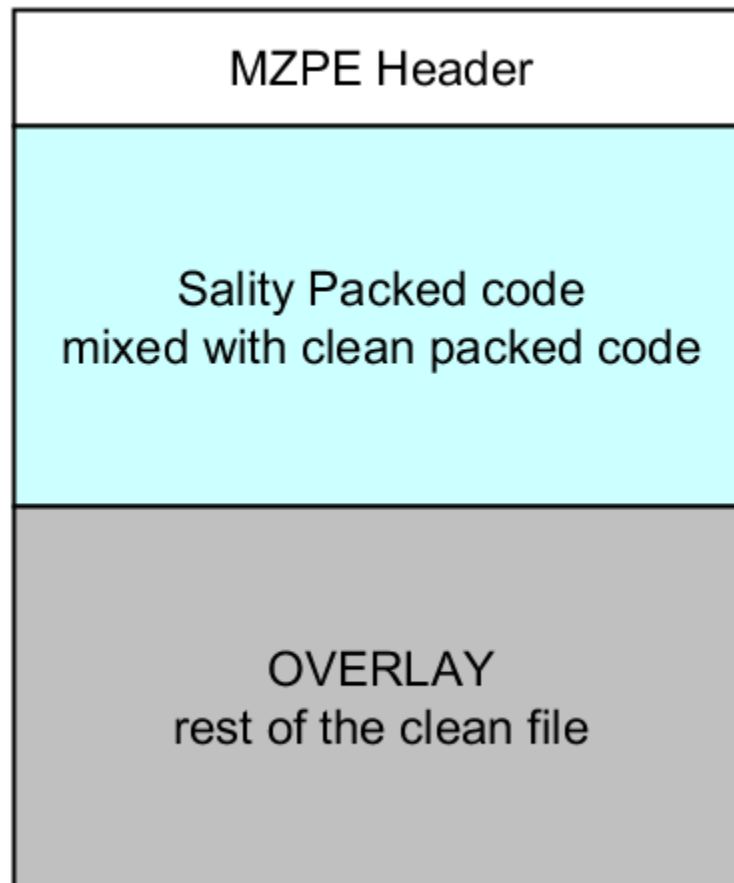
- File infectors
  - Purpose
    - Delivery and persistence of malware
  - Behavior
    - Alters the legit file by adding the malware payload





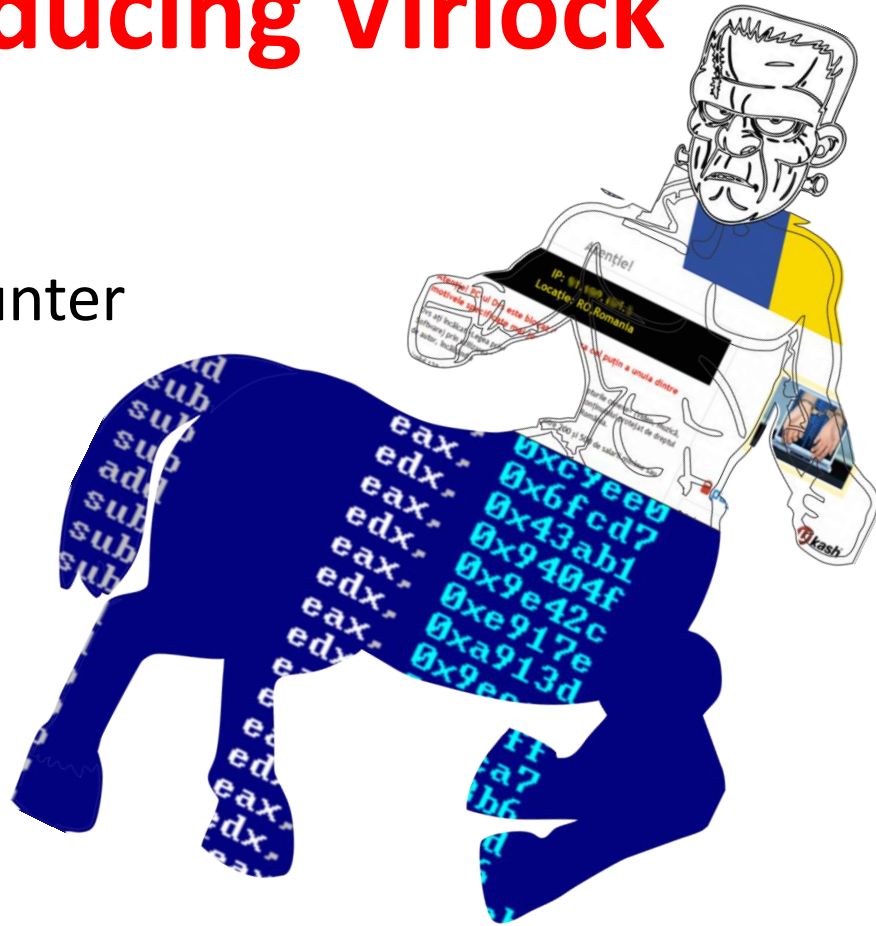
# Ransomwares and file infectors

- A 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.

This computer contains pirated software and has been blocked by ICE-Homeland Security Investigations.



**Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a \$250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)**

As a first-time offender you are required by law to pay a fine of 500 USD  
If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities. You will be charged, fined, convicted for up to 5 years.

How to pay a fine? There are two ways to pay a fine:

1. You can pay the fine online through BitCoin. BitCoin is available nationwide. Click the tabs below to find the nearest vendor. Your computer will be unlocked after the payment is made.
2. (Offline Option) You can come to your local courthouse and pay the fine at the 'Cashiers' window. A special restoration software will be sent to you by mail within a week after the payment is made.

