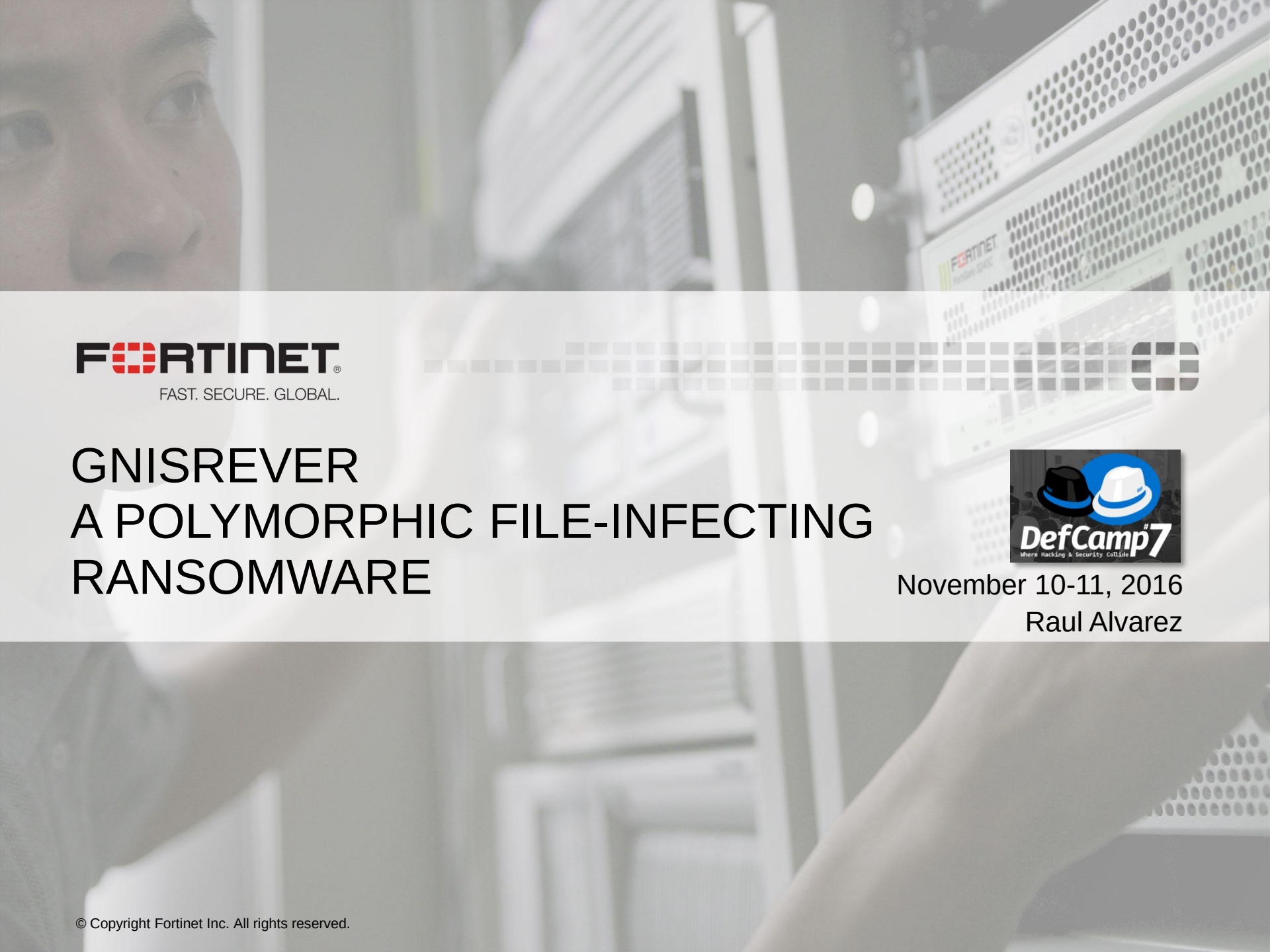


FAST. SECURE. GLOBAL.

GNISREVER
A POLYMORPHIC FILE-INFECTING RANSOMWARE

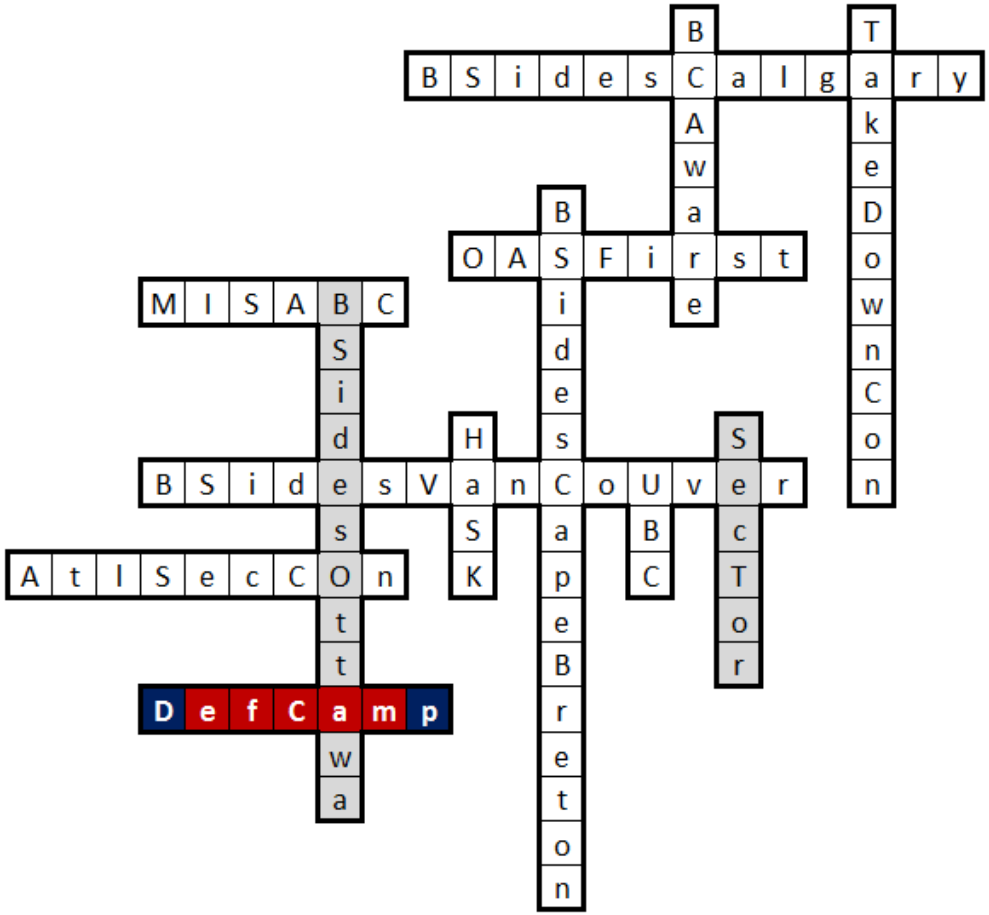
DefCamp#7
Where Hacking & Security Collide

November 10-11, 2016

Raul Alvarez

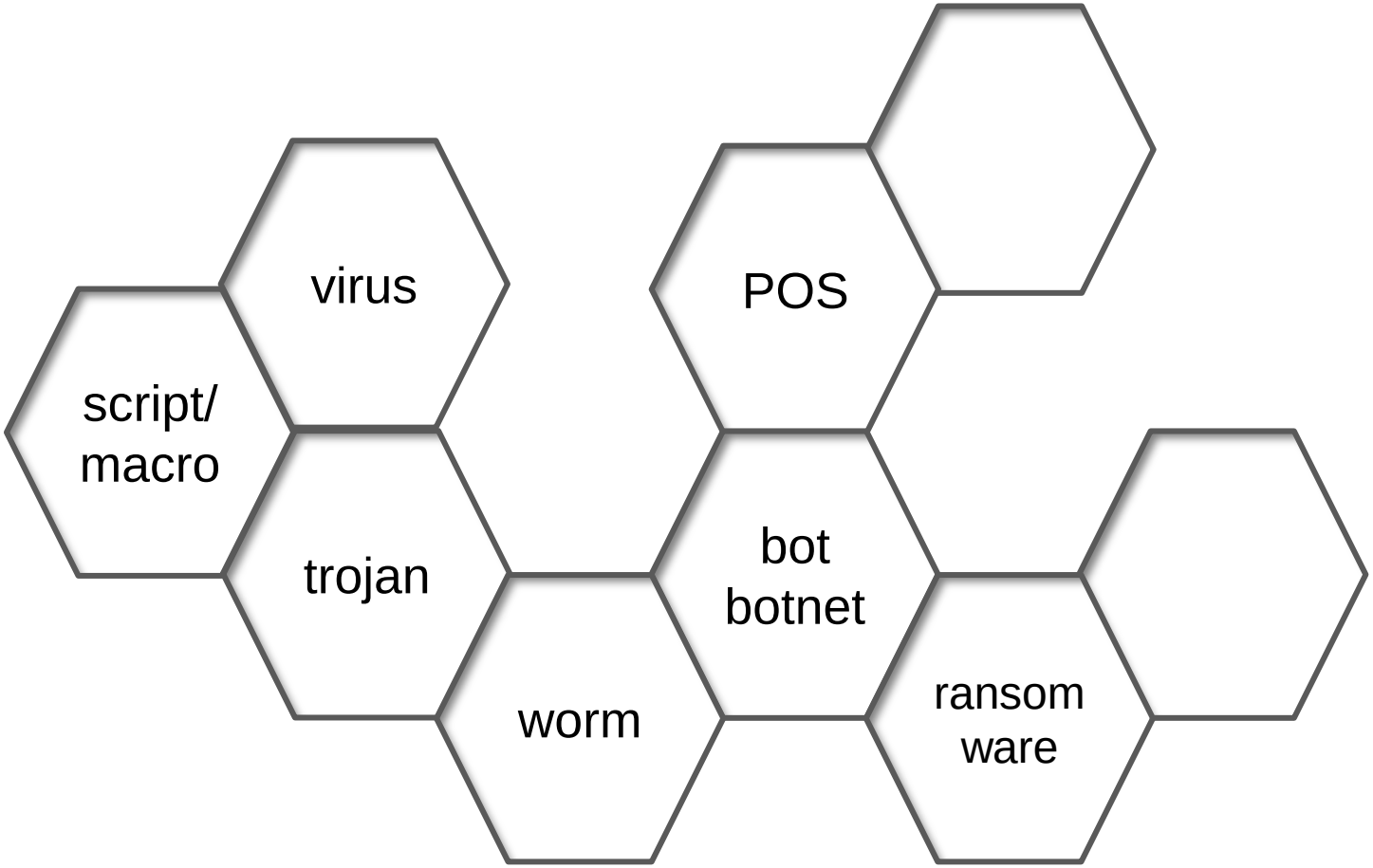
About Me

- Senior Security Researcher @ Fortinet
- 22 published articles in Virus Bulletin
- Regular contributor in our company blog

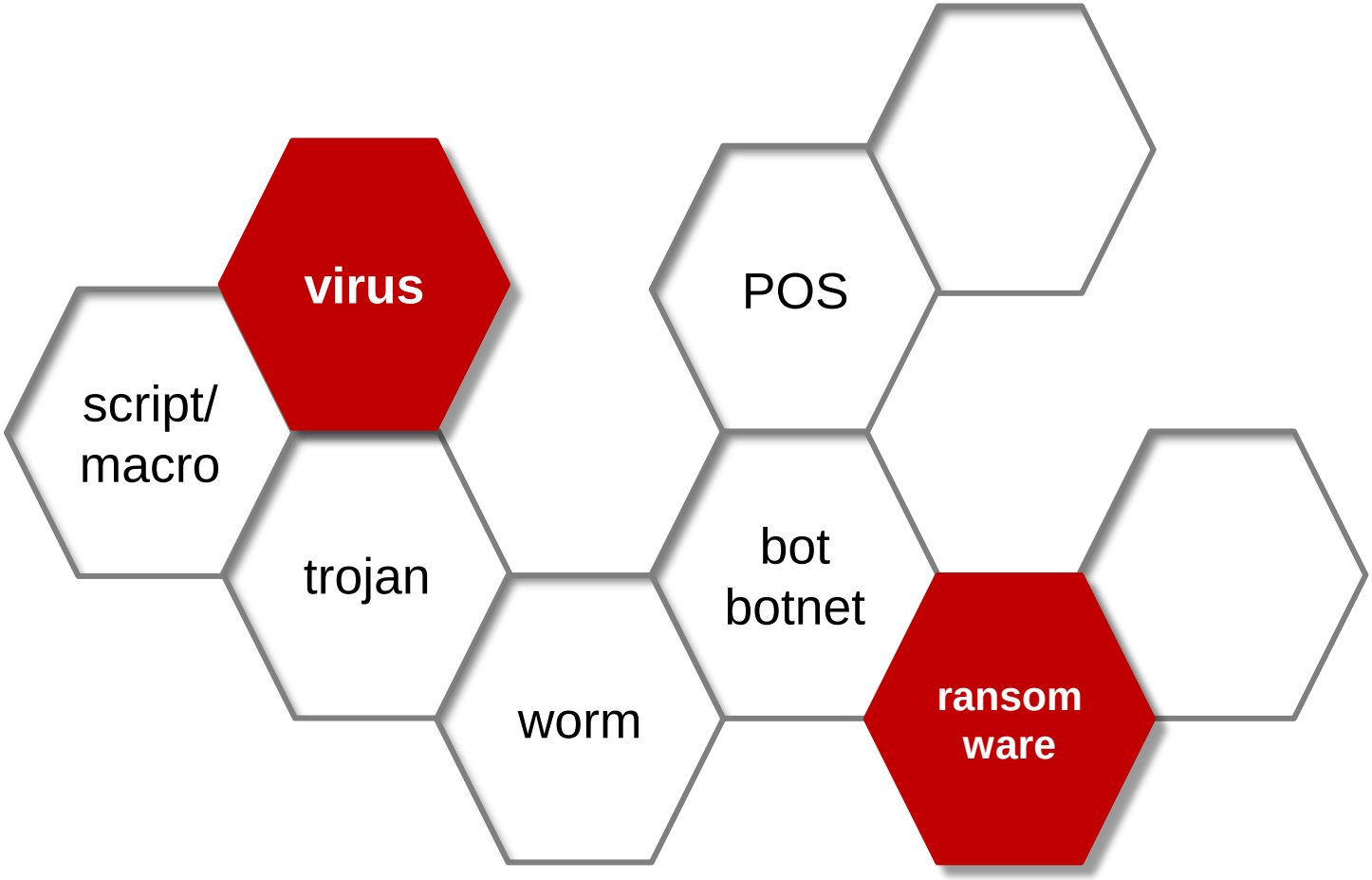


Malware Categories

Malware Honeycomb



Virlock



Agenda

FORTINET

Agenda

Virlock as a common malware
- Reversing stages
- Metamorphic algorithm

Virlock as a file infector
- Detection
- Extracting the host file

Virlock as a polymorphic malware
- On-demand polymorphic algorithm

Virlock as a ransomware
- Visible signs
- Unlocking

Virlock

FORTINET

What Is A File Infector?

- Attaches the malware code into the host file.
- Appending, prepending, and cavity type
- Maintains persistency within the computer system
- Infected file is hard to restore

What Is A Ransomware?

- Holds your computer for ransom
- Encrypts files
- Uses cryptocurrency, such as bitcoins, for payment

What Is Virlock?

- A ransomware
- A file infector
- Uses on-demand polymorphic algorithm
- Uses metamorphic algorithm
- Locks your screen

Canadian Security Intelligence Service Notice

Your computer was automatically blocked. Reason: Pirated software found on this computer.

Your computer is now blocked. 155 files have been temporarily blocked on your computer.
To regain computer access and restore files you are required to pay a fine of 250 CAD
Blocked files will be permanently removed from your computer if the fine is not paid.
The CSIS has two ways to pay a fine:
1.You can pay your fine online through BitCoin. BitCoin is available nationwide.
Click the tabs below to find the nearest vendor. Your computer will be unlocked after you make your payment.
2.You can come to your provincial courthouse and pay your fine at the Cashiers window.
Your computer will be unlocked within 4-5 working days.
To regain access transfer bitcoins to the following address (click to copy):
198tX7NmLg6o8qcTT2Uv9cSBVzN3oEozpv
After the payment is finalized enter Transfer ID below.

Online fine payments are processed by Royal Bank of Canada.

Amount: Transfer ID:

BTC 0.588 | PAY FINE

Internet connection is unavailable. Click Network Connections and connect to the Internet

If the fine is not paid, 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.

Payment | BitCoin Information | BitCoin Exchanges | BitCoin ATMs | Internet Browser | Notepad | Network Connections

CSIS.gc.ca

Canadian Security Intelligence Service Notice

Canada

What is BitCoin

Bitcoin is a software-based online payment system.

How to pay a fine?
1.Purchase bitcoins from an exchange or an ATM.
2.Transfer to the address (click to copy): 198tX7NmLq6o8qcTT2Uv9cSBVzN3oEozpv
To locate the nearest exchange or an ATM open the corresponding tab below.

If you purchased a paper wallet or you want to register a new bitcoin wallet follow the instructions below: Open Internet Browser. Go to the address: blockchain.info/wallet and click 'Start A New Wallet'.Enter your e-mail address(optional) and password. Make sure your password is secure. Save your password safely, preferably offline(click Notepad). Follow the steps prompted on the website and pay close attention to the security recommendations. Login to your Bitcoin wallet blockchain.info/wallet/login Click on Import / Export. Enter the paper wallet's private key by typing it manually (case sensitive) and click on 'Add Private Key'. Click 'Sweep Key'. Make sure your Bitcoin balance reflects the new deposit.

Making BitCoin payment: click 'Send Money' on the menu, enter the bitcoin address, click 'Send Payment'.

Learn more about BitCoin

howtobuybitcoins.info	bitcoin.org
en.bitcoin.it/wiki/Introduction	en.bitcoin.it/wiki/Getting_started
en.bitcoin.it/wiki/Buying_bitcoins	en.bitcoin.it/wiki/Main_Page

Canadian Security Intelligence Service Notice

View: Canadian Exchanges International Exchanges

CaVirtex
https://www.cavirtex.com/home
(888)812-2525

Bitcoiniacs
bitcoiniacs.com
Waves Coffee, #100 - 900 Howe St.
Vancouver
BC V6Z 2M4 Canada
1 (877) 814-7460
contact@bitcoiniacs.com

QuadrigaCX
quadrigacx.com
Phone: 1-604-757-9660
Email: contact@quadrigacx.com

QuickBT
quickbt.com/ca/
1-888-QUICK-55 (784-2555)

Aaron Buys Gold Ltd
aaronbuysgold.com
Canada Wide 1.866.549.7747
Edmonton 780.628.6895
947 Ordze Road Sherwood Park

Vault of Satoshi
vaultofsatoshi.com
(855) 457-0101
(519) 757-0101
340 Henry Street, Unit #16
Brantford, Ontario
Canada, N3S 7V9

Coin Clutch
coinclutch.com
Email: support@coinclutch.com
Toll-Free: 1-800-704-0012

Tradebitcoin.com

Canadian Security Intelligence Service Notice

BTM Locators

Edmonton (4)
Fort Mcmurray (1)
Montreal (7)
Vancouver (3)
Ottawa (2)
Quebec (3)
Sherwood Park (1)
Whistler (1)
Winnipeg (4)
Alberta (1)
Saskatoon (2)
Moncton (1)
North Bay (1)
Toronto (2)
Victoria (1)
Halifax (1)

Roboco roboco.in

BitCoin ATM bitcoinatm.com

CoinDesk coindesk.com/bitcoin-atm-map/

BitCoin ATM Map bitcoinatmmap.com

Canadian Security Intelligence Service Notice

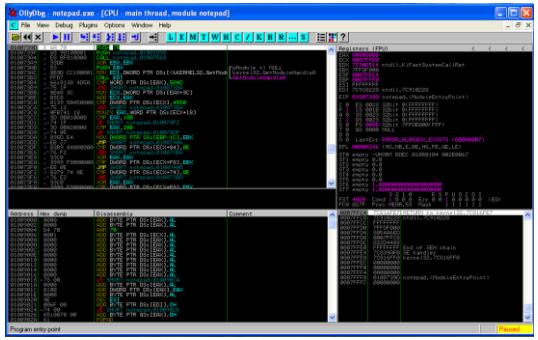
To save notepad contents click File->Save.
The file will be saved in My Documents folder as 'myfile'. You can access it later.

Payment | BitCoin Information | BitCoin Exchanges | BitCoin ATMs | Internet Browser | Notepad | Network Connections

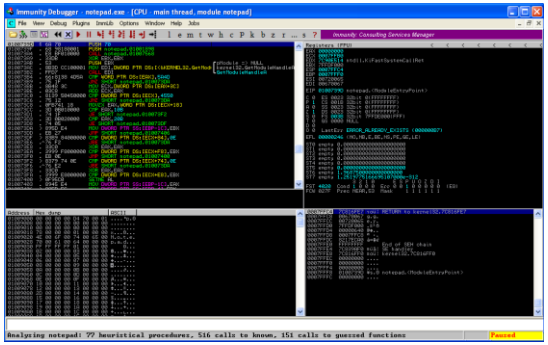
CSIS.gc.ca

Just kidding!

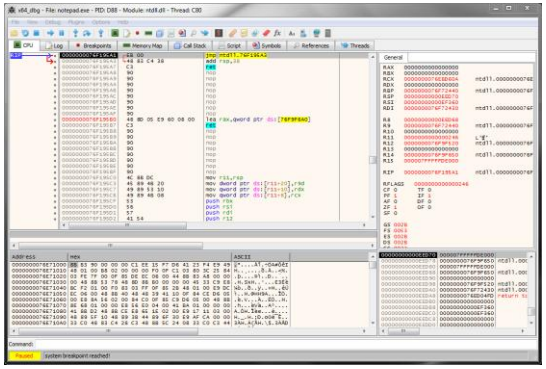
Debugging Tools



ollydbg
http://www.ollydbg.de/



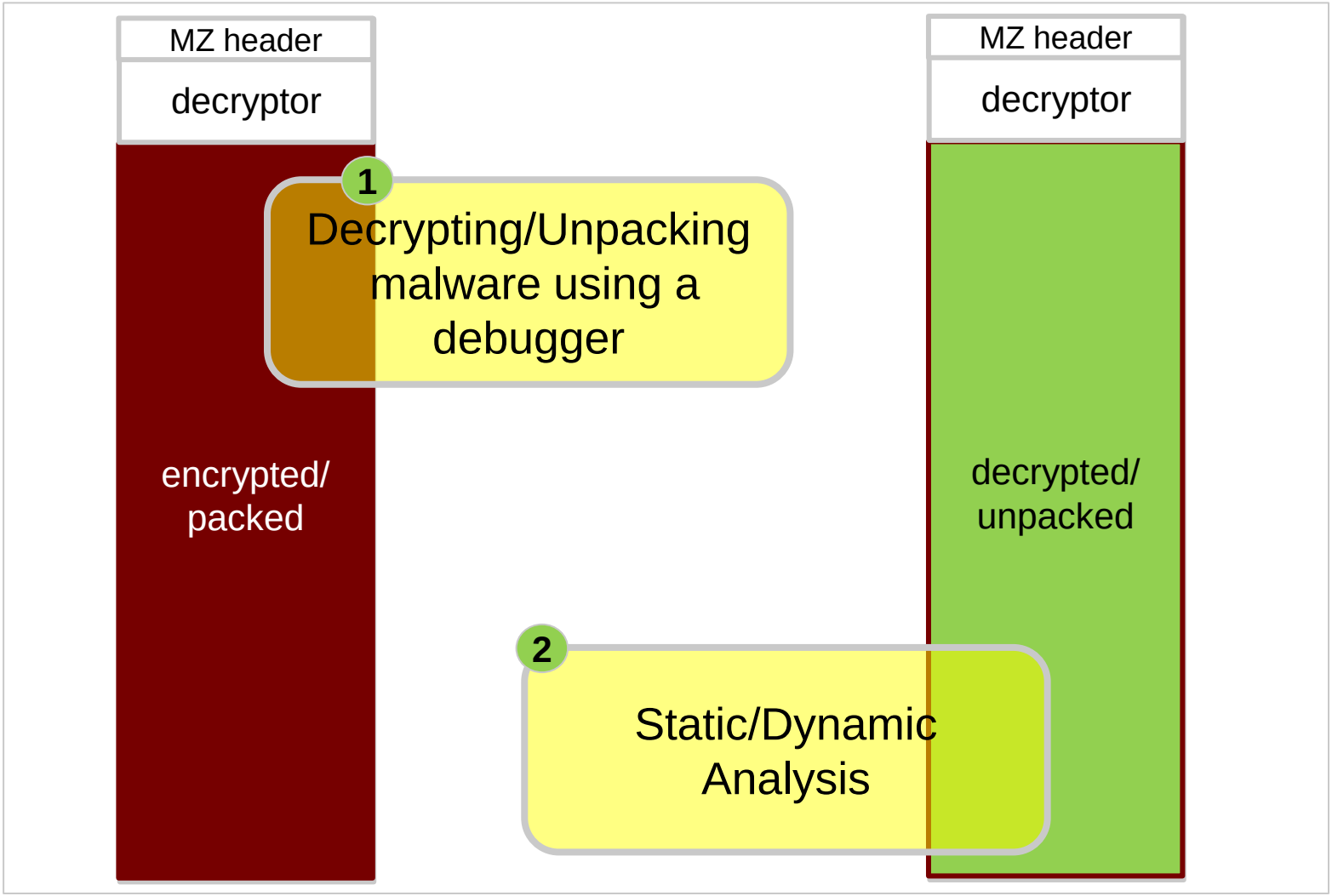
immunity debugger
http://www.immunityinc.com/products/debugger/