To regain access now transfer BitCoins to the following address (click to copy):  
1NdR8tEKRBoQ1oiyAPhpuks9Uct6XftEdW

After the payment is finalized enter Transfer ID below.

Amount:            Transfer ID:

BTC 1.773       

[PAY FINE](#)

Note: All files on this computer have been encrypted with a strong symmetric algorithm and a 4096-bit key. Files will be inaccessible until the fine is paid. Attempt to remove this message will result in irreversible damage to your files, hardware and Windows installation. [View encrypted files](#)

[Payment](#)    [BitCoin Information](#)    [BitCoin Exchanges](#)    [BitCoin ATMs](#)    [Internet Browser](#)    [Notepad](#)

Project Global 3 is a coordinated effort by U.S., Canadian, European, Australian, New Zealand and other law enforcement agencies across the globe targeting computers with pirated content and their operators.

# Introducing Virlock

## File infection techniques

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

# 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

```
popa
cmp     dword [0x4018c8], 0x4
jz     (2) loc_4029BE
call   (3) sub_45519D      initialization for case 0-3
loc_4029BE:
cmp     dword [0x4018c8], 0x3
jnz    (4) loc_4029E5
call   (5) sub_459679
call   (6) sub_455587
call   (7) sub_40B518
call   (8) sub_402F25
call   (9) sub_40BEDE
jmp    (A) loc_402A67
loc_4029E5:
cmp     dword [0x4018c8], 0x4
jnz    (B) loc_402A0E
call   (C) sub_459679
call   (D) sub_455587
call   (E) sub_40B88F
call   (F) sub_40B518
call   (G) sub_402F25
call   (H) sub_40BEDE
jmp    (I) loc_402A67
loc_402A0E:
cmp     dword [0x4018c8], 0x0
jnz    (J) loc_402A28
call   (K) sub_459365
call   (L) sub_407986
call   (M) sub_455F94
jmp    (N) loc_402A67
loc_402A28:
cmp     dword [0x4018c8], 0x3
jnz    (O) loc_402A3D
call   (P) sub_459365
call   (Q) sub_455F94
jmp    (R) loc_402A67
loc_402A3D:
cmp     dword [0x4018c8], 0x4
jnz    (S) loc_402A67
mov     dword [0x409075], 0x4092b1
mov     eax, 0x45518b
mov     [0x409071], eax
lea     eax, [0x409071]
push   eax
call   (T) [kernel32.dll:StartServiceCtrlDispatcherW]
loc_402A67:
push   0x0
call   (U) [kernel32.dll:ExitProcess]
mov     dword [0x402738], 0xdfd7d9
rdtsc
```