x64dbg
http://x64dbg.com/

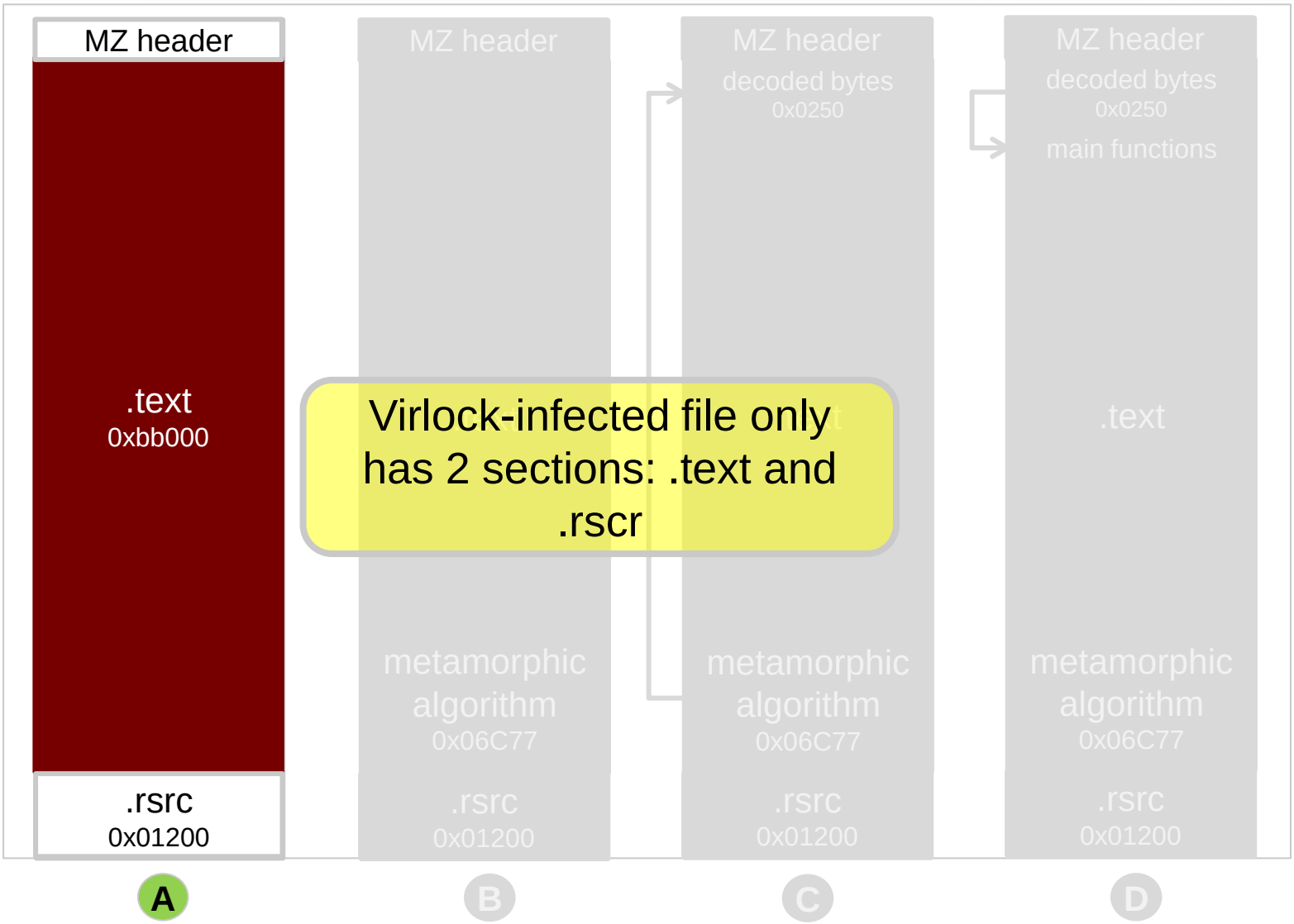
Virlock As A Common Malware

Common Reversing

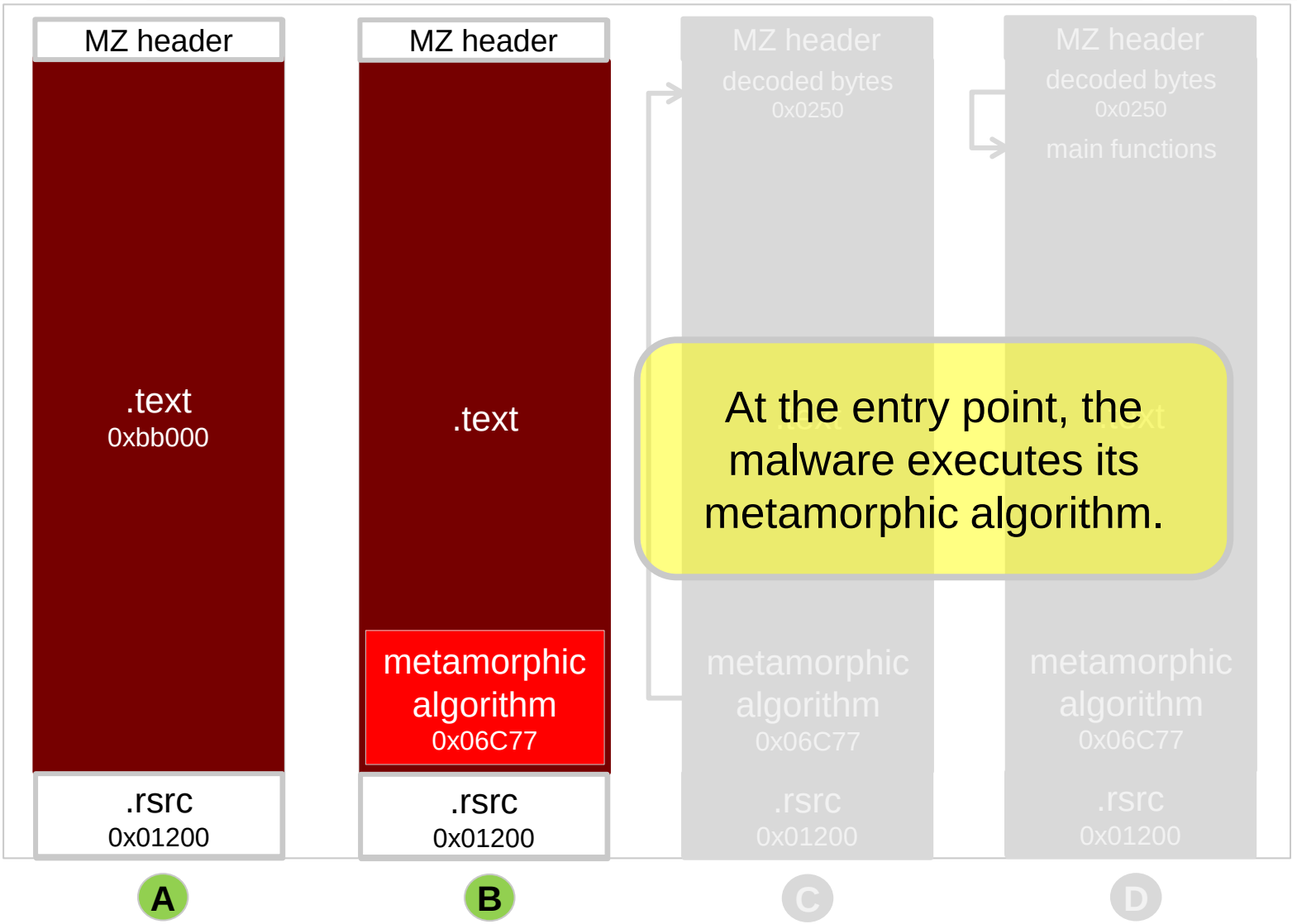


Reversing Stages

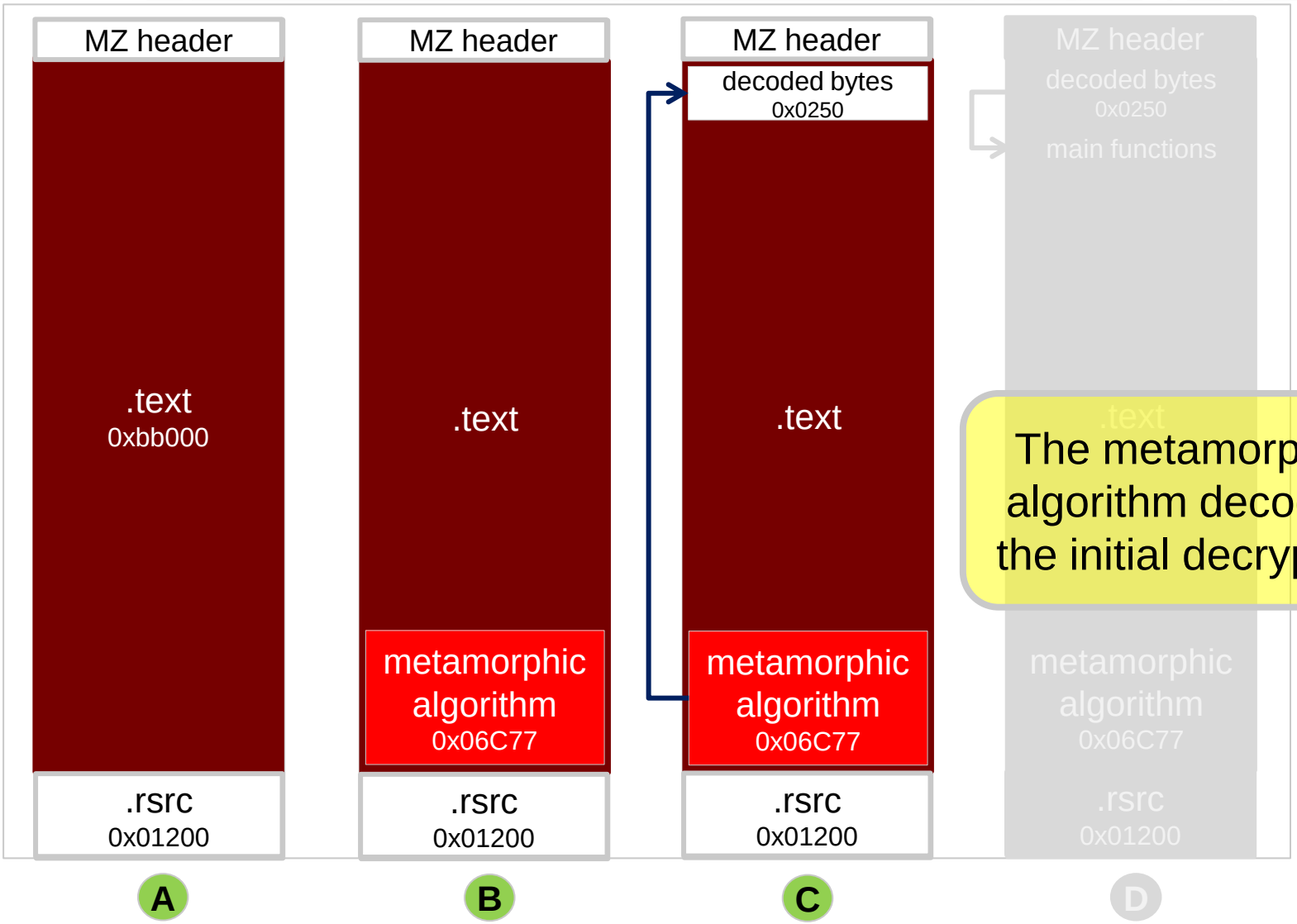
Reversing Stages



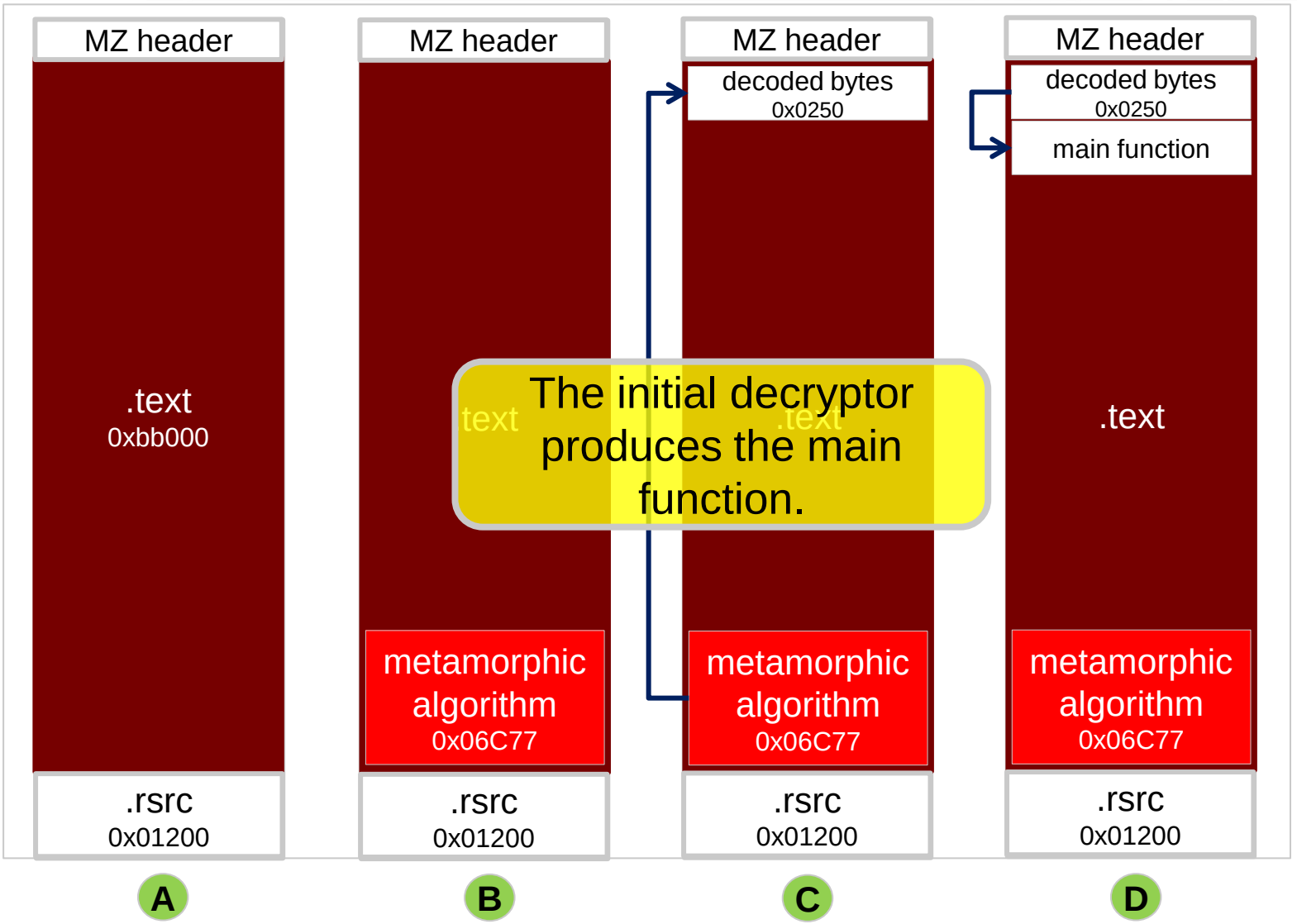
Reversing Stages



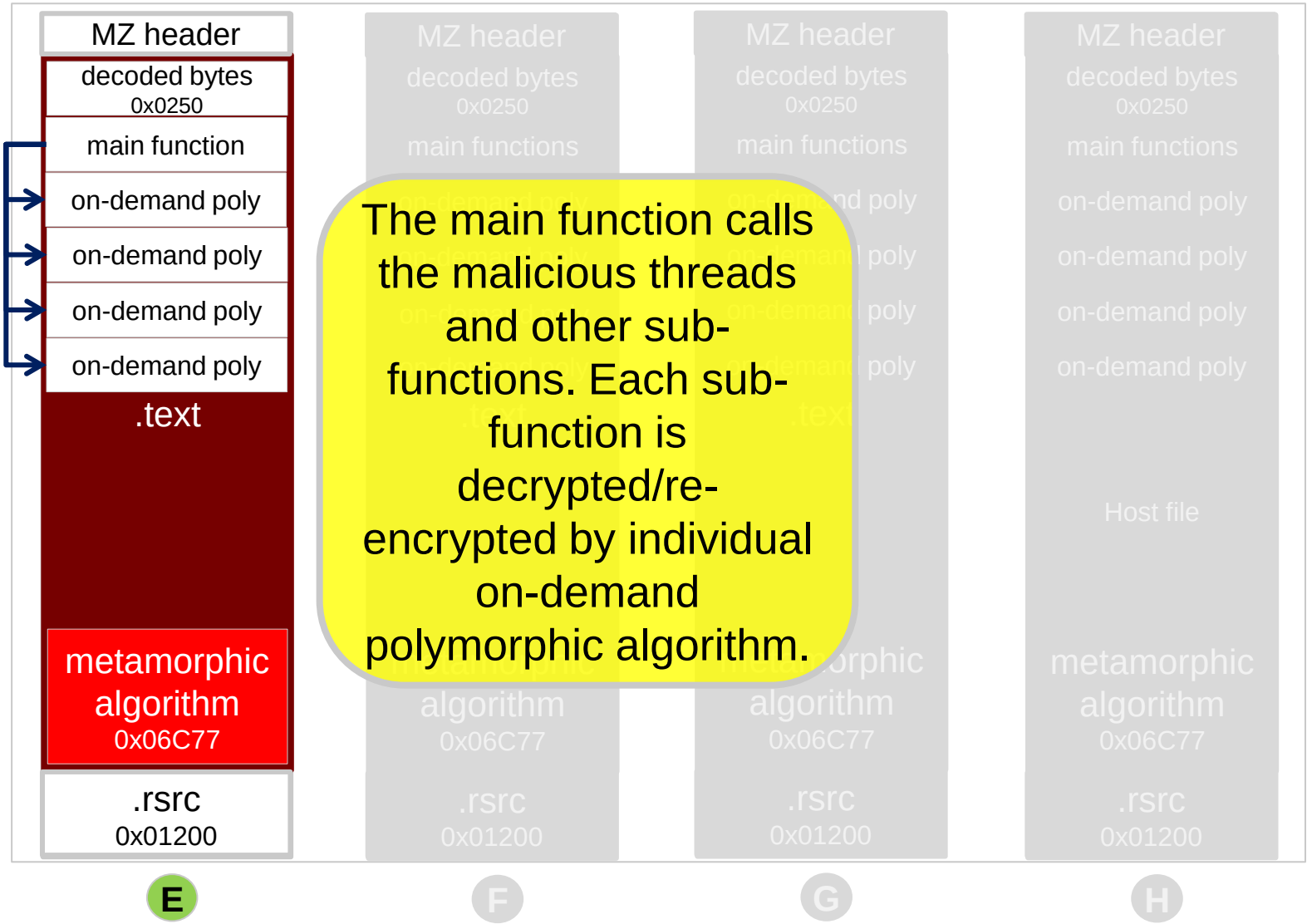
Reversing Stages



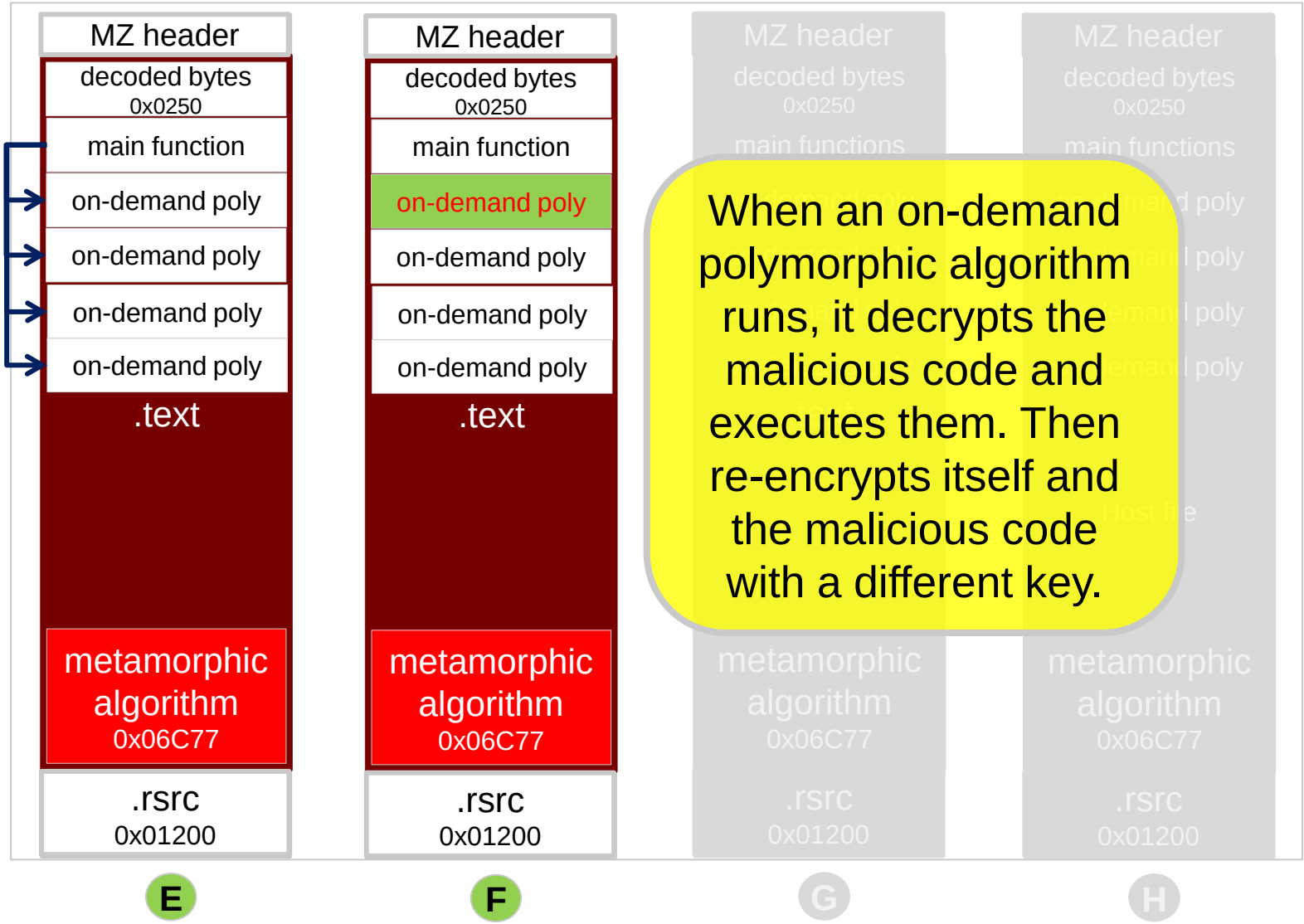
Reversing Stages



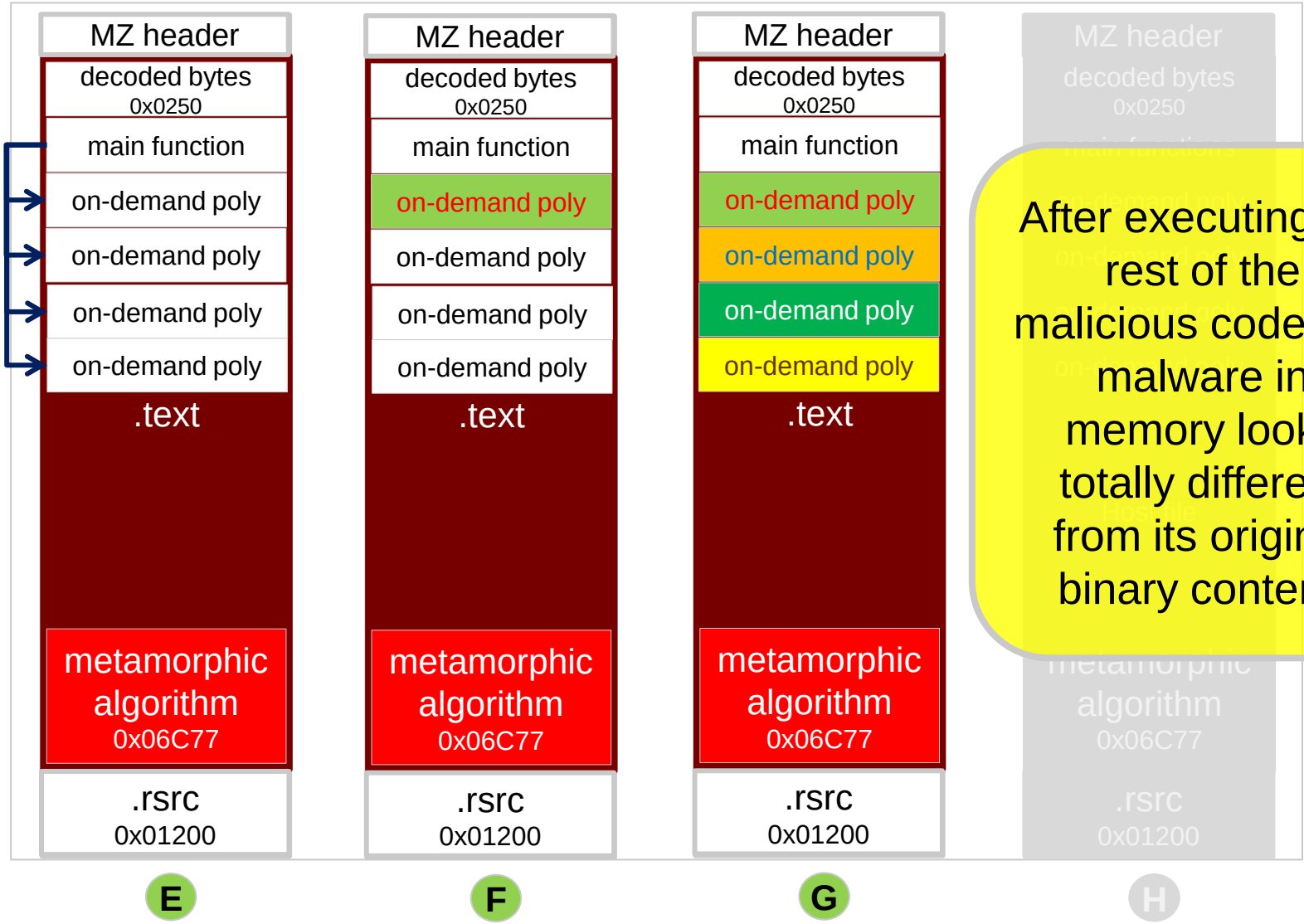
Reversing Stages



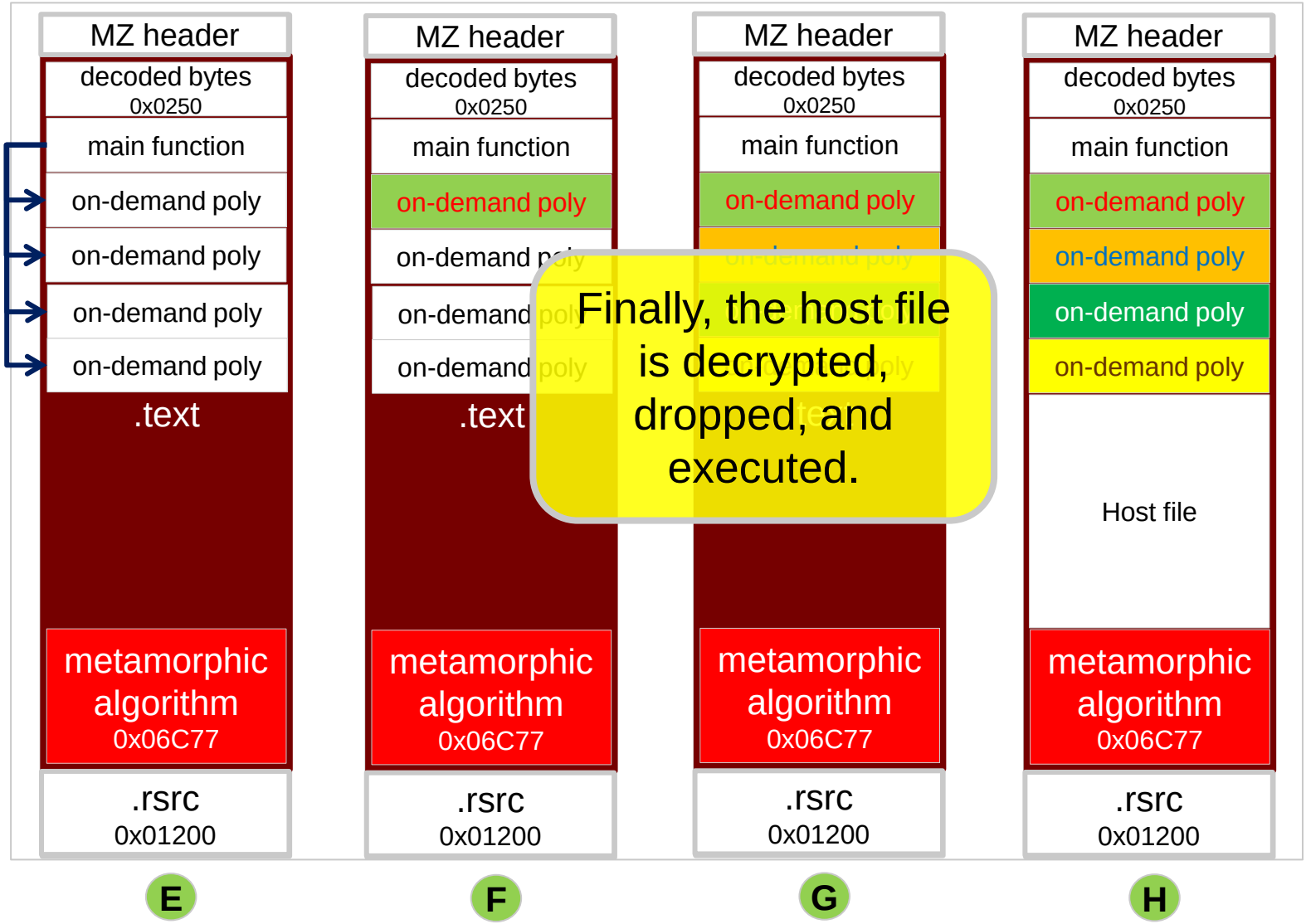
Reversing Stages



Reversing Stages



Reversing Stages



Metamorphic Algorithm

Metamorphic Algorithm

Basics:

Putting a value(0) in a register(EAX)

MOV EAX,0	EAX register gets 0 directly
XOR EAX,EAX	XORing the same register by itself also generates a zero value placed into a given register
SUB EAX,EAX	SUBtracting any register by itself also generates the same result.

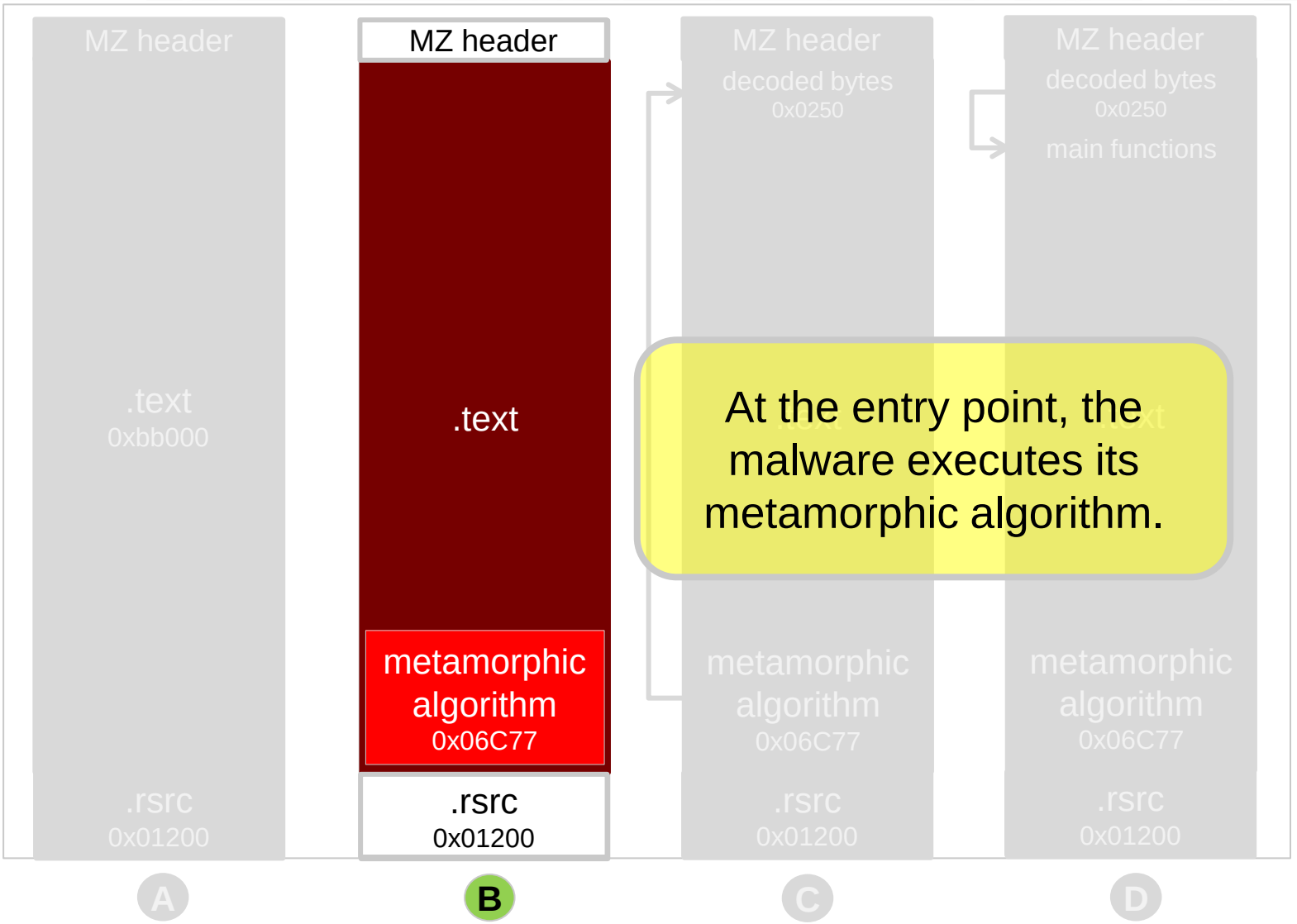
MOV EAX, 0x10
ADD EAX, 0x10
SUB EAX, 0x20
	EAX also gets 0

Metamorphic Algorithm

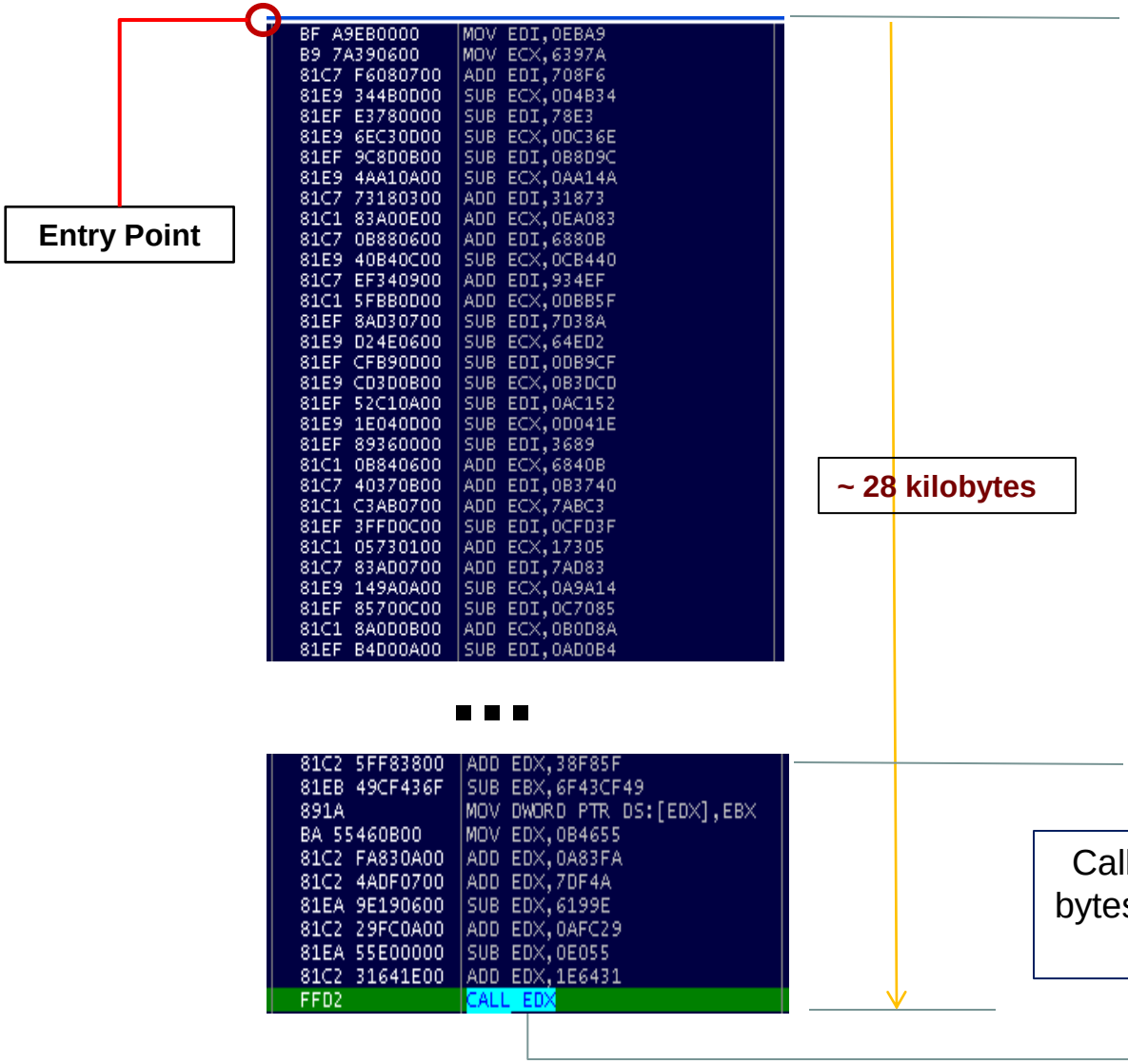
Detection Limitation

- Hard to find similar bytes
- Unknown length of bytes
- Unpredictable code

Reversing Stages



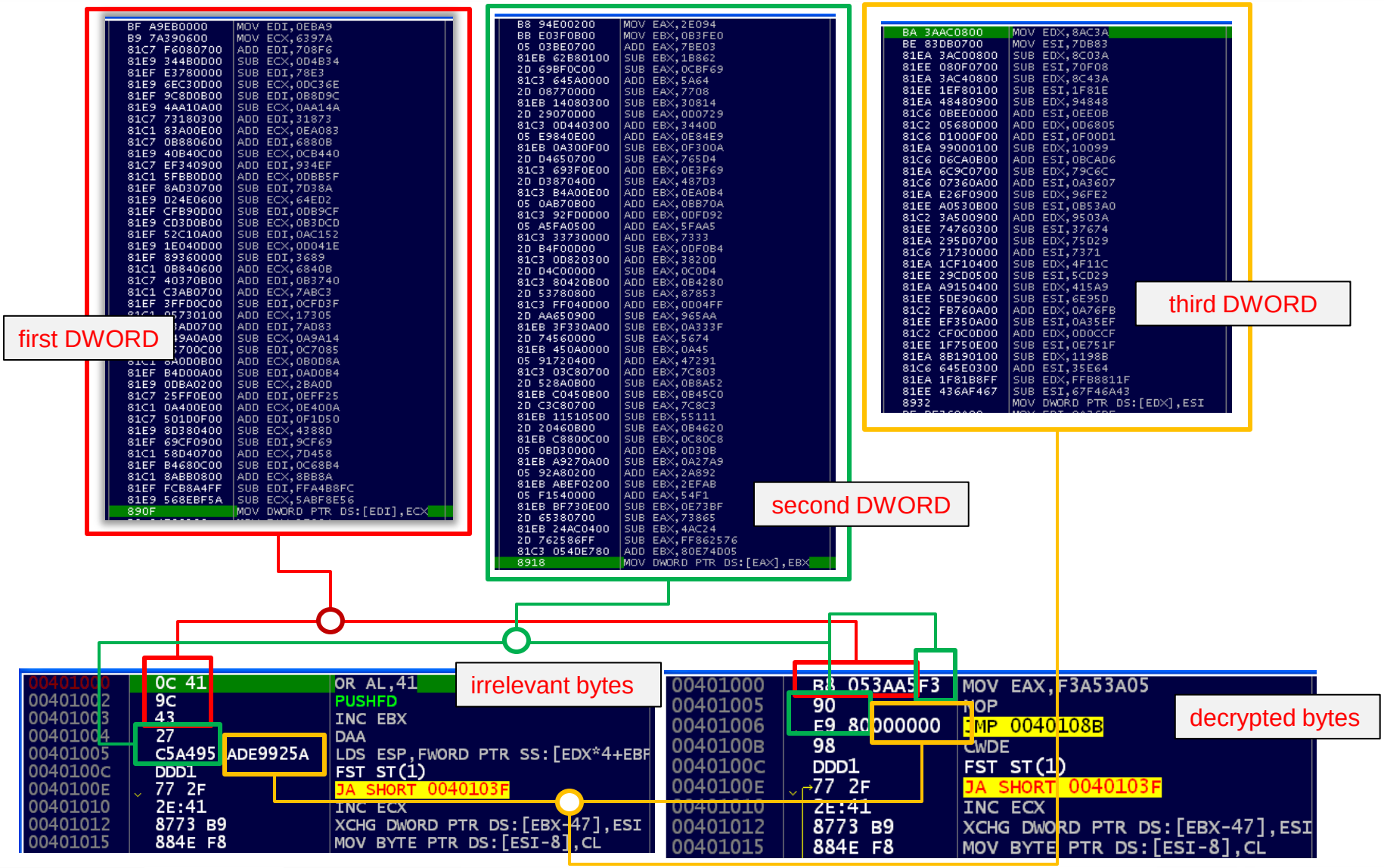
Metamorphic Algorithm (sample 1)



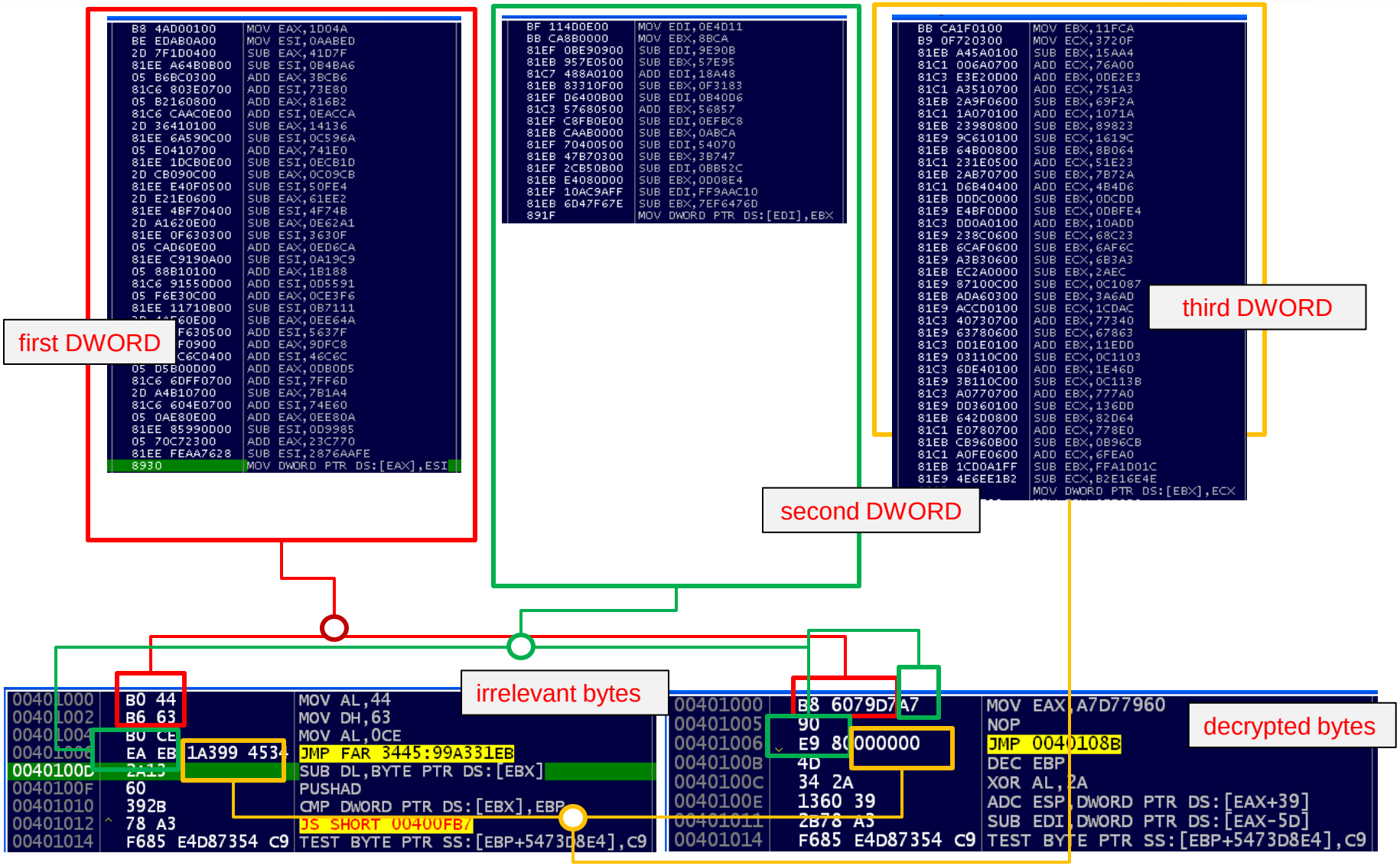
The size of the metamorphic code varies per infected file.