2 - user password brute force

1 - original sample installs the malware

0 - installed process infects / supervise

3 - creates threads process keep-alive

4 - service

# Malware installation

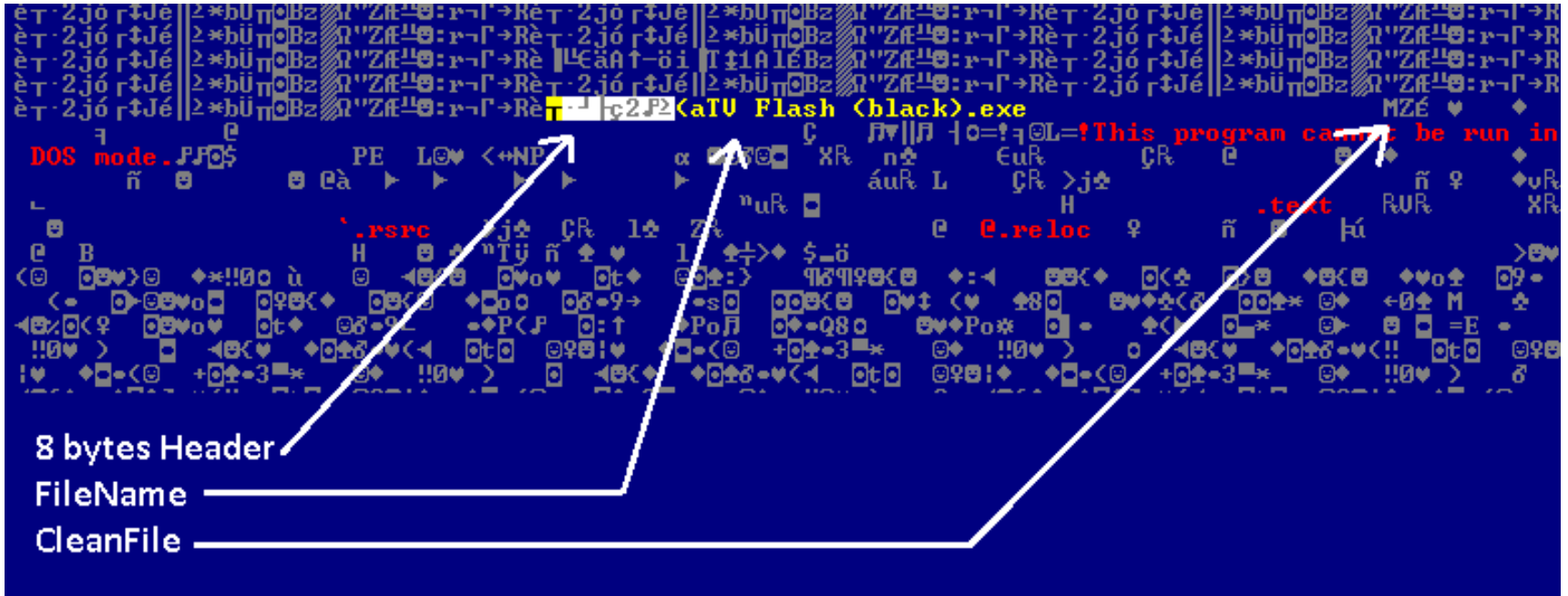
- Executing a fresh infected file

```
push    dword [0x40170c]
pop     dword [0x4016f4]
call    <1> sub_401404
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(DecryptionCode)
add     edi, 0x8             Sizeof(HeaderStructure)
mov     ebx, [0x401714]
mov     [0x4016ec], eax
mov     [0x4016f0], edi
mov     [0x4016f4], ebx
call    <4> sub_401404      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



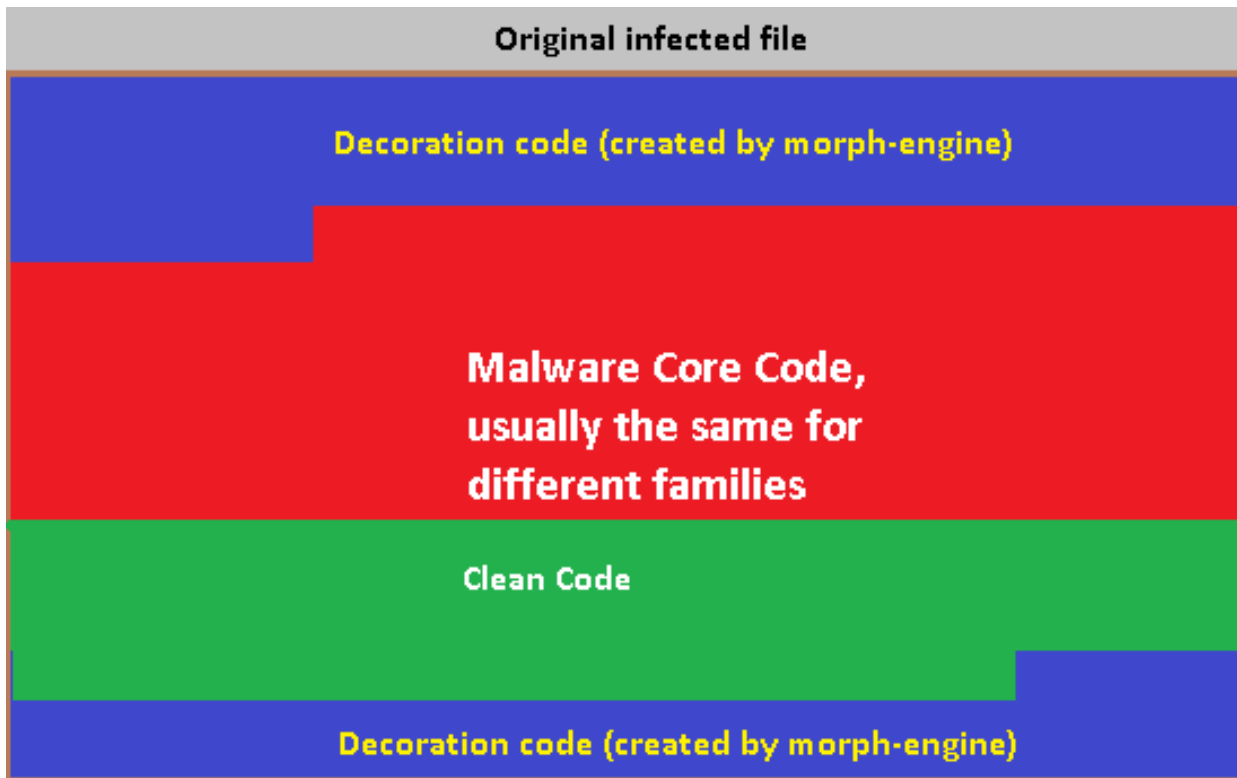
# Account password brute-force

- 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



# Anti-analysis tricks

- Detecting the debugger presence

```

004959F8 BA 905531F8 mov     edx, 0xf8315590
004959FD 3106        xor     [esi], eax
004959FF 83C6 04     add     esi, 0x4
00495A02 EB B4        jmp     (4) loc_4959B8
00495A04 81F2 A84C90F7 xor     edx, 0xf7904ca8
00495A0A BB CDAD76FD mov     ebx, 0xfd76adcd
00495A0F 81F3 2A786AFD xor     ebx, 0xfd6a782a
00495A15 81F3 BFCB2DF9
00495A1B 64 A1 30000000 mov     eax, fs:[0x30]
00495A21 8A40 02     mov     al, [eax+0x2]
00495A24 3C 01        cmp     al, 0x1
00495A26 75 05        jnz    (5) loc_495A2D
00495A28 E8 2CBEF6FF call   (6) sub_401859
00495A2D
00495A2D C705 EB584900 mov     dword [0x4958eb], 0xc10bcc
00495A37 0F31        rdtsc
  
```

```

00401885 0F31        rdtsc
00401885 0F31        rdtsc
00401887 33C2        xor     eax, eax
00401889 33D2        xor     edx, edx
0040188B BB 00040000 mov     ebx, 0x400
00401890 F7F3        div     ebx
00401892 42         inc     edx
00401893 81C2 00020000 add     edx, 0x200
00401899 33C9        xor     ecx, ecx
0040189B
0040189B 0FC8        bswap  eax
0040189D 93         xchg  ebx, eax
0040189E 0FCB        bswap  ebx
004018A0 87DE        xchg  esi, ebx
004018A2 0FCE        bswap  esi
004018A4 87F7        xchg  edi, esi
004018A6 0FCF        bswap  edi
004018A8 41         inc     ecx
004018A9 3BCA        cmp     ecx, edx
004018AB 75 EE        jnz    (1) loc_40189B
004018AD 833D F3044900 cmp     dword [0x4904f3], 0x1
004018B4 75 CF        jnz    (2) loc_401885
004018B6 52         push  edx
004018B7 FF15 FF644900 call   (3) [Sleep]
004018BD EB C6        jmp     (4) loc_401885
  
```

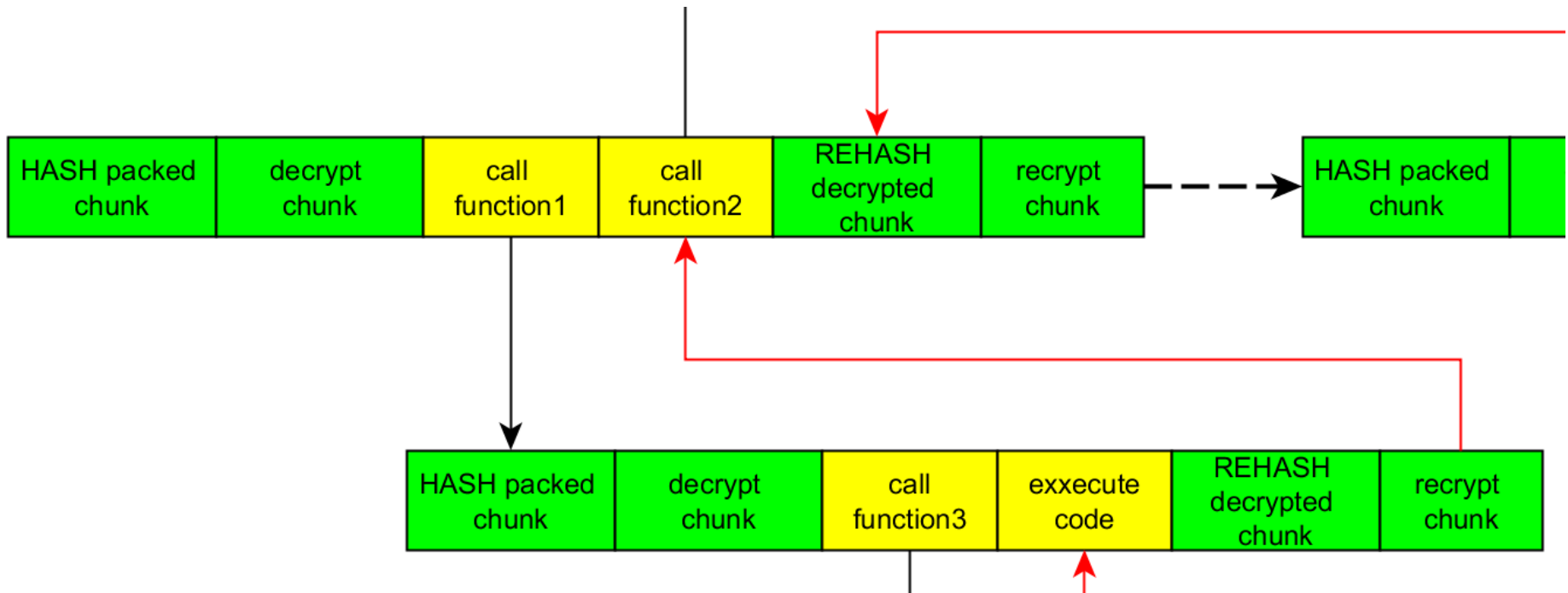
# Anti-analysis tricks

- Anti emulation tricks!

Hex	Asm	Comment
E8 25FC0700	call	(1) j_user32.dll:GetShellWindow
3D D9FEFFFF	cmp	eax, 0xfffffed9
0F85 88000000	jnz	(2) loc_401098
E8 09FC0700	call	(3) j_oleaut32.dll:VarI8FromR4
E8 0AFC0700	call	(4) j_ntdll.dll:RtlGetLastNtStatus
E8 FFFB0700	call	(5) j_oleaut32.dll:VarI8FromR4
E8 FAFB0700	call	(6) j_oleaut32.dll:VarI8FromR4
E8 FBFB0700	call	(7) j_ntdll.dll:RtlGetLastNtStatus
E8 F6FB0700	call	(8) j_ntdll.dll:RtlGetLastNtStatus
E8 EBFB0700	call	(9) j_oleaut32.dll:VarI8FromR4
E8 ECFB0700	call	(A) j_ntdll.dll:RtlGetLastNtStatus
E8 E1FB0700	call	(B) j_oleaut32.dll:VarI8FromR4
E8 DCFB0700	call	(C) j_oleaut32.dll:VarI8FromR4
E8 D7FB0700	call	(D) j_oleaut32.dll:VarI8FromR4
E8 D2FB0700	call	(E) j_oleaut32.dll:VarI8FromR4
E8 CDFB0700	call	(F) j_oleaut32.dll:VarI8FromR4
E8 C8FB0700	call	(G) j_oleaut32.dll:VarI8FromR4
E8 C9FB0700	call	(H) j_ntdll.dll:RtlGetLastNtStatus
E8 C4FB0700	call	(I) j_ntdll.dll:RtlGetLastNtStatus
E8 B9FB0700	call	(J) j_oleaut32.dll:VarI8FromR4
E8 B4FB0700	call	(K) j_oleaut32.dll:VarI8FromR4
E8 AFFB0700	call	(L) j_oleaut32.dll:VarI8FromR4
E8 B0FB0700	call	(M) j_ntdll.dll:RtlGetLastNtStatus
E8 ABFB0700	call	(N) j_ntdll.dll:RtlGetLastNtStatus