Approximately 28kb of code constitutes the metamorphic algorithm that generates the rest of the malicious code, including the polymorphic algorithm.

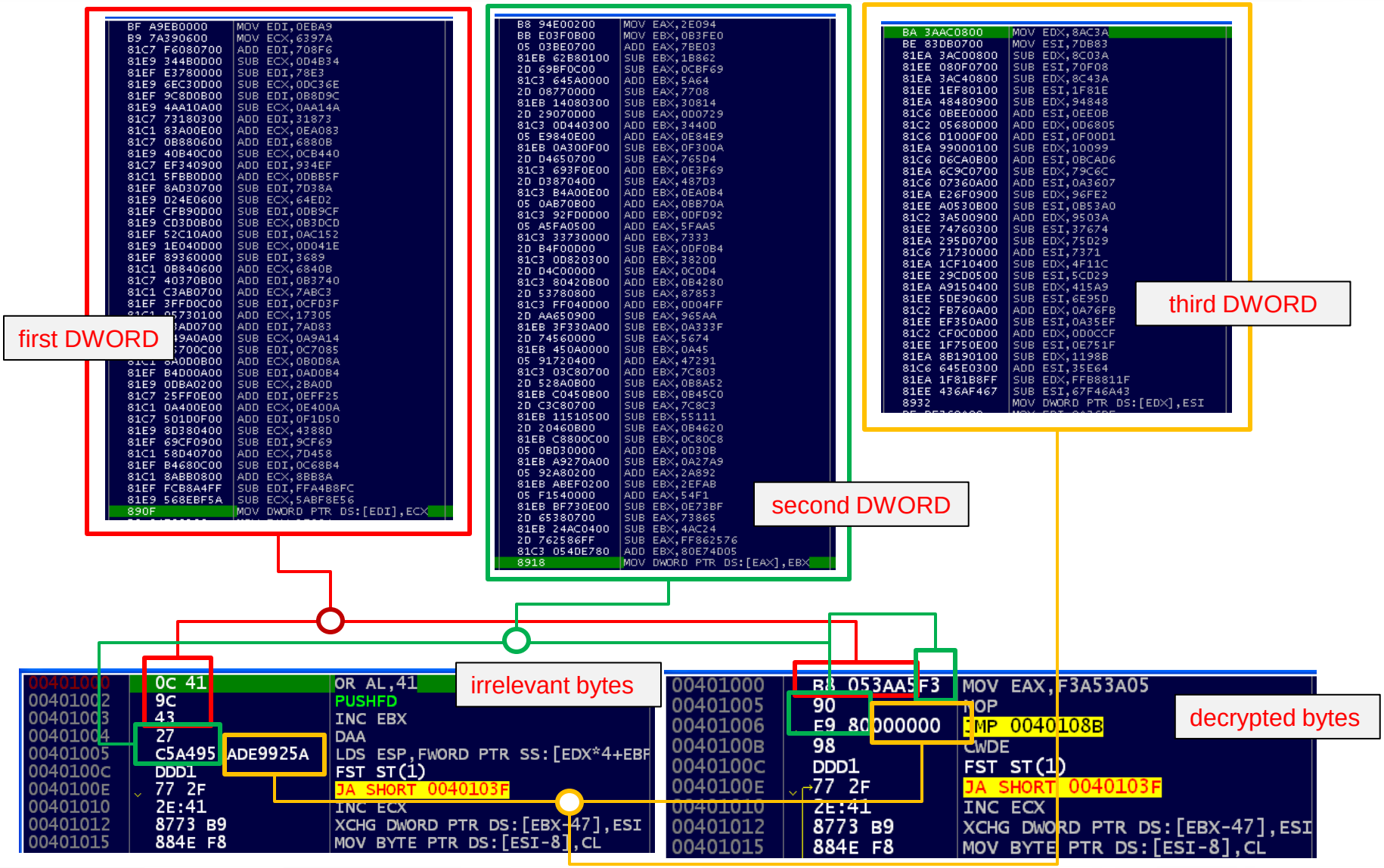
Metamorphic Algorithm (sample 1)



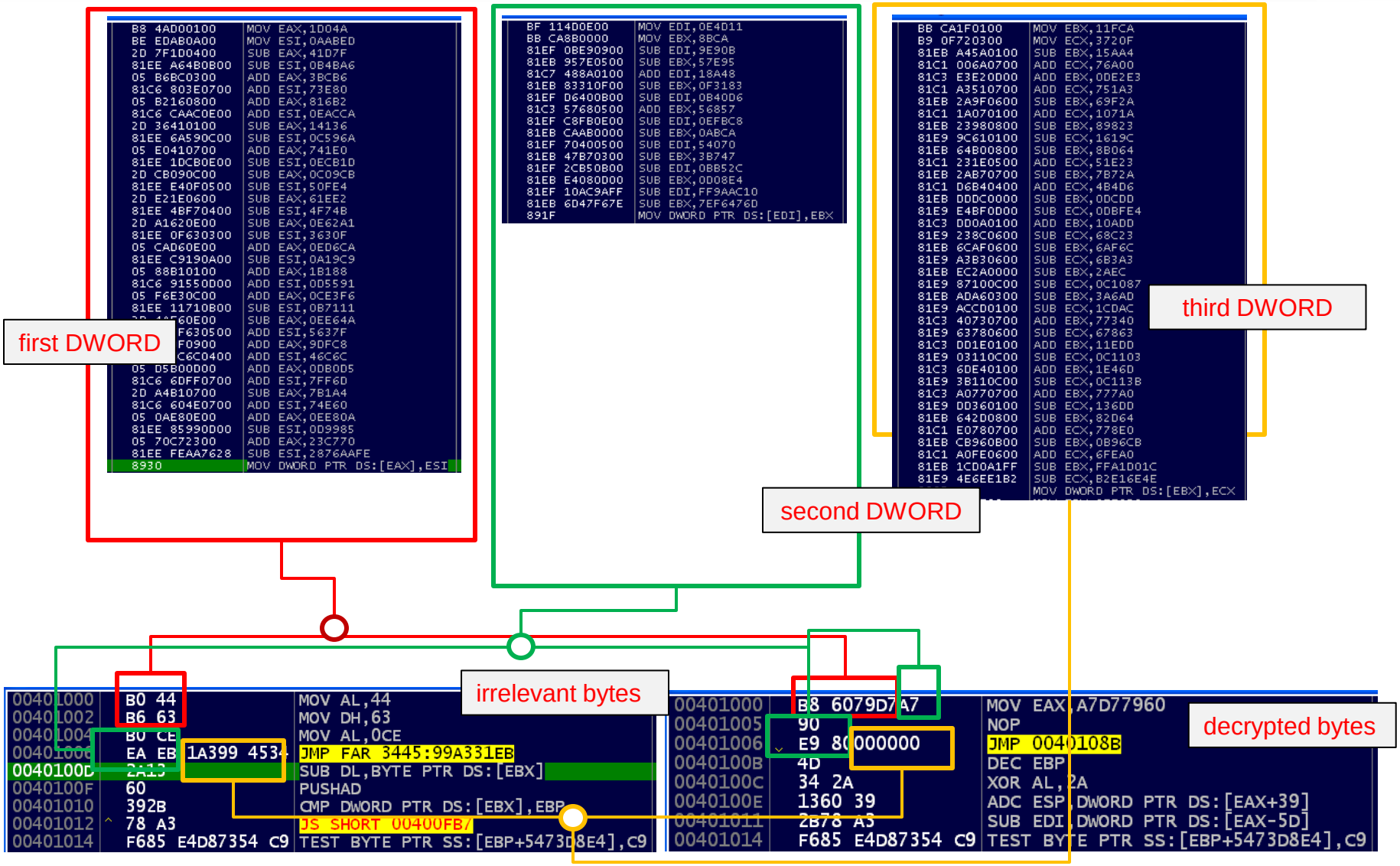
Metamorphic Algorithm (sample 2)



Metamorphic Algorithm (sample 1)



Metamorphic Algorithm (sample 2)



Metamorphic Algorithm (comparison)

first DWORD

```
BF A9EB0000    MOV EDI,0EBA9
B9 7A390600    MOV ECX,6397A
81C7 F6080700  ADD EDI,708F6
81E9 344B0D00  SUB ECX,0D4B34
81EF E3780000  SUB EDI,78E3
81E9 6EC30D00  SUB ECX,0DC36E
81EF 9C8D0B00  SUB EDI,0B8D9C
81E9 4AA10A00  SUB ECX,0AA14A
81C7 73180300  ADD EDI,31873
81C1 83A00E00  ADD ECX,0EA083
81C7 0B880600  ADD EDI,6880B
81E9 40B40C00  SUB ECX,0CB440
81C7 EF340900  ADD EDI,934EF
81C1 5FBB0D00  ADD ECX,0DBB5F
81EF 8AD30700  SUB EDI,7D38A
81E9 D24E0600  SUB ECX,64ED2
81EF CFB90D00  SUB EDI,0DB9CF
81E9 CD3D0B00  SUB ECX,0B3DCD
81EF 52C10A00  SUB EDI,0AC152
81E9 1E040D00  SUB ECX,0D041E
81EF 89360000  SUB EDI,3689
81C1 0B840600  ADD ECX,6840B
81C7 40370B00  ADD EDI,0B3740
81C1 C3AB0700  ADD ECX,7ABC3
81EF 3FFD0C00  SUB EDI,0CFD3F
81C1 05730100  ADD ECX,17305
81C7 83AD0700  ADD EDI,7AD83
81E9 149A0A00  SUB ECX,0A9A14
81EF 85700C00  SUB EDI,0C7085
81C1 8A0D0B00  ADD ECX,0B0D8A
81EF B4D00A00  SUB EDI,0AD0B4
81E9 0DBA0200  SUB ECX,2BA0D
81C7 25FF0E00  ADD EDI,0EFF25
81C1 0A400E00  ADD ECX,0E400A
81C7 501D0F00  ADD EDI,0F1D50
81E9 8D380400  SUB ECX,4388D
81EF FCB8A4FF  SUB EDI,FFA4B8FC
81E9 568EBF5A  SUB ECX,5ABF8E56
890F           MOV DWORD PTR DS:[EDI],ECX
```

MOV [EDI],ECX

Sample 1

```
B8 4AD00100    MOV EAX,1D04A
BE EDAB0A00    MOV ESI,0AABED
2D 7F1D0400    SUB EAX,41D7F
81EE A64B0B00  SUB ESI,0B4BA6
05 B6BC0300    ADD EAX,3BCB6
81C6 803E0700  ADD ESI,73E80
05 B2160800    ADD EAX,816B2
81C6 CAAC0E00  ADD ESI,0EACCA
2D 36410100    SUB EAX,14136
81EE 6A590C00  SUB ESI,0C596A
05 E0410700    ADD EAX,741E0
81EE 1DCB0E00  SUB ESI,0ECB1D
2D CB090C00    SUB EAX,0C09CB
81EE E40F0500  SUB ESI,50FE4
2D E21E0600    SUB EAX,61EE2
81EE 4BF70400  SUB ESI,4F74B
2D A1620E00    SUB EAX,0E62A1
81EE 0F630300  SUB ESI,3630F
05 CAD60E00    ADD EAX,0ED6CA
81EE C9190A00  SUB ESI,0A19C9
05 88B10100    ADD EAX,1B188
81C6 91550D00  ADD ESI,0D5591
05 F6E30C00    ADD EAX,0CE3F6
81EE 11710B00  SUB ESI,0B7111
2D 4AE60E00    SUB EAX,0EE64A
81C6 7F630500  ADD ESI,5637F
05 C8DF0900    ADD EAX,9DFC8
81C6 6C6C0400  ADD ESI,46C6C
05 D5B00D00    ADD EAX,0DB0D5
81C6 6DFF0700  ADD ESI,7FF6D
2D A4B10700    SUB EAX,7B1A4
81EE 85990D00  SUB ESI,0D9985
05 70C72300    ADD EAX,23C770
81EE FEAA7628  SUB ESI,2876AAFE
8930           MOV DWORD PTR DS:[EAX],ESI
```

MOV [EAX],ESI

Sample 2

Metamorphic Algorithm (comparison)

second DWORD

```
B8 94E00200    MOV EAX,2E094
BB E03F0B00    MOV EBX,0B3FE0
05 03BE0700    ADD EAX,7BE03
81EB 62B80100  SUB EBX,1B862
2D 69BF0C00    SUB EAX,0CBF69
81C3 645A0000  ADD EBX,5A64
2D 08770000    SUB EAX,7708
81EB 14080300  SUB EBX,30814
2D 29070D00    SUB EAX,0D0729
81C3 0D440300  ADD EBX,3440D
05 E9840E00    ADD EAX,0E84E9
81EB 0A300F00  SUB EBX,0F300A
2D D4650700    SUB EAX,765D4
81C3 693F0E00  ADD EBX,0E3F69
2D D3870400    SUB EAX,487D3
81C3 B4A00E00  ADD EBX,0EA0B4
05 0AB70B00    ADD EAX,0BB70A
81C3 92FD0D00  ADD EBX,0DFD92
05 A5FA0500    ADD EAX,5FAA5
81C3 33730000  ADD EBX,7333
2D B4F00D00    SUB EAX,0DF0B4
81C3 0D820300  ADD EBX,3820D
2D D4C00000    SUB EAX,0C0D4
81C3 80420B00  ADD EBX,0B4280
2D 53780800    SUB EAX,87853
81C3 FF040D00  ADD EBX,0D04FF
2D AA650900    SUB EAX,965AA
81EB 3F330A00  SUB EBX,0A333F
2D 74560000    SUB EAX,5674
81EB 450A0000  SUB EBX,0A45
05 91720400    ADD EAX,47291
81C3 03C80700  ADD EBX,7C803
2D 528A0B00    SUB EAX,0B8A52
81EB C0450B00  SUB EBX,0B45C0
2D C3C80700    SUB EAX,7C8C3
81EB 11510500  SUB EBX,55111
2D 20460B00    SUB EAX,0B4620
81EB C8800C00  SUB EBX,0C80C8
05 0BD30000    ADD EAX,0D30B
81EB A9270A00  SUB EBX,0A27A9
05 92A80200    ADD EAX,2A892
81EB ABEF0200  SUB EBX,2EFAB
2D 762586FF    SUB EAX,FF862576
81C3 054DE780  ADD EBX,80E74D05
8918           MOV DWORD PTR DS:[EAX],EBX
```

MOV [EAX],EBX

Sample 1

```
BF 114D0E00    MOV EDI,0E4D11
BB CA8B0000    MOV EBX,8BCA
81EF 0BE90900  SUB EDI,9E90B
81EB 957E0500  SUB EBX,57E95
81C7 488A0100  ADD EDI,18A48
81EB 83310F00  SUB EBX,0F3183
81EF D6400B00  SUB EDI,0B40D6
81C3 57680500  ADD EBX,56857
81EF C8FB0E00  SUB EDI,0EFBC8
81EB CAAB0D00  SUB EBX,0ABCA
81EF 10AC9AFF  SUB EDI,FF9AAC10
81EB 6D47F67E  SUB EBX,7EF6476D
891F           MOV DWORD PTR DS:[EDI],EBX
```

MOV [EDI],EBX

Sample 2

Metamorphic Algorithm (comparison)

third DWORD

```
BA 3AAC0800    MOV EDX,8AC3A
BE 83DB0700    MOV ESI,7DB83
81EA 3AC00800  SUB EDX,8C03A
81EE 080F0700  SUB ESI,70F08
81EA 3AC40800  SUB EDX,8C43A
81EE 1EF80100  SUB ESI,1F81E
81EA 48480900  SUB EDX,94848
81C6 0BEE0000  ADD ESI,0EE0B
81C2 05680D00  ADD EDX,0D6805
81C6 D1000F00  ADD ESI,0F00D1
81EA 99000100  SUB EDX,10099
81C6 D6CA0B00  ADD ESI,0BCAD6
81EA 6C9C0700  SUB EDX,79C6C
81C6 07360A00  ADD ESI,0A3607
81EA E26F0900  SUB EDX,96FE2
81EE A0530B00  SUB ESI,0B53A0
81C2 3A500900  ADD EDX,9503A
81EE 74760300  SUB ESI,37674
81EA 295D0700  SUB EDX,75D29
81C6 71730000  ADD ESI,7371
81EA 1CF10400  SUB EDX,4F11C
81EE 29CD0500  SUB ESI,5CD29
81EA A9150400  SUB EDX,415A9
81EE 5DE90600  SUB ESI,6E95D
81C2 FB760A00  ADD EDX,0A76FB
81EE EF350A00  SUB ESI,0A35EF
81C2 CF0C0D00  ADD EDX,0D0CCF
81EE 436AF467  SUB ESI,67F46A43
8932           MOV DWORD PTR DS:[EDX],ESI
```

MOV [EDX],ESI

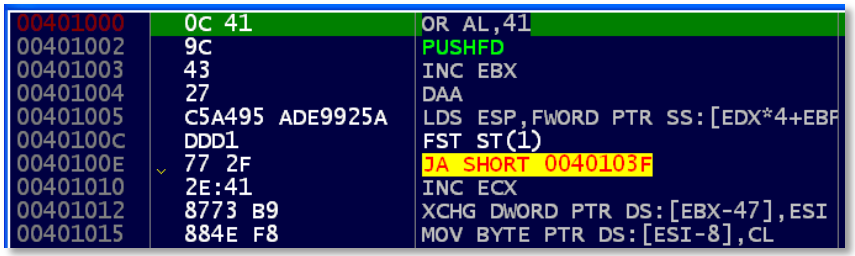
Sample 1

```
BB CA1F0100    MOV EBX,11FCA
B9 0F720300    MOV ECX,3720F
81EB A45A0100  SUB EBX,15AA4
81C1 006A0700  ADD ECX,76A00
81C3 E3E20D00  ADD EBX,0DE2E3
81C1 A3510700  ADD ECX,751A3
81EB 2A9F0600  SUB EBX,69F2A
81C1 1A070100  ADD ECX,1071A
81EB 23980800  SUB EBX,89823
81E9 9C610100  SUB ECX,1619C
81EB 64B00800  SUB EBX,8B064
81C1 231E0500  ADD ECX,51E23
81EB 2AB70700  SUB EBX,7B72A
81C1 D6B40400  ADD ECX,4B4D6
81EB DDDC0000  SUB EBX,0DCDD
81E9 E4BF0D00  SUB ECX,0DBFE4
81C3 DD0A0100  ADD EBX,10ADD
81E9 238C0600  SUB ECX,68C23
81EB 6CAF0600  SUB EBX,6AF6C
81E9 A3B30600  SUB ECX,6B3A3
81EB EC2A0000  SUB EBX,2AEC
81E9 87100C00  SUB ECX,0C1087
81EB ADA60300  SUB EBX,3A6AD
81E9 ACCD0100  SUB ECX,1CDAC
81C3 40730700  ADD EBX,77340
81E9 63780600  SUB ECX,67863
81C3 DD1E0100  ADD EBX,11EDD
81E9 03110C00  SUB ECX,0C1103
81C3 6DE40100  ADD EBX,1E46D
81E9 3B110C00  SUB ECX,0C113B
81EB CB960B00  SUB EBX,0B96CB
81C1 A0FE0600  ADD ECX,6FEA0
81EB 1CD0A1FF  SUB EBX,FFA1D01C
81E9 4E6EE1B2  SUB ECX,B2E16E4E
890B           MOV DWORD PTR DS:[EBX],ECX
```

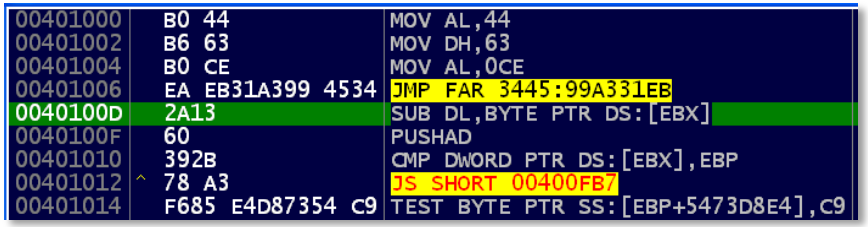
MOV [EBX],ECX

Sample 2

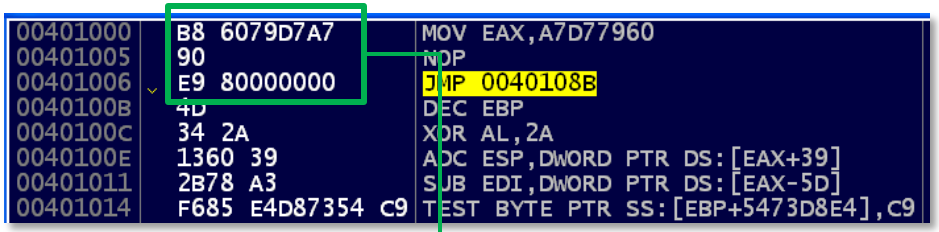
Metamorphic Algorithm (detection)



Sample 1



Sample 2



MOV EAX, --------
NOP
JMP 0040108B

Demo – Metamorphic Algorithm

Virlock As A File Infector

Cleaning: How To Clean An Infected File

Basics:

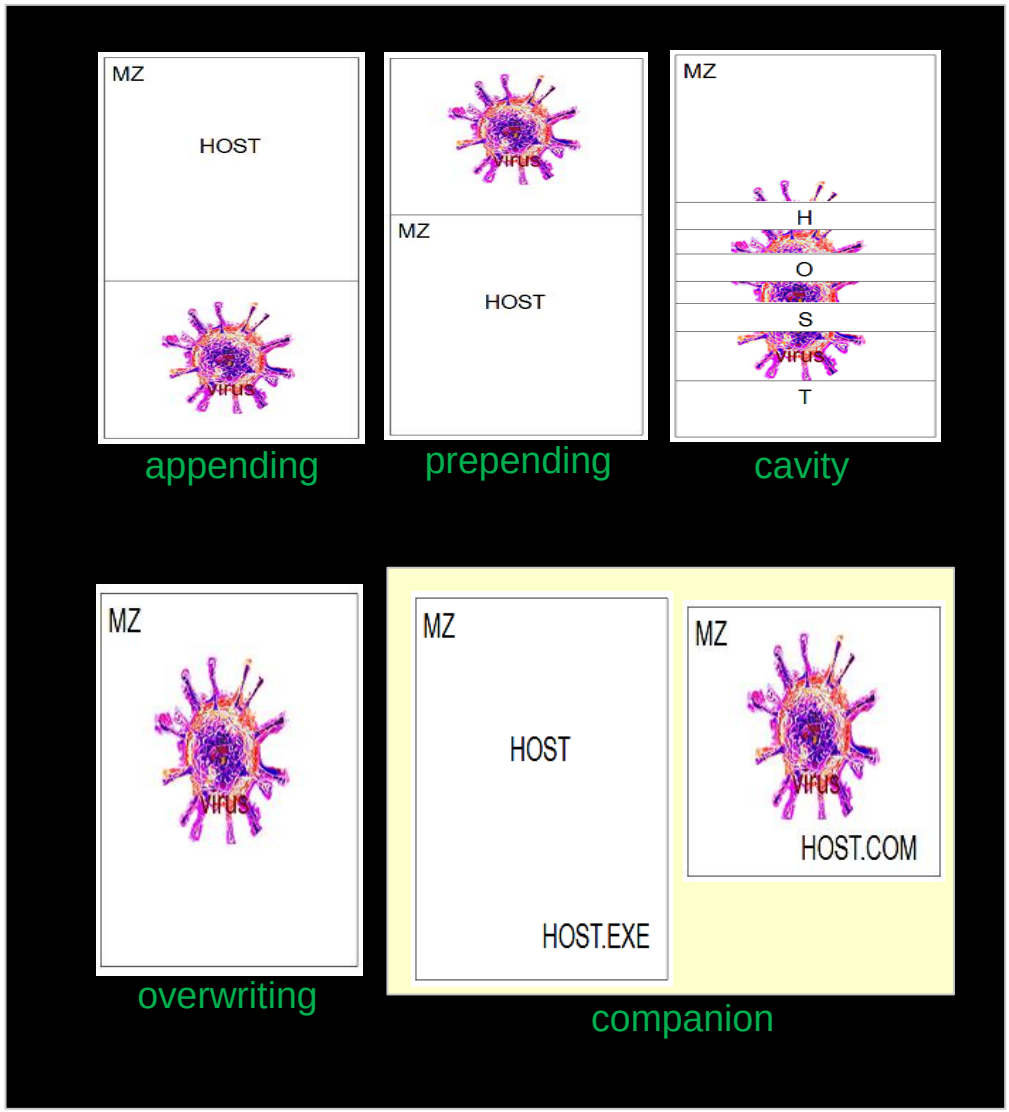
- Determine the kind of virus
- Determine how to extract and restore the host file

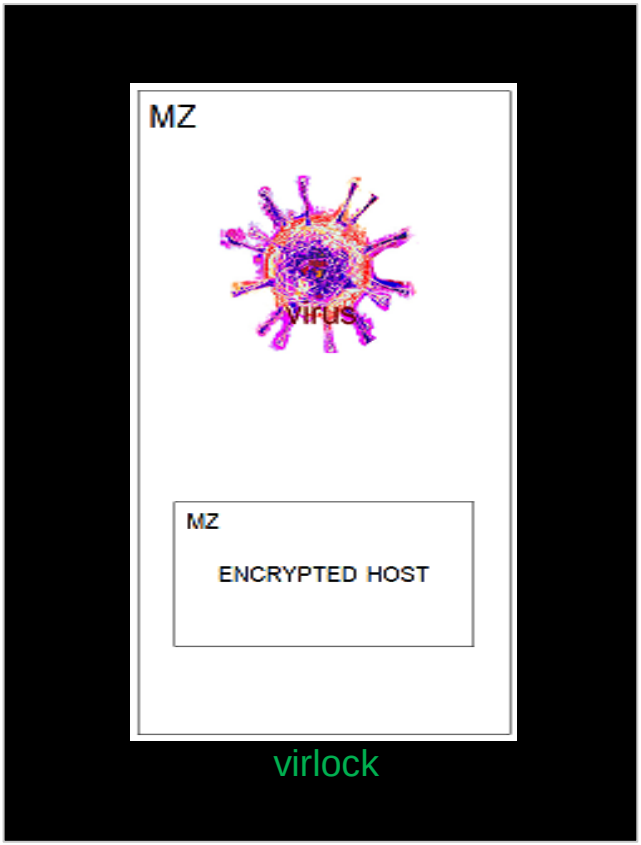
Different Kinds Of File Infectors

Basics:

- Appending
- Prepending
- Cavity
- Overwriting
- Companion

Different Kinds Of File Infectors



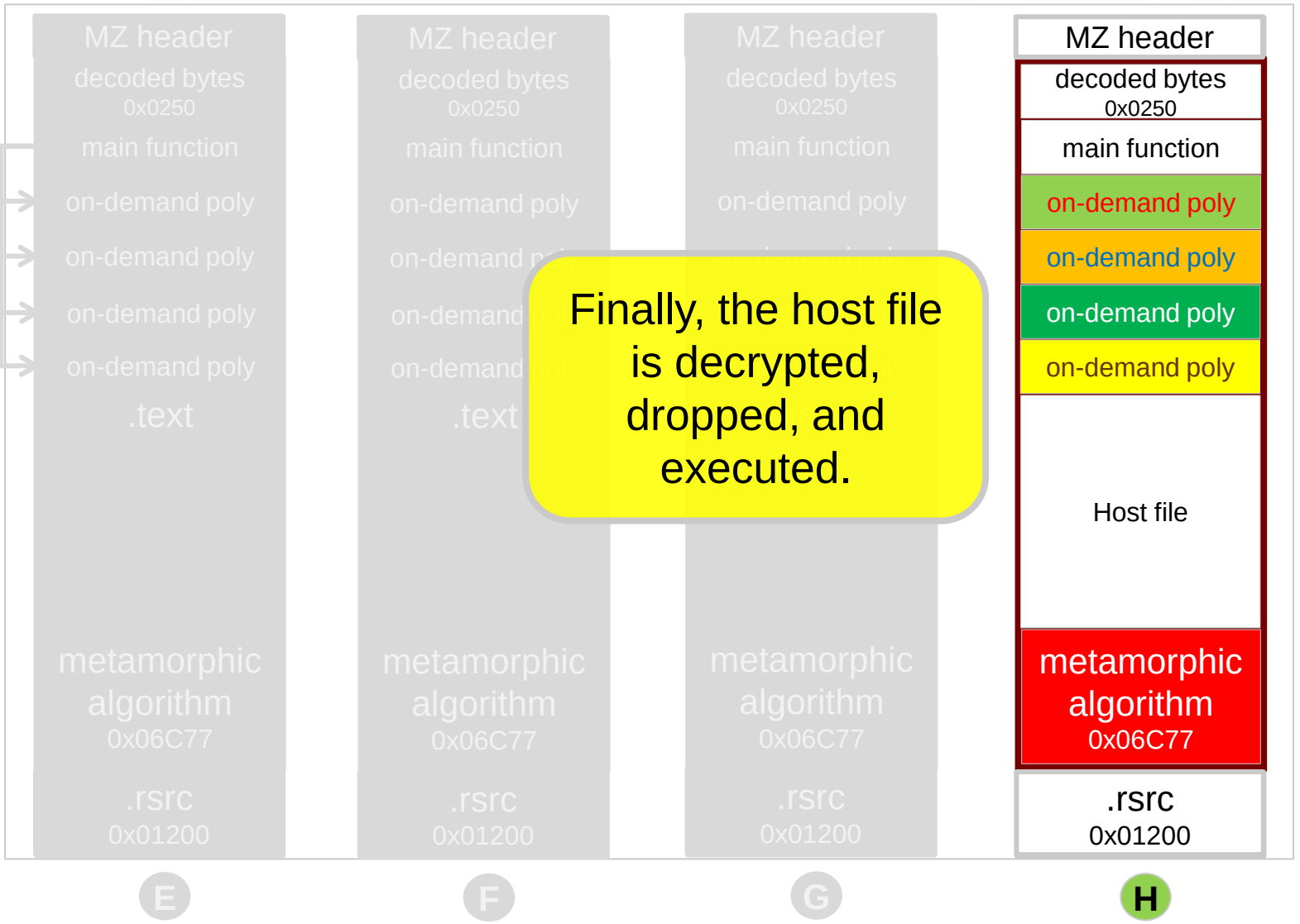


Cleaning: Extracting The Host File From Virlock

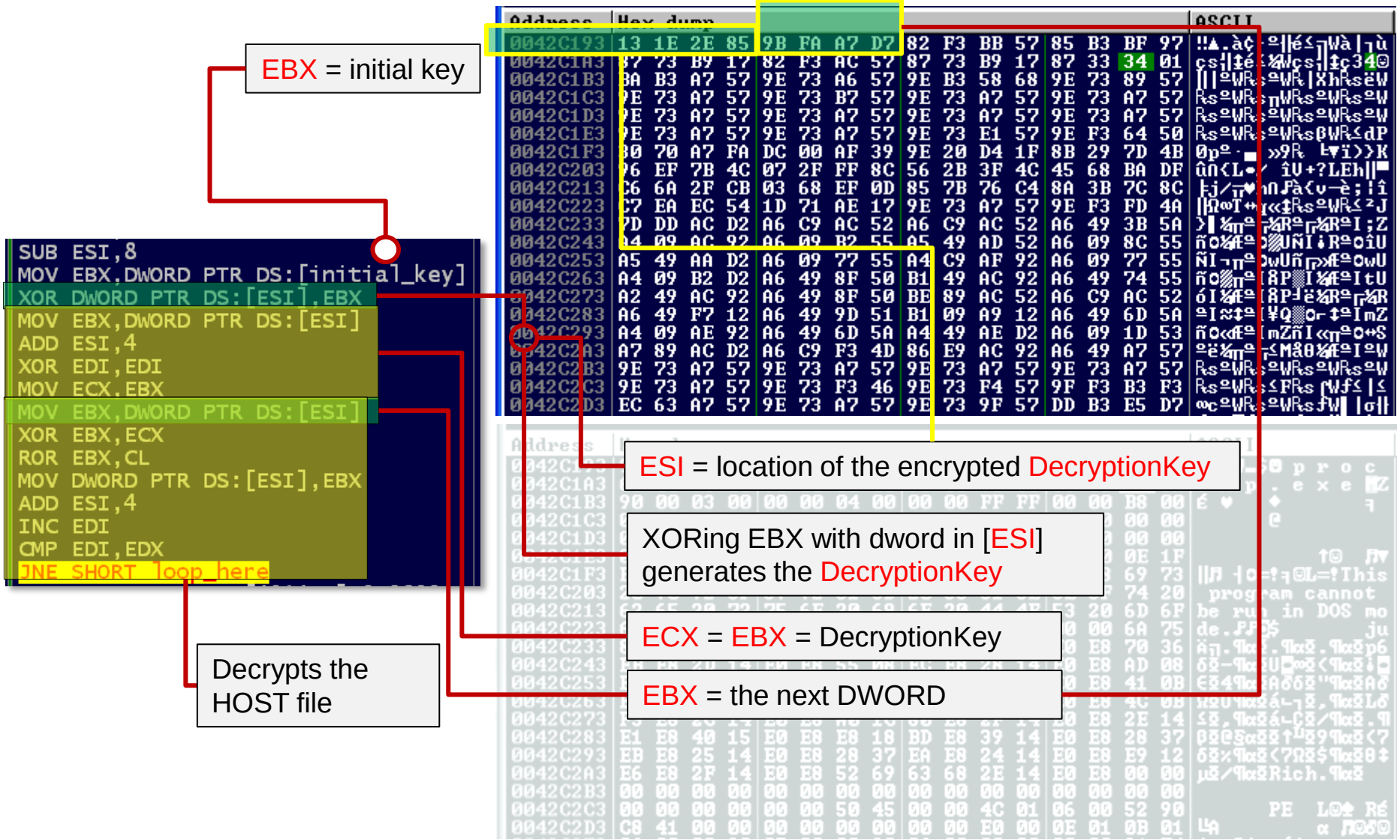
Details:

- Host file is encrypted and embedded within the malware
- DecryptionKey can be found within the malware
- DecryptionKey is encrypted using a simple XOR
- Uses a simple decryption algorithm to extract the host file