E8 A0FB0700	call	(O) j_oleaut32.dll:VarI8FromR4
E8 9BFB0700	call	(P) j_oleaut32.dll:VarI8FromR4
E8 9CFB0700	call	(Q) j_ntdll.dll:RtlGetLastNtStatus
E8 91FB0700	call	(R) j_oleaut32.dll:VarI8FromR4
E8 8CFB0700	call	(S) j_oleaut32.dll:VarI8FromR4
E8 87FB0700	call	(T) j_oleaut32.dll:VarI8FromR4
C3	ret	

# Anti-analysis tricks

- Decrypt → Execute → Re-Encrypt



# Anti-analysis tricks

- Decrypt → Execute → Re-Encrypt

00401914	81D 26194000	ii=&10	cmp	dword [0x401926], 0xd2bbec				
0040191E	0F84 5A010000	W&Z0	jz	(1) loc_401A7E				
00401924	EB 04	δ◆	jmp	(2) loc_40192A				
00401926	F4	↑	hlt					
00401927	98	ÿ	cwde					
00401928	8100 81F26247	ü ü2bG	add	dword [eax], 0x4762f281				
0040192E			<b>loc_40192A:</b>					
0040192E	47	G	inc	edi				
0040192F	F9	.	stc					
00401930	BA 3DEEB8FC	=€~n	mov	edx, 0xfcb8ee3d				
00401935	BA 2B5C29F7	+\)\\$	mov	edx, 0xf7295c2b				
0040193A	BA 53ECAEF9	\$œ<	mov	edx, 0xf9aeeec53				
0040193F	E8 63000000	çc	call	(3) sub_4019A7	Get Buffer HASH in EAX			
00401944	BB 8A82BCFC	èéµu	mov	ebx, 0xfcb828a				
00401949	81F3 E2E465F9	çΓEe-	xor	ebx, 0xf965e4e2				
0040194F	81F3 FA2C66FE	ç·,f	xor	ebx, 0xfe662cfa				
00401955	BA 23C31AFA	→	mov	edx, 0xfa1ac323				
0040195A	3D B58C12A7	ç±	cmp	eax, 0xa7128cb5				
0040195F	0F85 F4FEFFFF	W&f	jnz	(4) loc_401859				
00401965	E9 87000000	0ç	jmp	(5) loc_4019F1				
0040196A	3006	0œ	xor	[esi], al				
0040196C	EB 5E	δ&	jmp	(6) loc_4019CC				
0040196E	EB 43	δC	jmp	(7) loc_4019B3				
00401970			<b>loc_40196A:</b>					
00401970	BA F8877BFF	ç<	mov	edx, 0xff7b87f8				
00401975	3306	3&	xor	eax, [esi]				
00401977	BB 7E2BEBFA	ç~+δ-	mov	ebx, 0xfaeb2b7e				
0040197C	E9 92000000	0è	jmp	(8) loc_401A13				
00401981			<b>sub_401981:</b>					
00401981	BA 4CD796F9	ç  ü-	mov	edx, 0xf996d74c				
00401986	B9 E2010000	ç  0	mov	ecx, 0x1c2				
0040198B	BB B8B060FF	ç  /	mov	ebx, 0xf60b0b8				
00401990	83E9 04	ç  /	sub	ecx, 0x4				
00401993	BB E38D8CF8	ç  i0	mov	ebx, 0xf88c8de3				
00401998	E9 9C000000	0è	jmp	(9) loc_401A39				
0040199D			<b>loc_40199D:</b>					
0040199D	E9 DC000000	0m	jmp	(A) loc_401A7E				
004019A2	BB 95274D75	ç  'Mu	mov	ebx, 0x754d2795				
004019A7			<b>sub_4019A7:</b>					
004019A7	B9 8D000000	ç	mov	ecx, 0x8d				
004019AC	BA F5DDEFFA	ç  n-	mov	edx, 0xfaefddf				
004019B1	EB 21	0?	jmp	(B) loc_4019D4				
004019B3			<b>loc_4019B3:</b>					
004019B3	33F9 01	ç  @	cmp	ecx, 0x1				
004019B6	75 B2	ç  B2	jnz	(C) loc_40196A				
004019B8	BA 3C394BFB	ç  <9K^	mov	edx, 0xfb4b393c				
004019BD	C3	ç	ret					
004019BE	EB AA	ç	jmp	(D) loc_40196A				
004019C0			<b>loc_4019C0:</b>					
004019C0	E8 BCF9FFFF	ç	call	(E) sub_401981	DECRYPT NEXT CHUNK			
004019C5	BB 109B958E	ç  çδ&	mov	ebx, 0x8e959b10				
004019CA	EB D1	ç	jmp	(F) loc_40199D	JUMP TO DECRYPTED-CHUNK			
004019CC			<b>loc_4019CC:</b>					

00401A7E	83EC 1C	ç	sub	esp, 0xc				
00401A81	C70424 000000	ç	mov	dword [esp+0x4], 0x0				
00401A88	C74424 04 0000	ç	mov	dword [esp+0x8], 0x0				
00401A90	C74424 08 0000	ç	mov	dword [esp+0xc], 0x0				
00401A98	C74424 0c 0000	ç	mov	dword [esp+0x10], 0x0				
00401AA0	C74424 10 0000	ç	mov	dword [esp+0x14], 0x0				
00401AA8	C74424 14 0000	ç	mov	dword [esp+0x18], 0x0				
00401AB0	C74424 18 0000	ç	mov	dword [esp+0x1c], 0x0				
00401AB8	64 A1 30000000	ç	mov	eax, fs:[0x30]				
00401ABE	8B40 0C	ç	mov	eax, [eax+0xc]				
00401AC1	8B40 0C	ç	mov	eax, [eax+0xc]				
00401AC4	8B00	ç	mov	eax, [eax]				
00401AC6	8B00	ç	mov	eax, [eax]				
00401AC8	8B40 18	ç	mov	eax, [eax+0x18]				
00401ACB	8B48 3C	ç	mov	ecx, [eax+0x3c]				

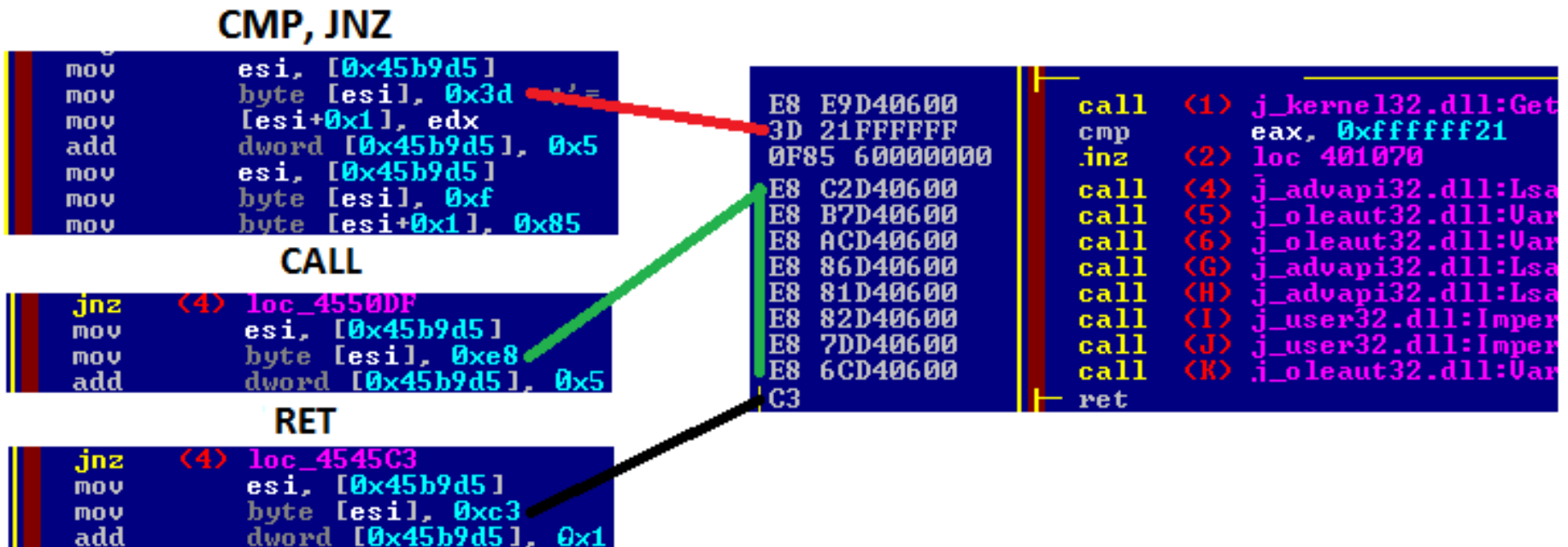
  

00401C24	8B4C24 14	ç	mov	ecx, [esp+0x14]				
00401C28	890D F0184000	ç	xor	[0x4018f0], ecx				
00401C2E	83C4 1C	ç	add	esp, 0xc				
00401C31	C705 26194000	ç	mov	dword [0x401926], 0x8198f4				
00401C3B	0F31	ç	rdtsc					
00401C3D	3105 FC194000	ç	xor	[0x4019fc], eax				
00401C43	3105 C6194000	ç	xor	[0x4019c6], eax				
00401C49	3105 A3194000	ç	xor	[0x401921], eax				
00401C4F	E8 53FDFFFF	ç	call	(8) sub_4019A7	REHASH			
00401C54	A3 5B194000	ç	mov	[0x40195b], eax				
00401C59	E8 23FDFFFF	ç	call	(9) sub_401981	RECRYPT			
00401C5E	90	ç	nop					
00401C60	90	ç	nop					
00401C6F	C3	ç	ret					



# Polymorphic engine

- Basic reshape technique



# Different malware versions

- [Hash encrypted code, compare hash] - template