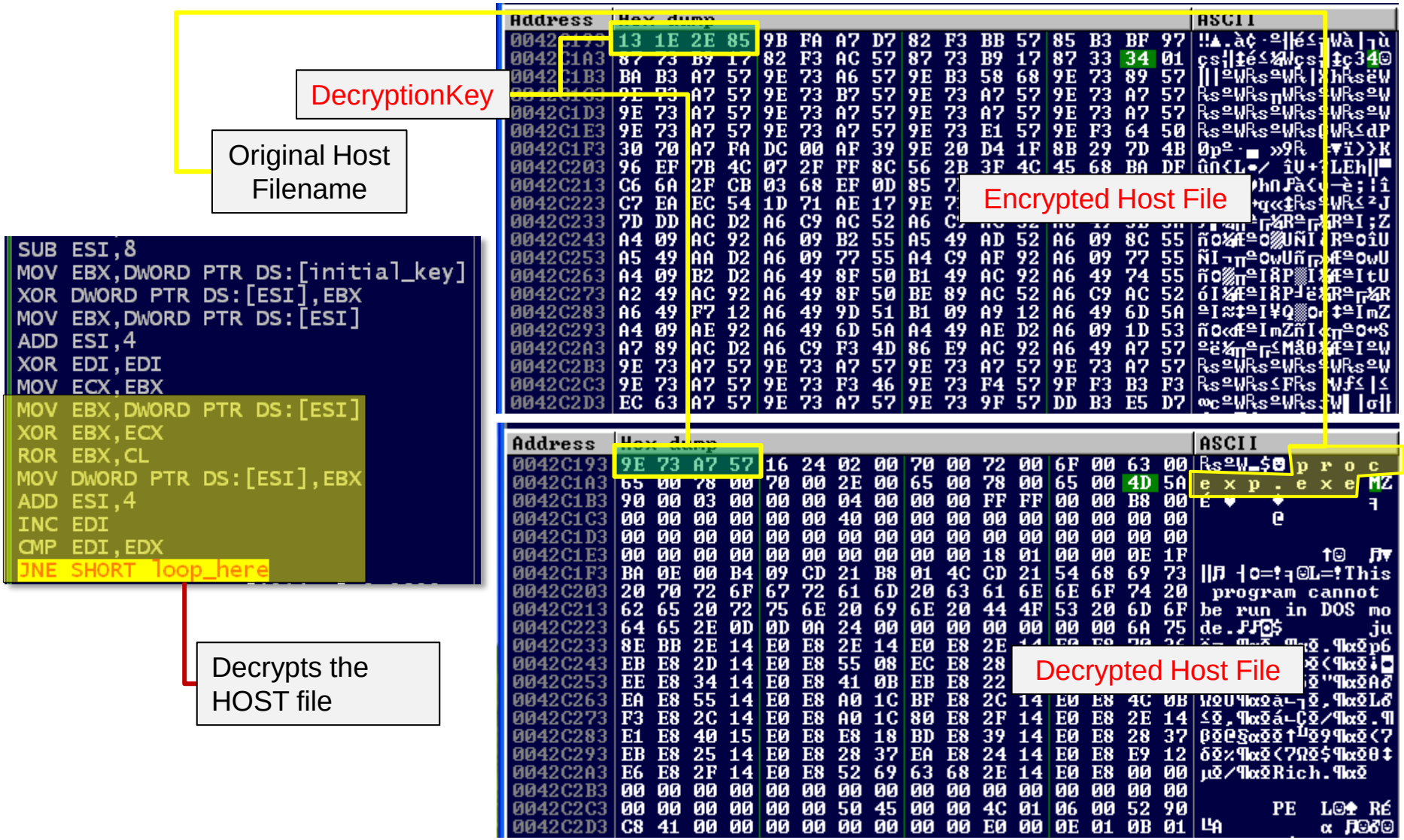
Reversing Stages



Cleaning: Extracting The Host File From Virlock

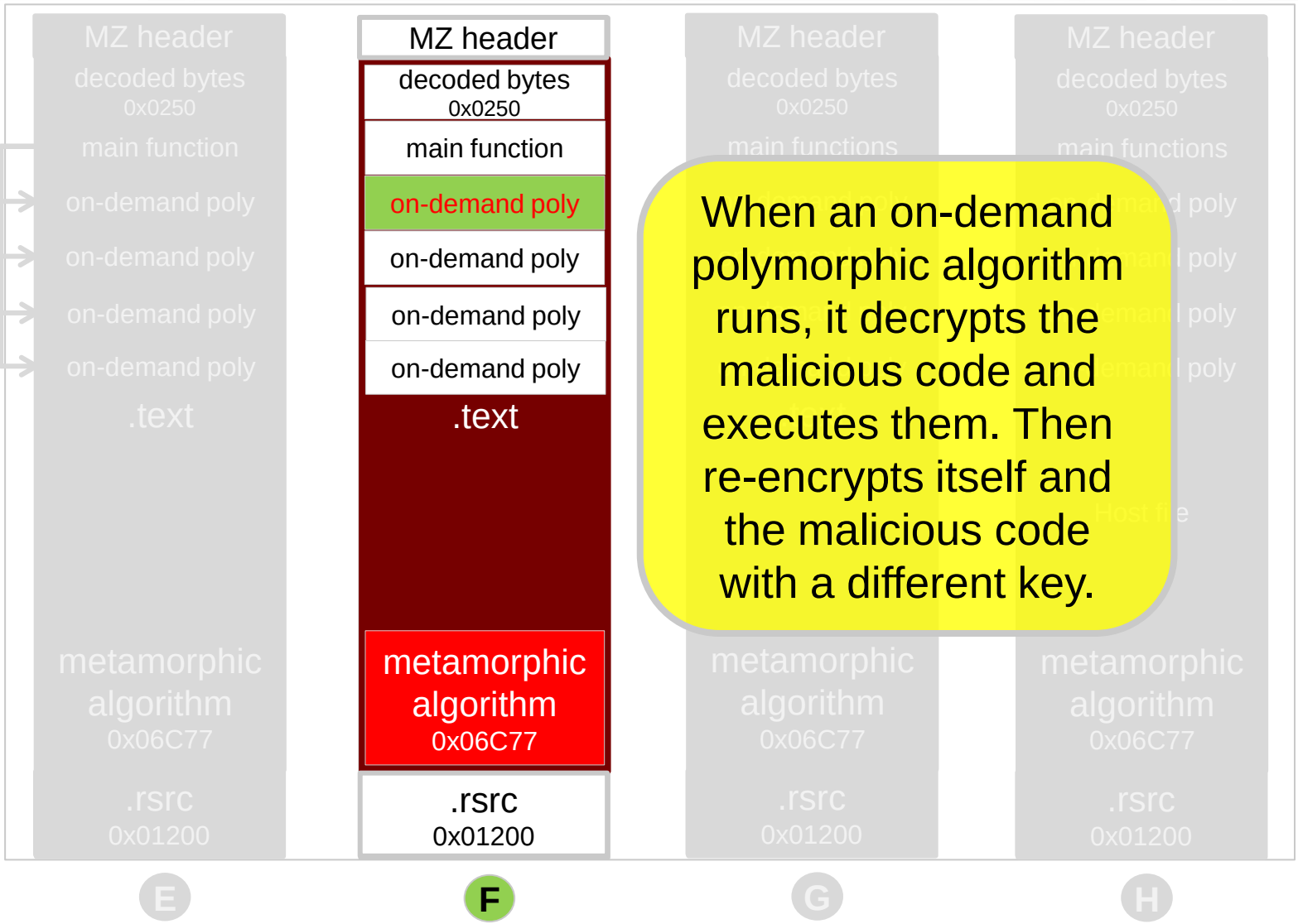


Cleaning: Extracting The Host File From Virlock



Virlock As A Polymorphic Malware

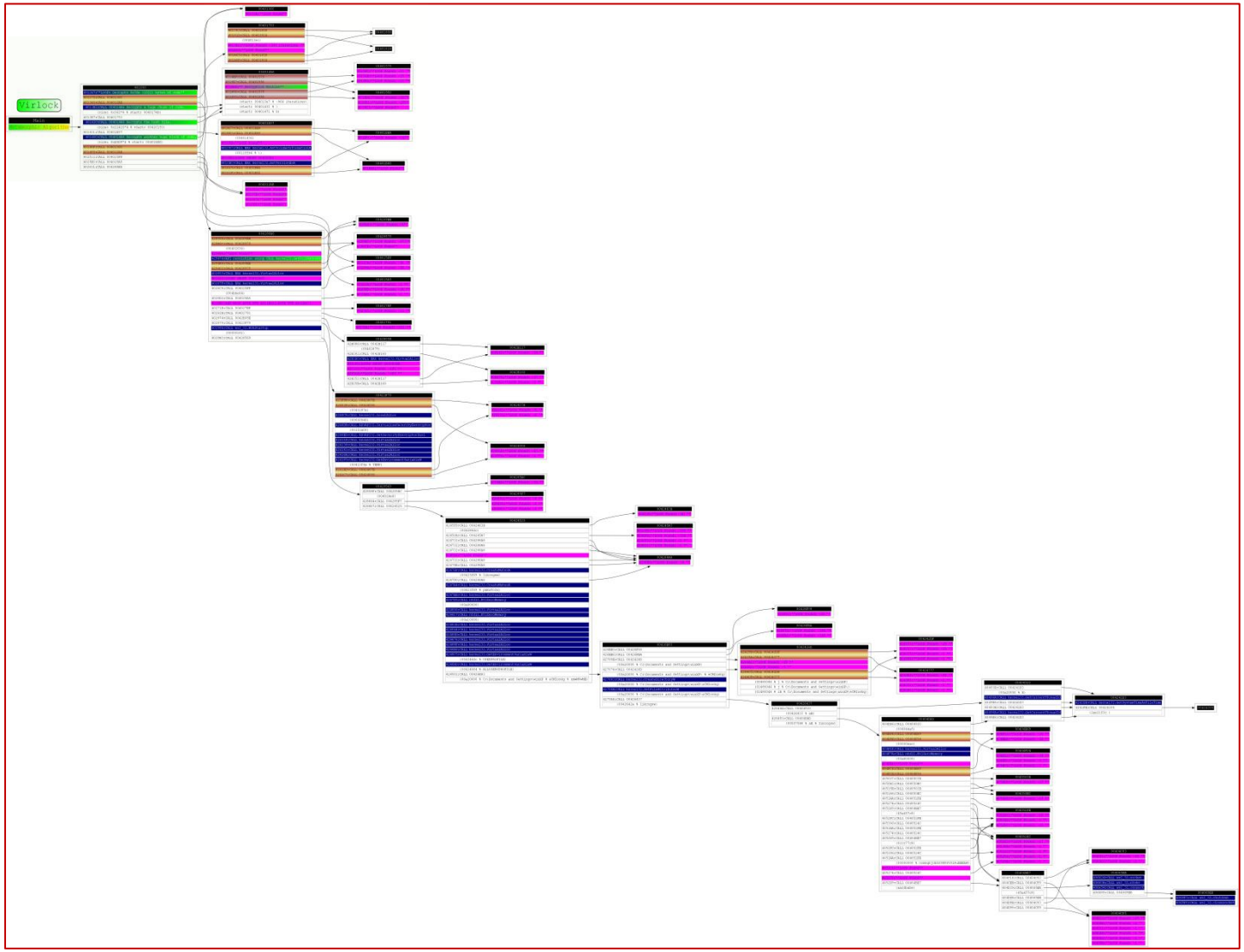
Reversing Stages



Dynamic Routine Execution Map

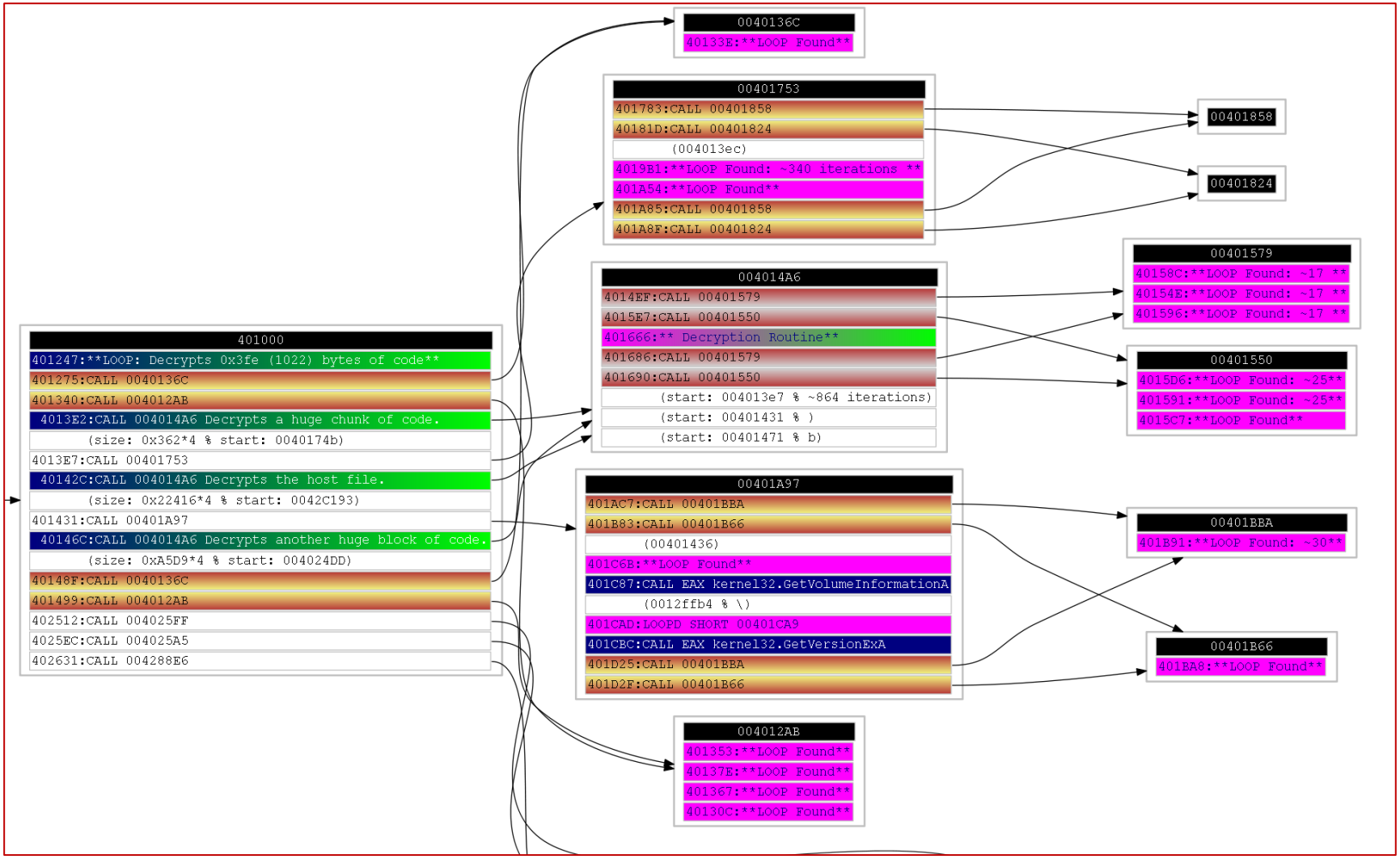
FORTINET

Dynamic Routine Execution Map

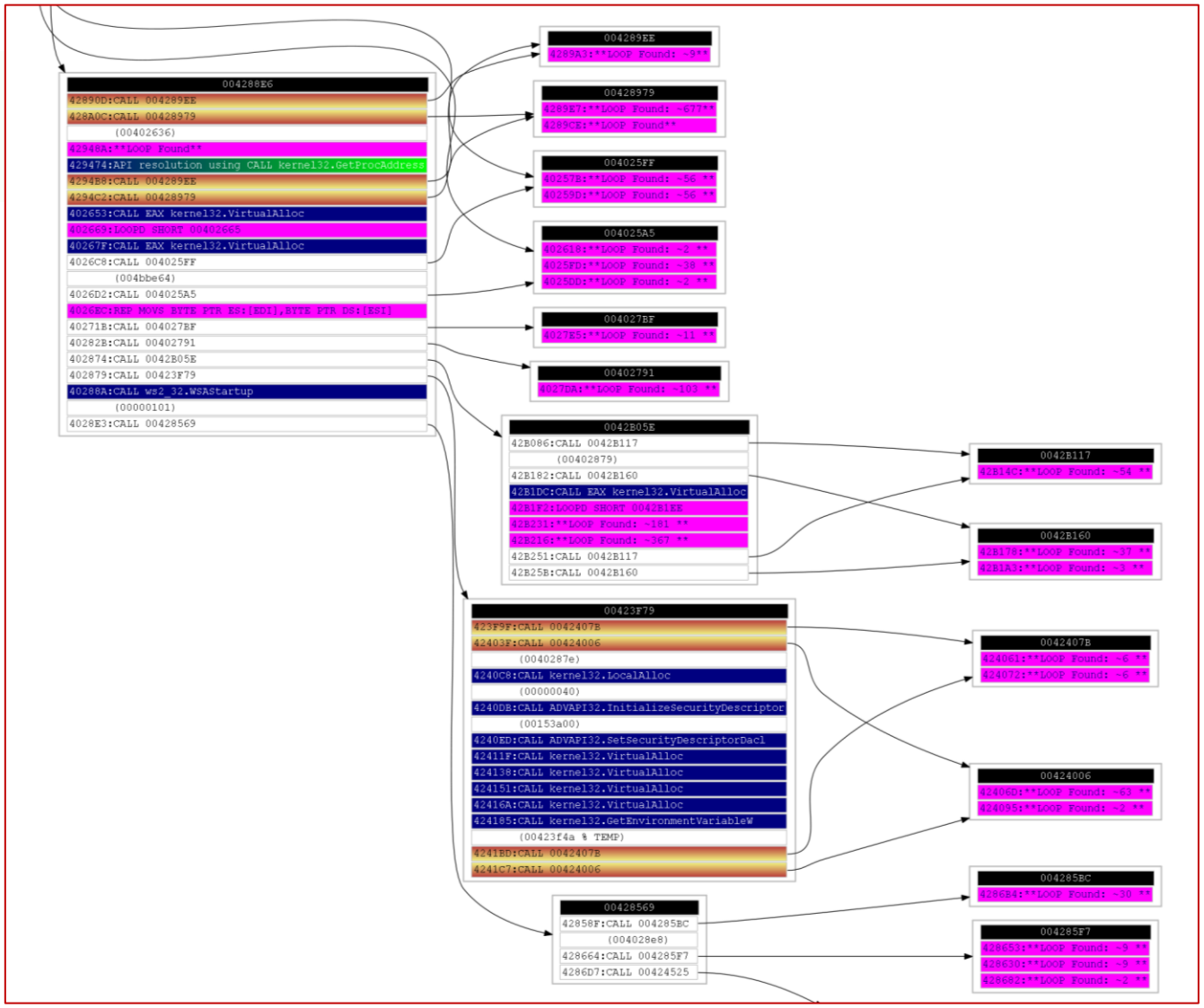


Dynamic Routine Execution Map

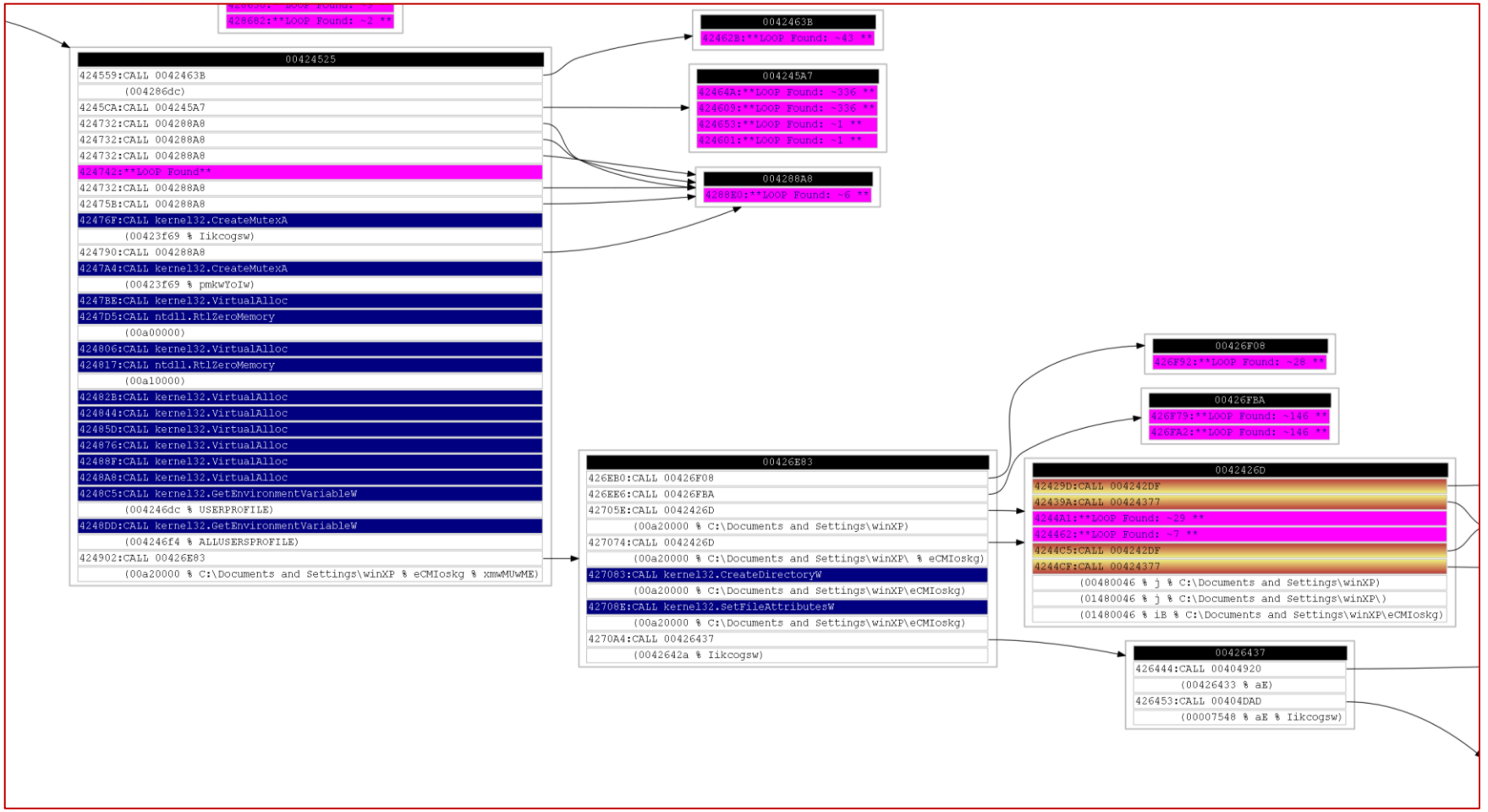
Dynamic Routine Execution Map



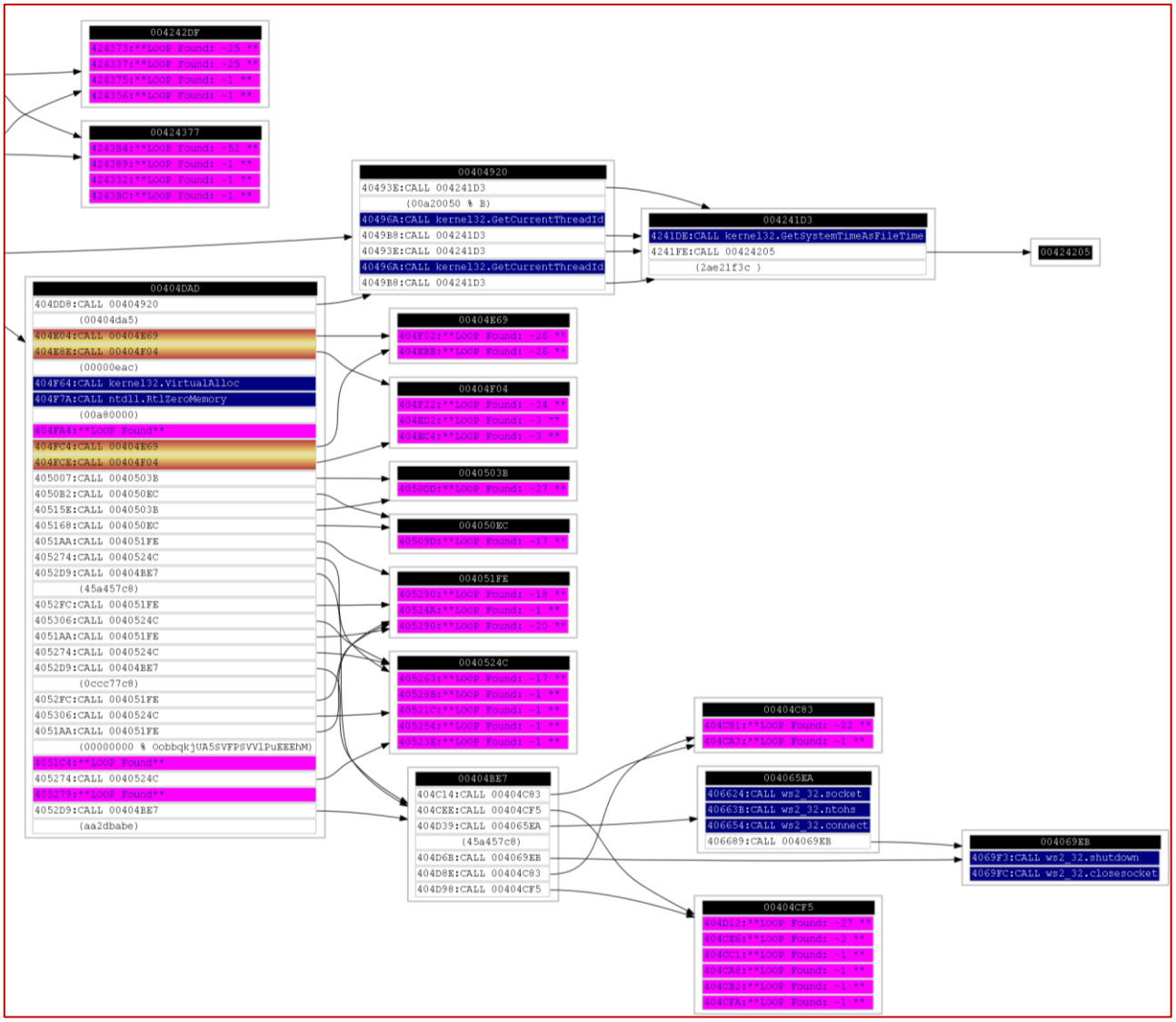
Dynamic Routine Execution Map



Dynamic Routine Execution Map



Dynamic Routine Execution Map

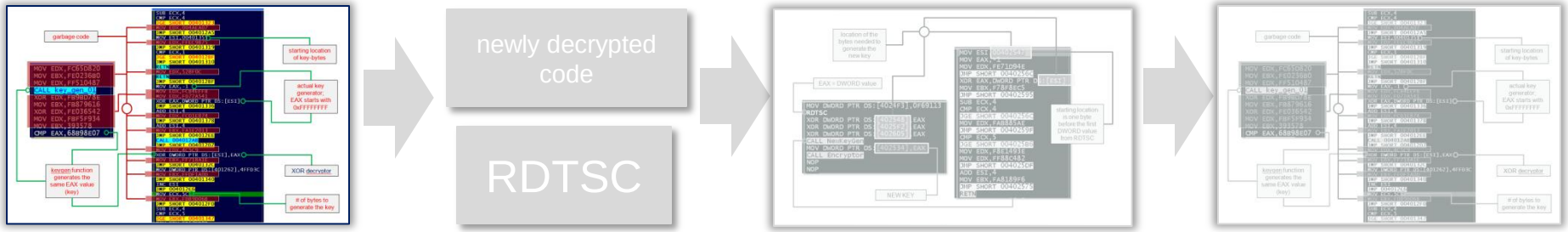


On-Demand Polymorphic Algorithm

On-Demand Polymorphic Algorithm

Implementation

- Uses Decryptor to decrypt a block of code using an old key
- Executes the newly decrypted code
- Uses RDTSC (Read Time-Stamp Counter) to generate a new dword value
- Uses NewKeyGenerator to generate new key
- Uses Encryptor to encrypt the same block of code using the new key

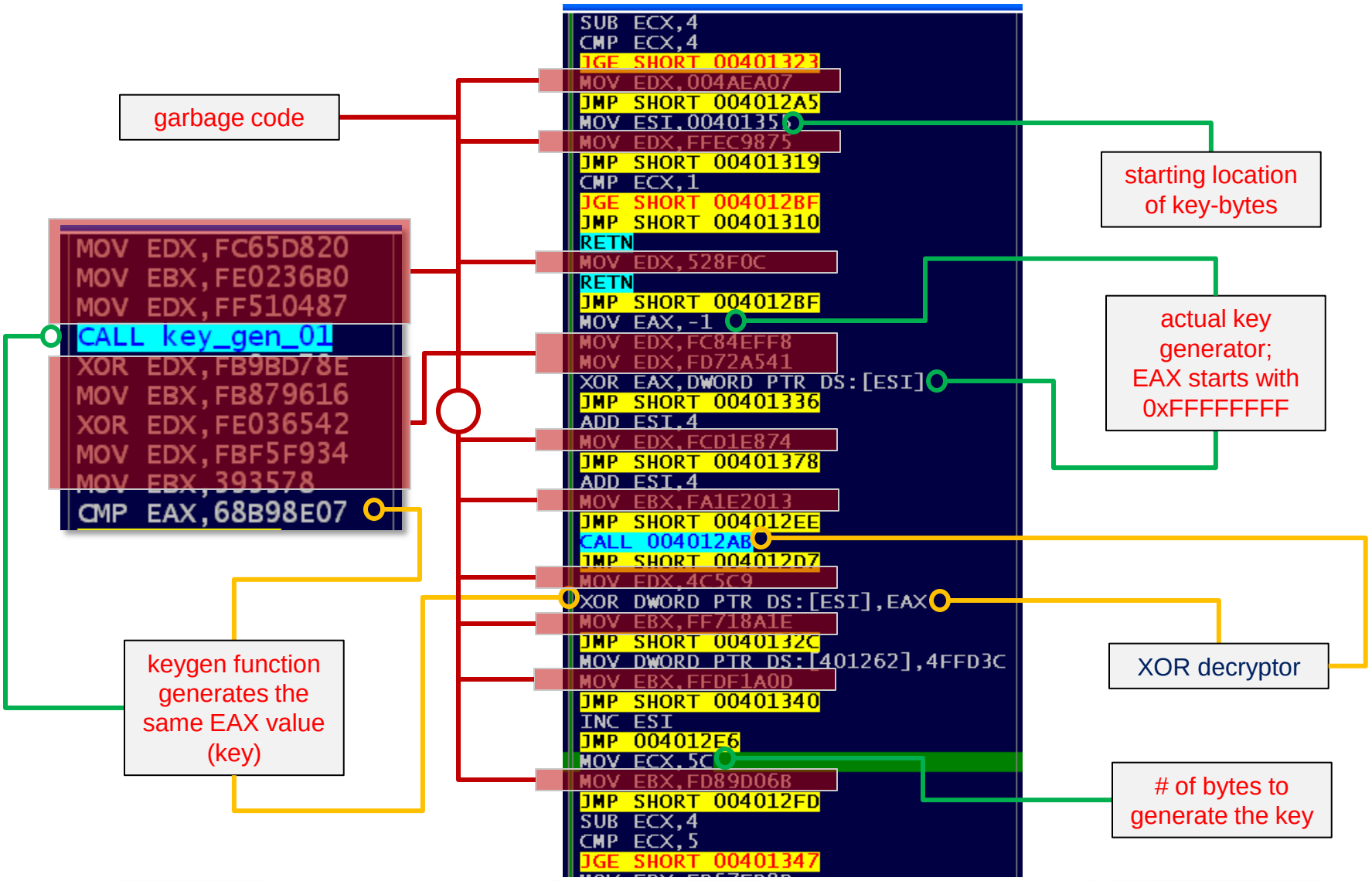


Decryptor

Features:

- Uses garbage code
- Keygen function for redundancy check
- Uses XOR to generate the key
- Uses XOR to decrypt a block of code

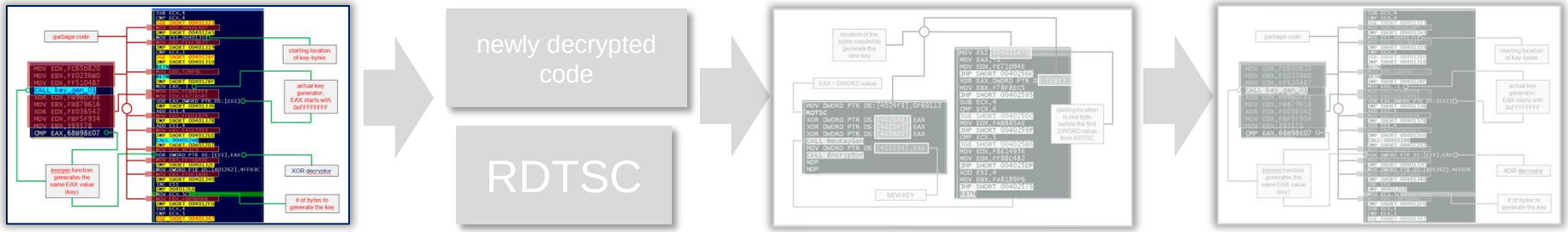
Decryptor


garbage code
starting location of key-bytes
actual key generator; EAX starts with 0xFFFFFFFF
XOR decryptor
# of bytes to generate the key
keygen function generates the same EAX value (key)
SUB ECX,4
CMP ECX,4
JGE SHORT 00401323
MOV EDX,004AEA07
JMP SHORT 004012A5
MOV ESI,00401350
MOV EDX,FFEC9875
JMP SHORT 00401319
CMP ECX,1
JGE SHORT 004012BF
JMP SHORT 00401310
RETN
MOV EDX,528F0C
RETN
JMP SHORT 004012BF
MOV EAX,-1
MOV EDX,FC84EFF8
MOV EDX,FD72A541
XOR EAX,DWORD PTR DS:[ESI]
JMP SHORT 00401336
ADD ESI,4
MOV EDX,FCD1E874
JMP SHORT 00401378
ADD ESI,4
MOV EBX,FA1E2013
JMP SHORT 004012EE
CALL 004012AB
JMP SHORT 004012D7
MOV EDX,4C5C9
XOR DWORD PTR DS:[ESI],EAX
MOV EBX,FF718A1E
JMP SHORT 0040132C
MOV DWORD PTR DS:[401262],4FFD3C
MOV EBX,FFDF1A0D
JMP SHORT 00401340
INC ESI
JMP 004012E6
MOV ECX,5C
MOV EBX,FD89D06B
JMP SHORT 004012FD
SUB ECX,4
CMP ECX,5
JGE SHORT 00401347
MOV EDX,FC65D820
MOV EBX,FE0236B0
MOV EDX,FF510487
CALL key_gen_01
XOR EDX,FB9BD78E
MOV EBX,FB879616
XOR EDX,FE036542
MOV EDX,FBF5F934
MOV EBX,393578
CMP EAX,68B98E07

On-Demand Polymorphic Algorithm

Implementation

- Uses Decryptor to decrypt a block of code using an old key
- Executes the newly decrypted code
- Uses RDTSC (Read Time-Stamp Counter) to generate a new dword value
- Uses NewKeyGenerator to generate new key
- Uses Encryptor to encrypt the same block of code using the new key



On-Demand Polymorphic Algorithm

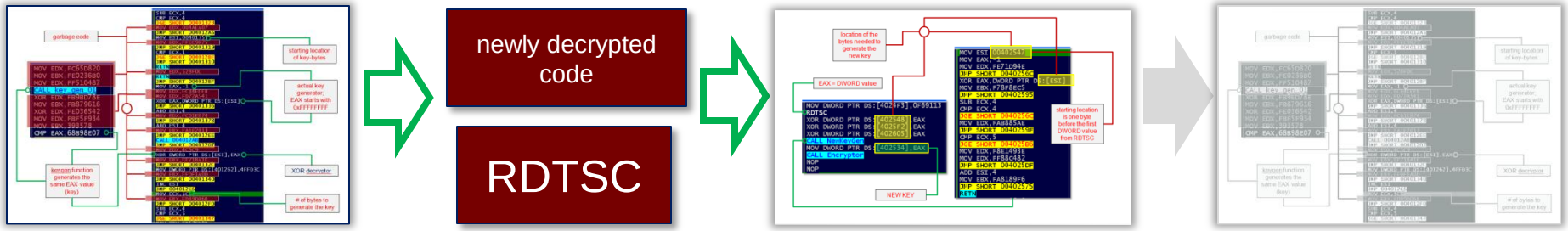
Implementation

- Uses Decryptor to decrypt a block of code using an old key
- Executes the newly decrypted code
- Uses RDTSC (Read Time-Stamp Counter) to generate a new dword value
- Uses NewKeyGenerator to generate new key
- Uses Encryptor to encrypt the same block of code using the new key

On-Demand Polymorphic Algorithm

Implementation

- Uses Decryptor to decrypt a block of code using an old key
- Executes the newly decrypted code
- Uses RDTSC (Read Time-Stamp Counter) to generate a new dword value
- Uses NewKeyGenerator to generate new key
- Uses Encryptor to encrypt the same block of code using the new key

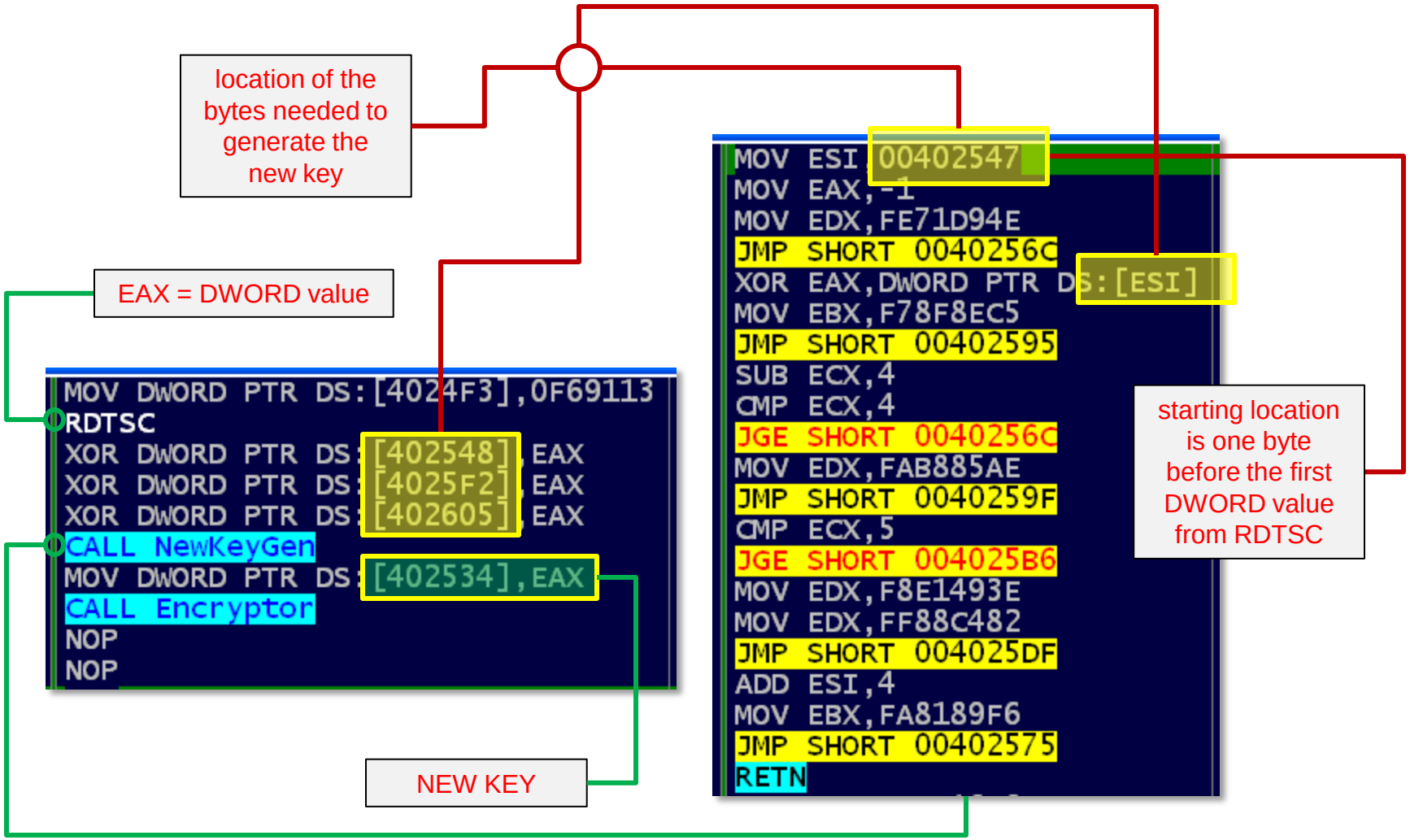


NewKeyGenerator

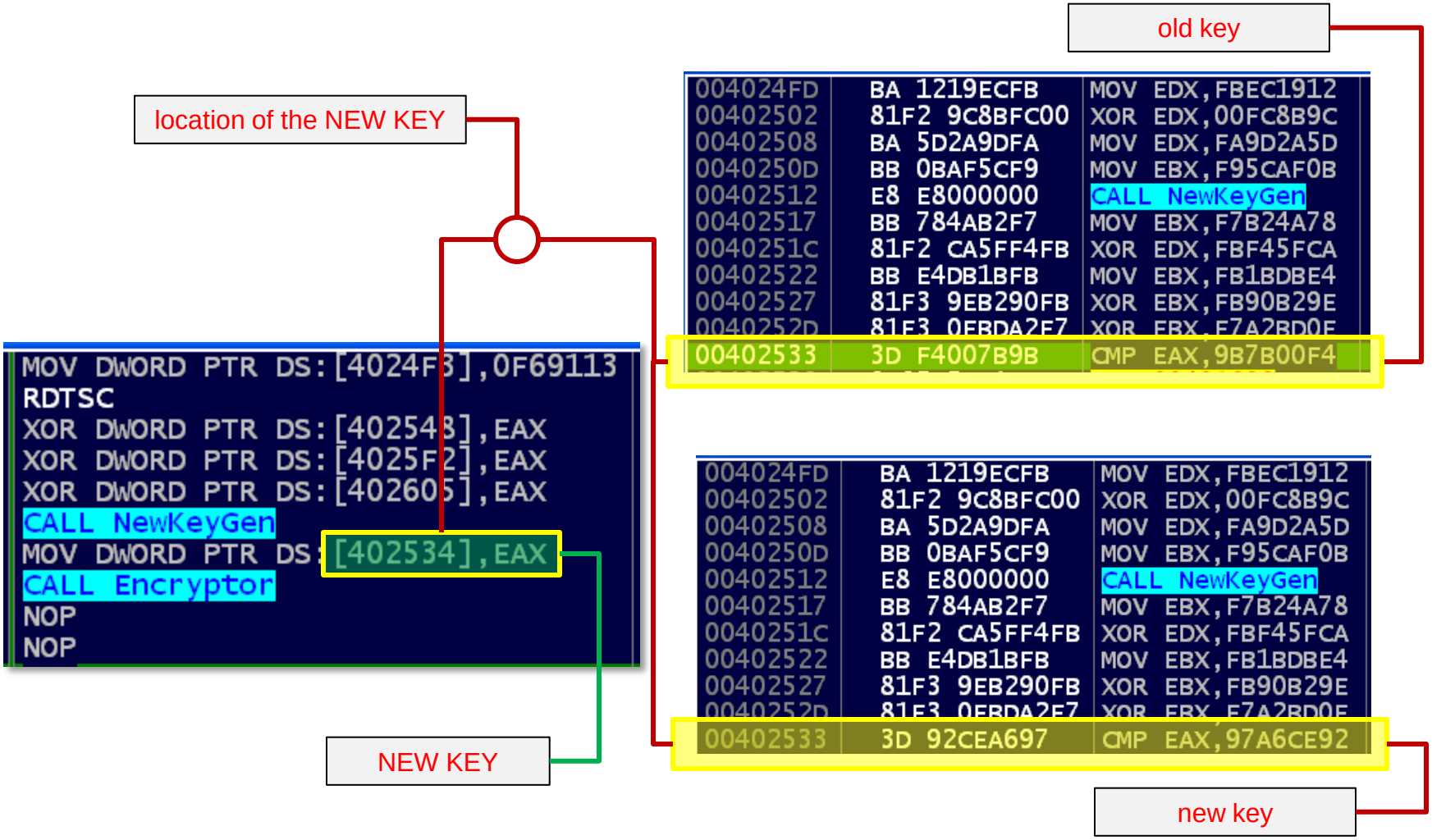
Implementation:

- RDTSC generates a new dword value
- Saves it in different memory locations
- The memory locations are within the memory range that contains key bytes
- Generates new key by XORing the key bytes
- Saves the new key to the original location of the old key used in the Decryptor

NewKeyGenerator



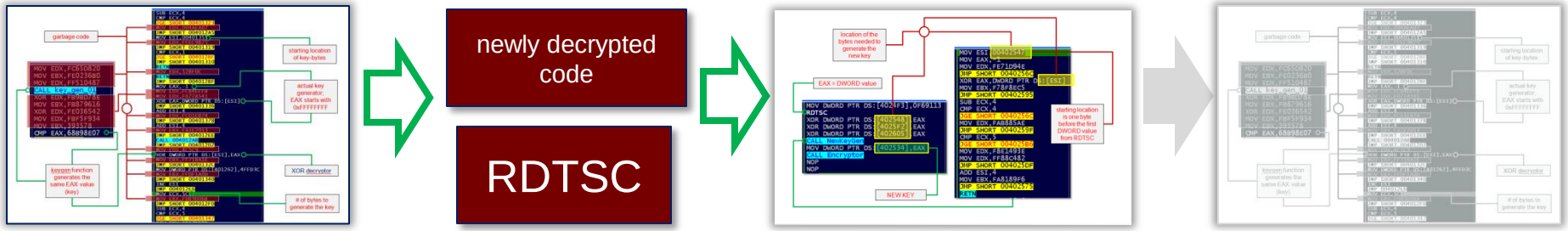
NewKeyGenerator



On-Demand Polymorphic Algorithm

Implementation

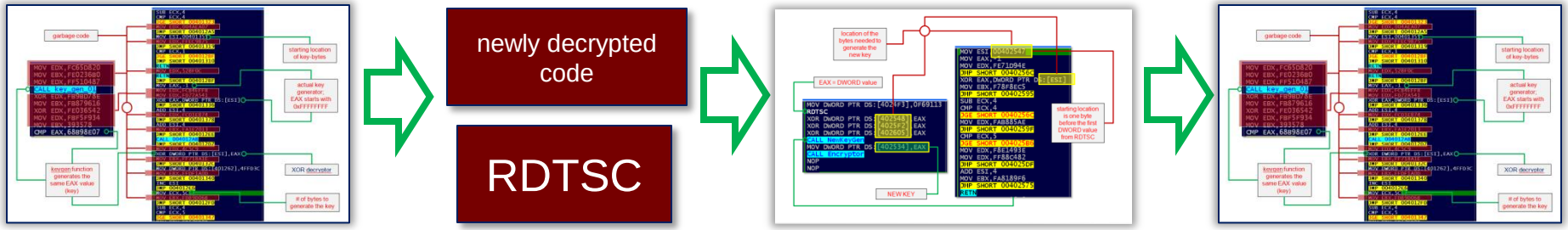
- Uses Decryptor to decrypt a block of code using an old key
- Executes the newly decrypted code
- Uses RDTSC (Read Time-Stamp Counter) to generate a new dword value
- Uses NewKeyGenerator to generate new key
- Uses Encryptor to encrypt the same block of code using the new key



On-Demand Polymorphic Algorithm

Implementation

- Uses Decryptor to decrypt a block of code using an old key
- Executes the newly decrypted code
- Uses RDTSC (Read Time-Stamp Counter) to generate a new dword value
- Uses NewKeyGenerator to generate new key
- Uses Encryptor to encrypt the same block of code using the new key

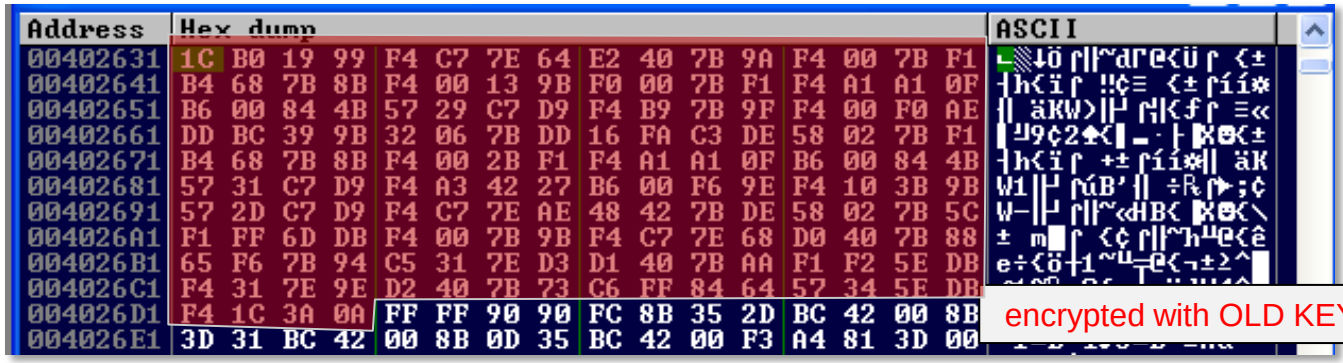


Encryptor

Features:

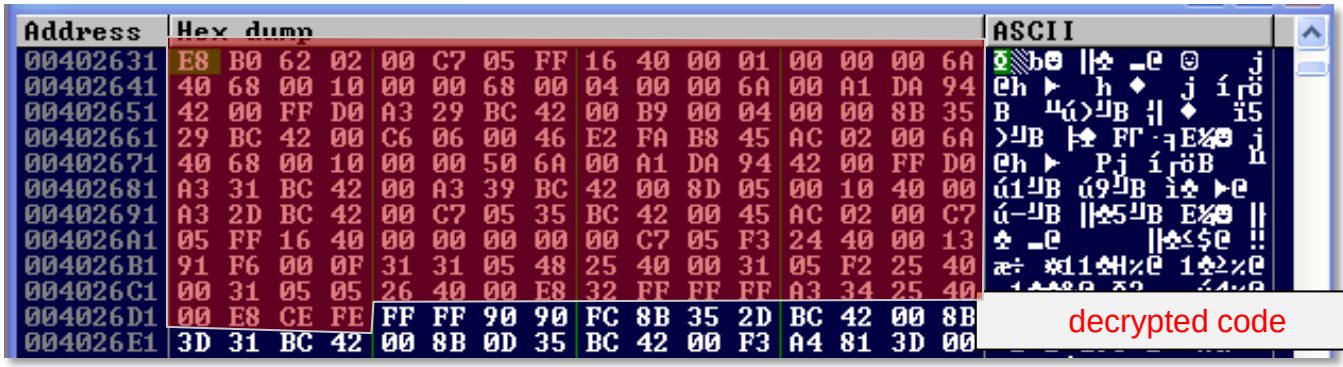
- Uses the same algorithm as the Decryptor
- Uses the new key to encrypt the same block of code

Sample On-demand Polymorphic Values



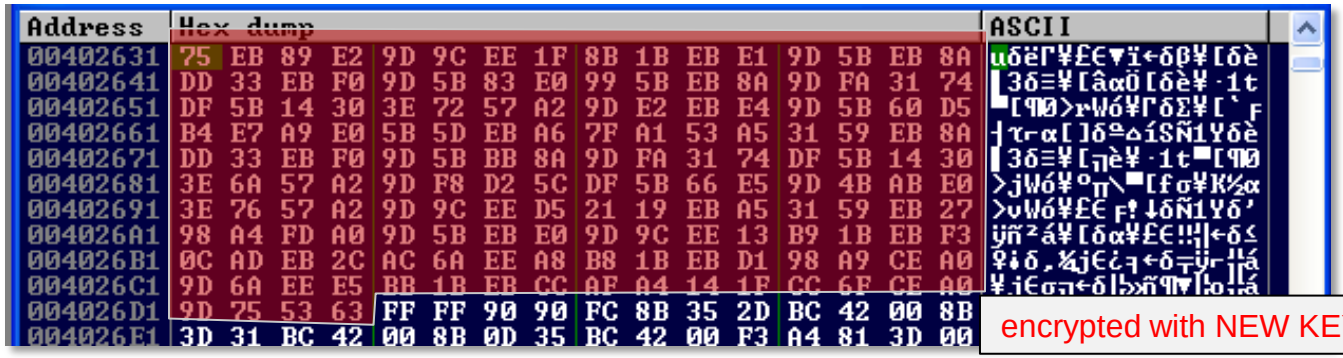
encrypted with OLD KEY

1C B0 19 99
F4 C7 7E 64
E2 40 7B 9A
F4 00 7B F1



decrypted code

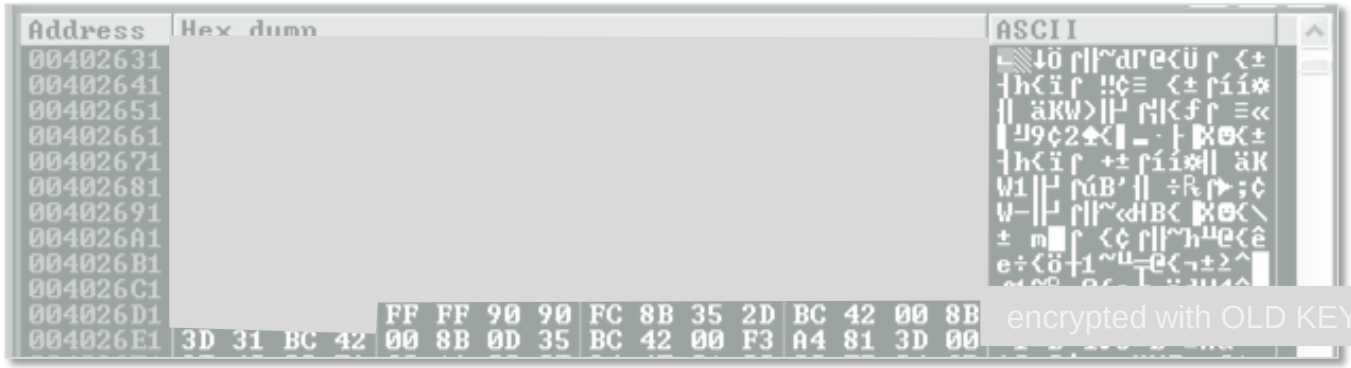
E8 B0 62 02
00 C7 05 FF
16 40 00 01
00 00 00 6A