```

Disasm
cmp     dword [0x401442], 0x1509fc
jz     (1) loc_40158F
jmp     (2) loc_401446
int     3
cmpsb
jecxz  (3) loc_401446
loc_401446:
xor     ebx, 0xf9f15aee
mov     edx, 0xfae24090
mov     edx, 0x9d9248
call    (4) sub_4014CD
xor     edx, 0xfc0f1a1a
mov     edx, 0xfd855def
mov     edx, 0xfd88c264
mov     edx, 0xfee329e7
cmp     eax, 0x70da3037
jnz    (5) loc_40197C
jmp     (6) loc_401514
sub     ecx, 0x4
    
```

```

Disasm
cmp     dword [0x401442], 0xd0bc8a
jz     (1) loc_401587
jmp     (2) loc_401446
dec     edi
retf
test
loc_401446:
dword [eax], 0x8b3c15bb
idiv   dword [edx-0x3199b91]
xor     edx, 0xfeb1b76f
xor     edx, 0xfd5cb6d7
call    (3) sub_401500
mov     edx, 0xfacac4b8
xor     edx, 0xfdd064a9
xor     ebx, 0xfd65cce9
xor     ebx, 0xfa514b2a
xor     edx, 0xfc3f8a47
cmp     eax, 0x4b296727 ;'g>K
jnz    (4) loc_40197B
jmp     (5) loc_4014C1
mov     ebx, 0xf8b8d3bf
    
```

```

Disasm
Entry Point
cmp     dword [0x401412], 0xef0d7d
jz     (1) loc_40154D
jmp     (2) loc_401416
test   eax, 0x8100d83f
loc_401416:
db     0xf2
pop     ds
pop     edi
jp     (3) loc_401416
mov     edx, 0xfd634b09
xor     ebx, 0xfb490a68
xor     ebx, 0xfdd11e29
xor     ebx, 0xfbfd9ca4
call    (4) sub_401492
mov     edx, 0xf17790
xor     ebx, 0xf89df869
mov     edx, 0xf938bae6
cmp     eax, 0x14c14bc
jnz    (5) loc_401843
jmp     (6) loc_401455
loc_401455:
    
```

```

Disasm
cmp     dword [0x401262], 0xec1132
jz     (1) loc_4013A6
jmp     (2) loc_401266
xchg   ebp, eax
cnc
popf
add     [ecx+0x4dd55af2], al
loc_401266:
db     0xfe
mov     edx, 0xffd42f10
xor     ebx, 0xfb40704e
call    (3) sub_40135A
xor     edx, 0xfcea7238
mov     edx, 0xfb87426e
xor     edx, 0xfe6e5846
xor     edx, 0xf746d7e8
xor     edx, 0xfab5c993
cmp     eax, 0x2aa2d2a1
jnz    (4) loc_401681
jmp     (5) loc_401369
loc_4012A9:
mov     esi, 0x4013a6
    
```

```

Disasm
cmp     dword [0x401262], 0x4ffd3c
jz     (1) loc_4013B1
jmp     (2) loc_401266
aam     0xca
iret
add     [edx-0x39a27e0], bh
mov     ebx, 0xfe0236b0
mov     edx, 0xff510487
call    (3) sub_40136C
xor     edx, 0xfb9bd78e
mov     ebx, 0xfb879616
xor     edx, 0xfe036542
mov     edx, 0xfbf5f934
mov     ebx, 0x393578 ;'x59'
cmp     eax, 0xcea62818
jnz    (4) loc_401698
jmp     (5) loc_401355
ret
    
```

# Different malware versions

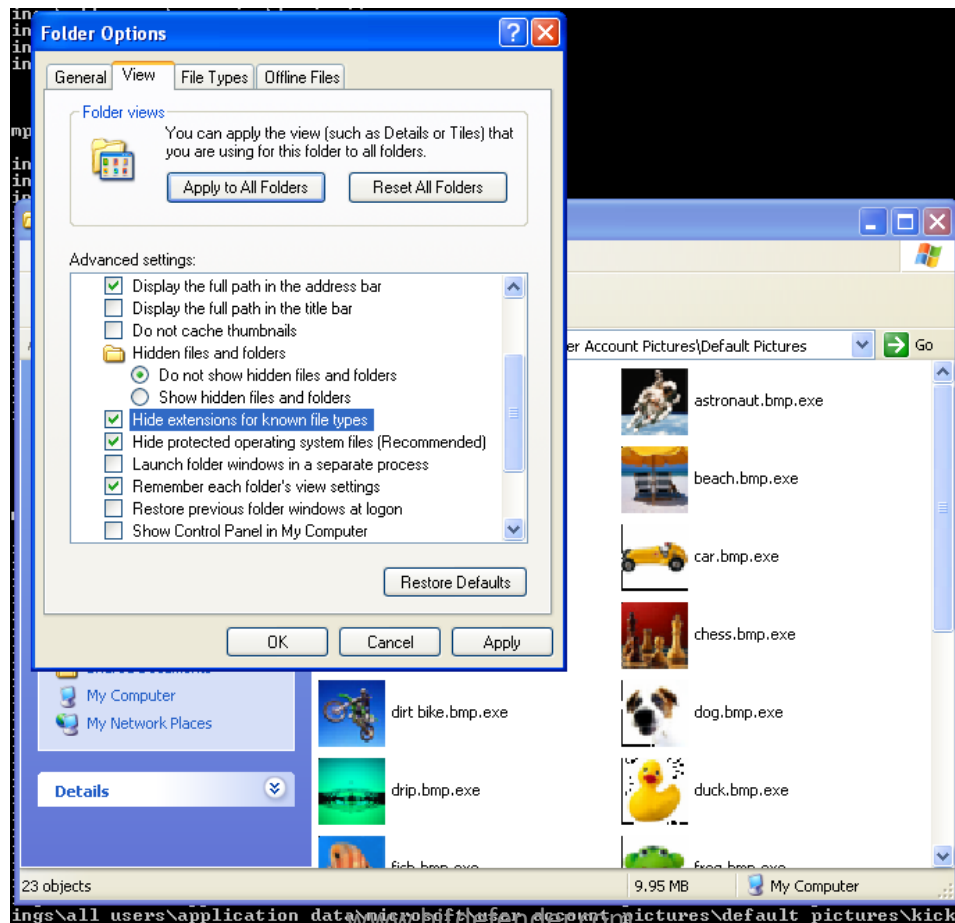
- Similar code within 2 different families

```
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]
```

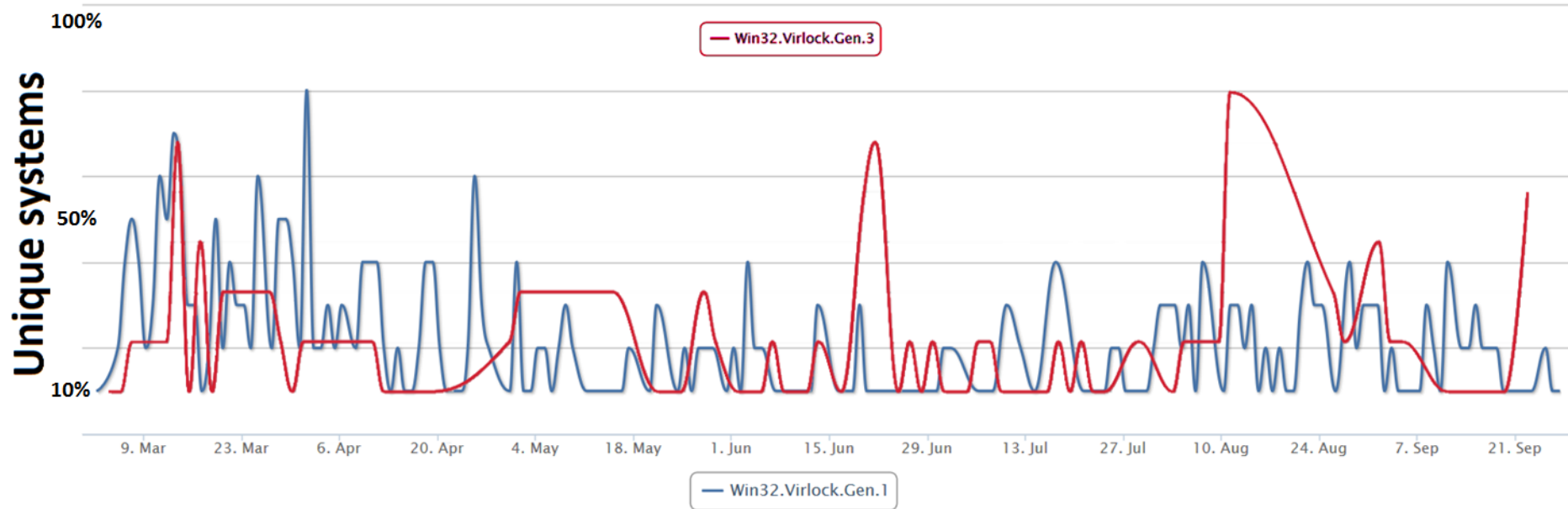
# Tricking users

- Why does my pictures have an exe extension?



# Statistics

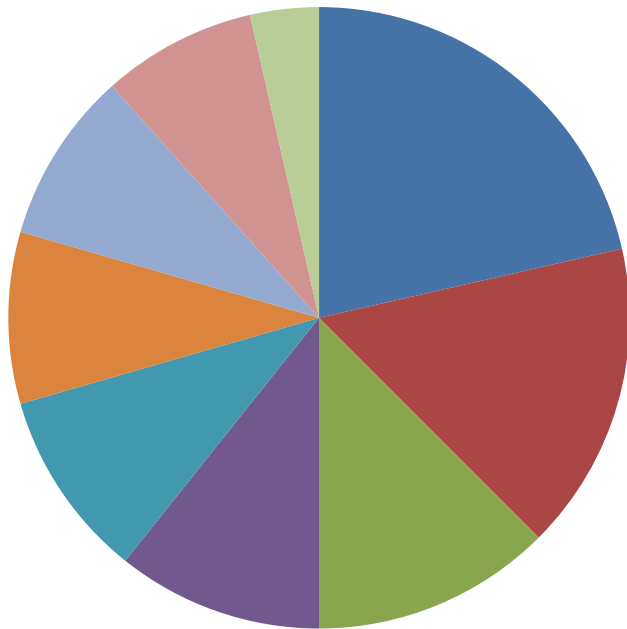
- Spreading of Win32.Virlock.Gen.1/3 until September 2015



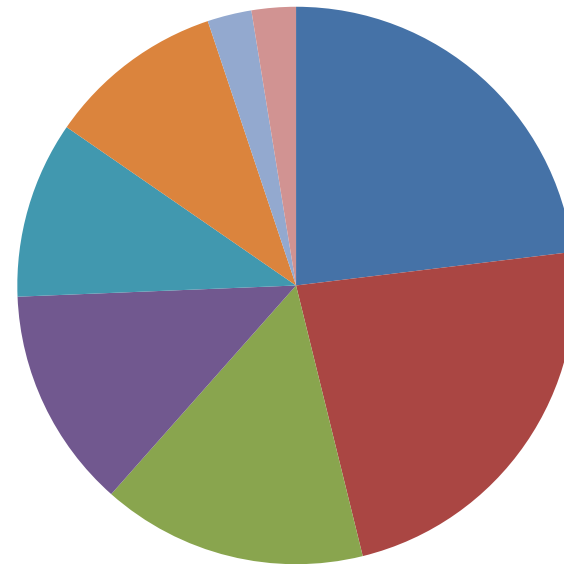
# Statistics

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

## Virlock.Gen.1



## Virlock.Gen.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%	-	-

# 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