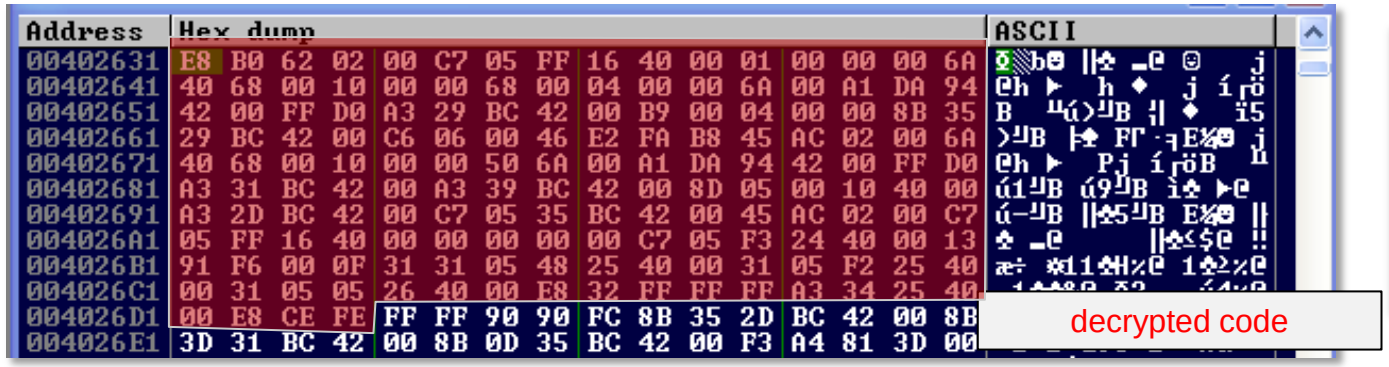
encrypted with NEW KEY

75 EB 89 E2
9D 9C EE 1F
8B 1B EB E1
9D 5B EB 8A

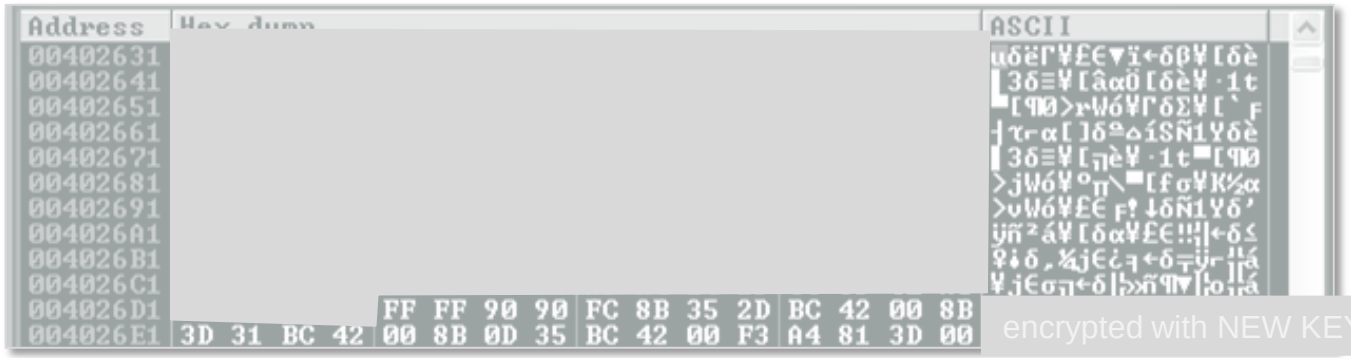
Detection




```
1C B0 19 99
F4 C7 7E 64
E2 40 7B 9A
F4 00 7B F1
```

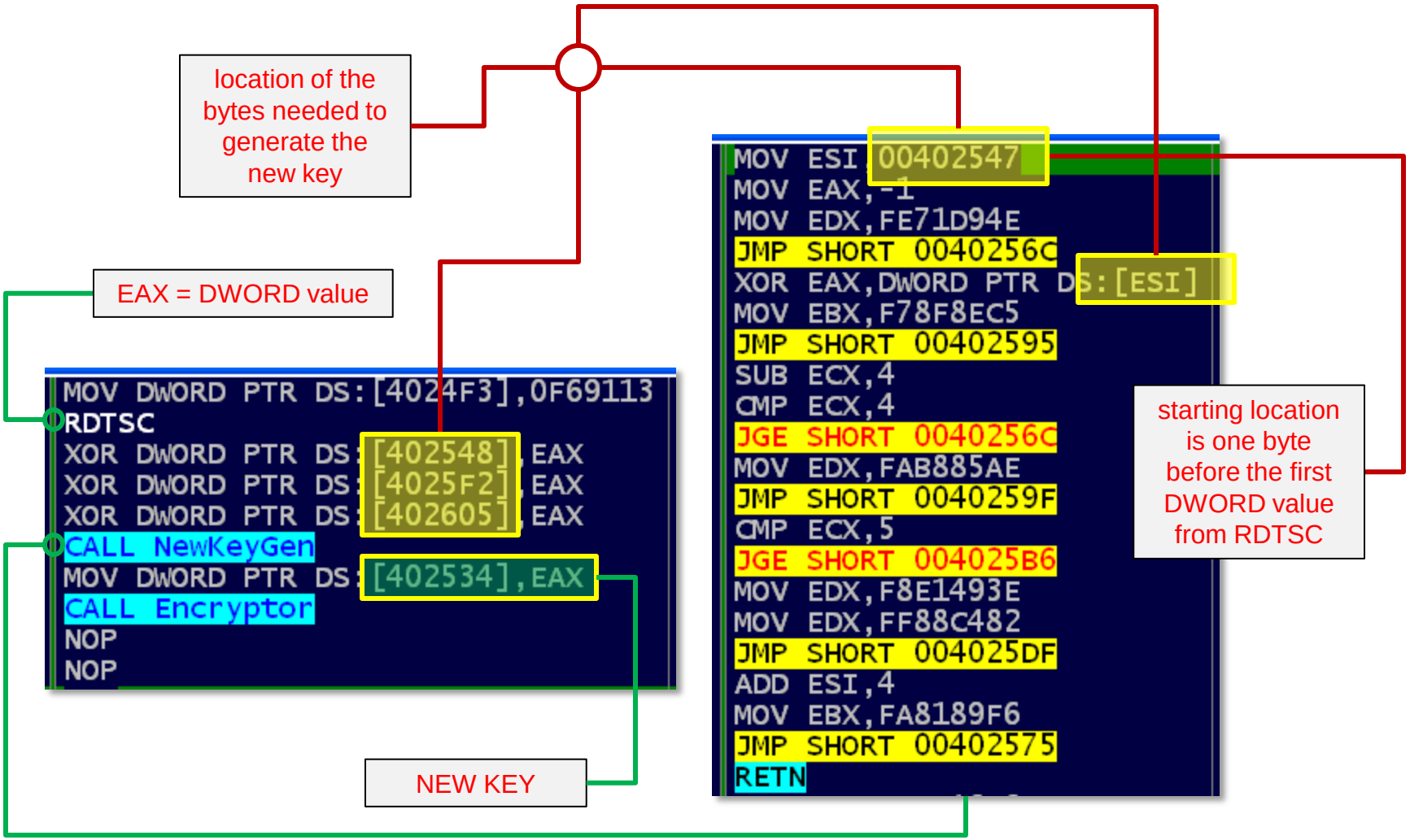



```
E8 B0 62 02
00 C7 05 FF
16 40 00 01
00 00 00 6A
```

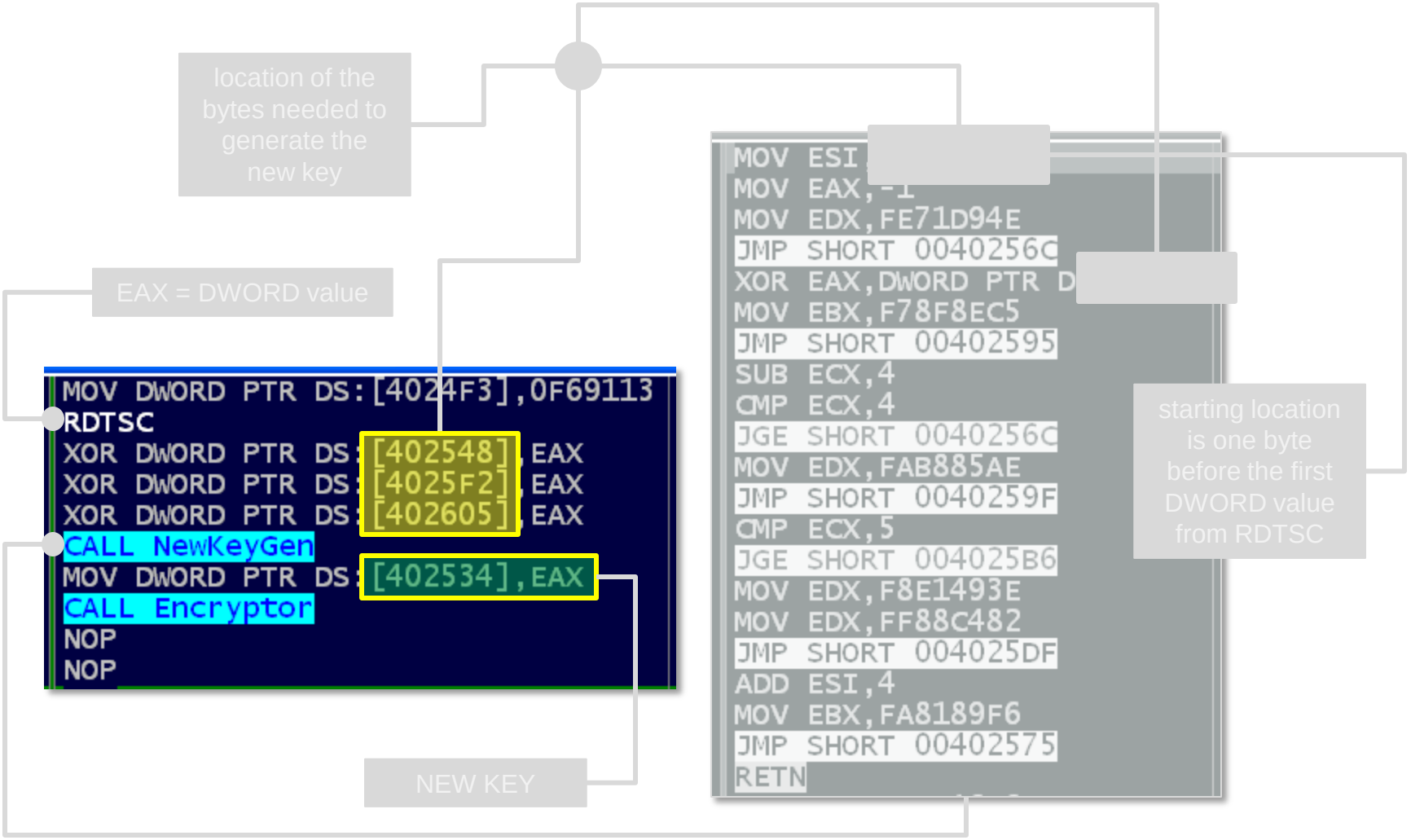



```
75 EB 89 E2
9D 9C EE 1F
8B 1B EB E1
9D 5B EB 8A
```

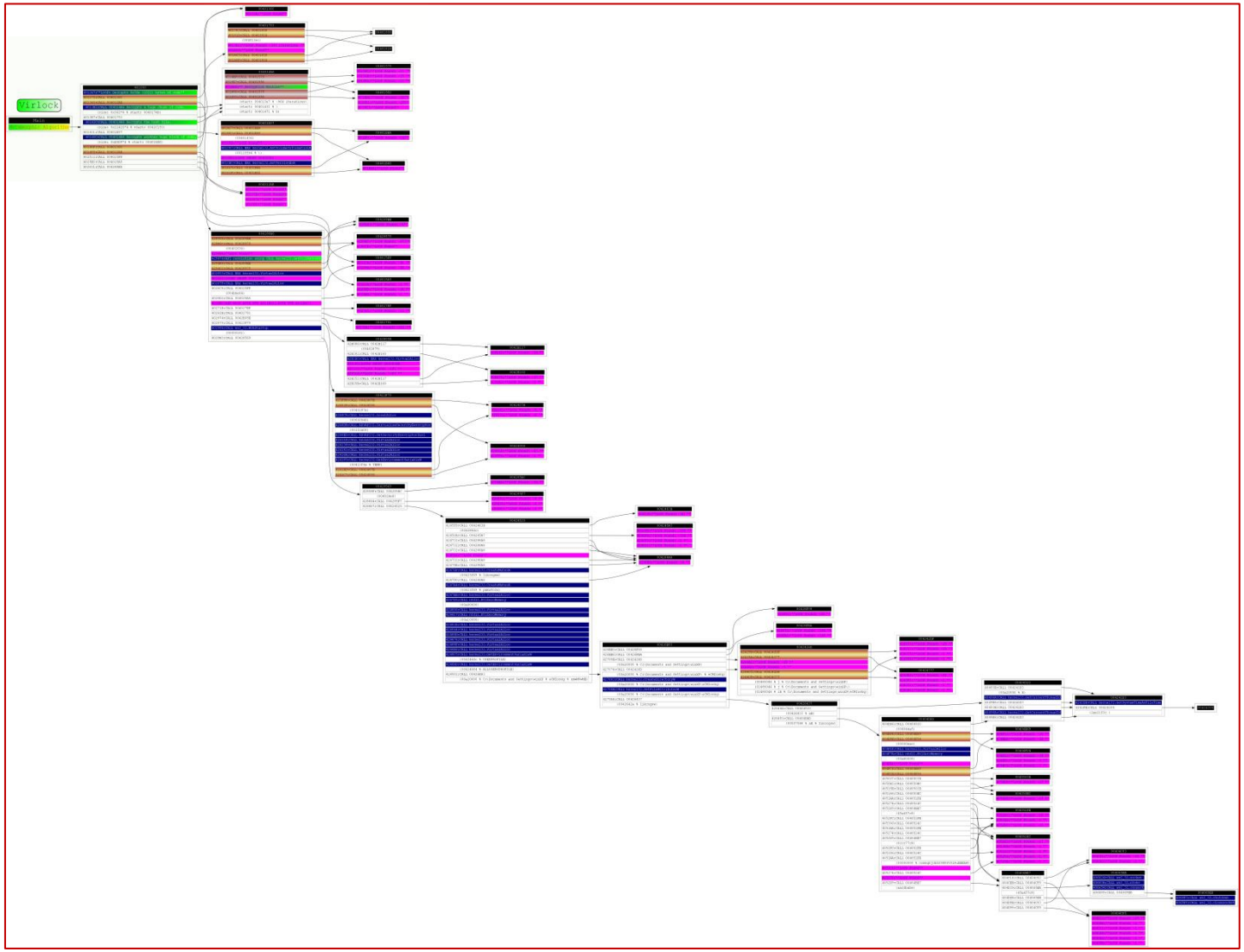
Detection


location of the bytes needed to generate the new key
EAX = DWORD value
MOV DWORD PTR DS:[4024F3],0F69113
RDTSC
XOR DWORD PTR DS:[402548],EAX
XOR DWORD PTR DS:[4025F2],EAX
XOR DWORD PTR DS:[402605],EAX
CALL NewKeyGen
MOV DWORD PTR DS:[402534],EAX
CALL Encryptor
NOP
NOP
NEW KEY
MOV ESI,00402547
MOV EAX,-1
MOV EDX,FE71D94E
JMP SHORT 0040256C
XOR EAX,DWORD PTR DS:[ESI]
MOV EBX,F78F8EC5
JMP SHORT 00402595
SUB ECX,4
CMP ECX,4
JGE SHORT 0040256C
MOV EDX,FAB885AE
JMP SHORT 0040259F
CMP ECX,5
JGE SHORT 004025B6
MOV EDX,F8E1493E
MOV EDX,FF88C482
JMP SHORT 004025DF
ADD ESI,4
MOV EBX,FA8189F6
JMP SHORT 00402575
RETN
starting location is one byte before the first DWORD value from RDTSC

Detection


location of the bytes needed to generate the new key
EAX = DWORD value
MOV DWORD PTR DS:[4024F3],0F69113
RDTSC
XOR DWORD PTR DS:[402548],EAX
XOR DWORD PTR DS:[4025F2],EAX
XOR DWORD PTR DS:[402605],EAX
CALL NewKeyGen
MOV DWORD PTR DS:[402534],EAX
CALL Encryptor
NOP
NOP
NEW KEY
MOV ESI
MOV EAX,-1
MOV EDX,FE71D94E
JMP SHORT 0040256C
XOR EAX,DWORD PTR D
MOV EBX,F78F8EC5
JMP SHORT 00402595
SUB ECX,4
CMP ECX,4
JGE SHORT 0040256C
MOV EDX,FAB885AE
JMP SHORT 0040259F
CMP ECX,5
JGE SHORT 004025B6
MOV EDX,F8E1493E
MOV EDX,FF88C482
JMP SHORT 004025DF
ADD ESI,4
MOV EBX,FA8189F6
JMP SHORT 00402575
RETN
starting location is one byte before the first DWORD value from RDTSC

Dynamic Routine Execution Map



Virlock As A Ransomware

FORTINET

Visible Signs of Infection

Canadian Security Intelligence Service Notice

Your computer was automatically blocked. Reason: Pirated software found on this computer.

Your computer is now blocked. 155 files have been temporarily blocked on your computer.
To regain computer access and restore files you are required to pay a fine of 250 CAD
Blocked files will be permanently removed from your computer if the fine is not paid.
The CSIS has two ways to pay a fine:
1.You can pay your fine online through BitCoin. BitCoin is available nationwide.
Click the tabs below to find the nearest vendor. Your computer will be unlocked after you make your payment.
2.You can come to your provincial courthouse and pay your fine at the Cashiers window.
Your computer will be unlocked within 4-5 working days.
To regain access transfer bitcoins to the following address (click to copy):
198tX7NmLg6o8qcTT2Uv9cSBVzN3oEozpv
After the payment is finalized enter Transfer ID below.

Online fine payments are processed by Royal Bank of Canada.

Amount: Transfer ID:

BTC 0.588 | PAY FINE

Internet connection is unavailable. Click Network Connections and connect to the Internet

If the fine is not paid, 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.

Payment | BitCoin Information | BitCoin Exchanges | BitCoin ATMs | Internet Browser | Notepad | Network Connections

CSIS.gc.ca

Canadian Security Intelligence Service Notice

Canada

What is BitCoin

Bitcoin is a software-based online payment system.

How to pay a fine?
1.Purchase bitcoins from an exchange or an ATM.
2.Transfer to the address (click to copy): 198tX7NmLq6o8qcTT2Uv9cSBVzN3oEozpv
To locate the nearest exchange or an ATM open the corresponding tab below.

If you purchased a paper wallet or you want to register a new bitcoin wallet follow the instructions below: Open Internet Browser. Go to the address: blockchain.info/wallet and click 'Start A New Wallet'.Enter your e-mail address(optional) and password. Make sure your password is secure. Save your password safely, preferably offline(click Notepad). Follow the steps prompted on the website and pay close attention to the security recommendations. Login to your Bitcoin wallet blockchain.info/wallet/login Click on Import / Export. Enter the paper wallet's private key by typing it manually (case sensitive) and click on 'Add Private Key'. Click 'Sweep Key'. Make sure your Bitcoin balance reflects the new deposit.

Making BitCoin payment: click 'Send Money' on the menu, enter the bitcoin address, click 'Send Payment'.

Learn more about BitCoin

howtobuybitcoins.info	bitcoin.org
en.bitcoin.it/wiki/Introduction	en.bitcoin.it/wiki/Getting_started
en.bitcoin.it/wiki/Buying_bitcoins	en.bitcoin.it/wiki/Main_Page

Canadian Security Intelligence Service Notice

View: Canadian Exchanges International Exchanges

CaVirtex
https://www.cavirtex.com/home
(888)812-2525

Bitcoiniacs
bitcoiniacs.com
Waves Coffee, #100 - 900 Howe St.
Vancouver
BC V6Z 2M4 Canada
1 (877) 814-7460
contact@bitcoiniacs.com

QuadrigaCX
quadrigacx.com
Phone: 1-604-757-9660
Email: contact@quadrigacx.com

QuickBT
quickbt.com/ca/
1-888-QUICK-55 (784-2555)

Aaron Buys Gold Ltd
aaronbuysgold.com
Canada Wide 1.866.549.7747
Edmonton 780.628.6895
947 Ordze Road Sherwood Park

Vault of Satoshi
vaultofsatoshi.com
(855) 457-0101
(519) 757-0101
340 Henry Street, Unit #16
Brantford, Ontario
Canada, N3S 7V9

Coin Clutch
coinclutch.com
Email: support@coinclutch.com
Toll-Free: 1-800-704-0012

Tradebitcoin.com

Canadian Security Intelligence Service Notice

BTM Locators

Edmonton (4)
Fort Mcmurray (1)
Montreal (7)
Vancouver (3)
Ottawa (2)
Quebec (3)
Sherwood Park (1)
Whistler (1)
Winnipeg (4)
Alberta (1)
Saskatoon (2)
Moncton (1)
North Bay (1)
Toronto (2)
Victoria (1)
Halifax (1)

Roboco roboco.in

BitCoin ATM bitcoinatm.com

CoinDesk coindesk.com/bitcoin-atm-map/

BitCoin ATM Map bitcoinatmmap.com

Canadian Security Intelligence Service Notice

To save notepad contents click File->Save.
The file will be saved in My Documents folder as 'myfile'. You can access it later.

Payment | BitCoin Information | BitCoin Exchanges | BitCoin ATMs | Internet Browser | Notepad | Network Connections

CSIS.gc.ca

Eradication

FORTINET

Eradication

- Manually create solution to clean the infected files
- Download reliable standalone solution to remove the malware from the system
- Always make sure that your antivirus and security apps are updated

What if your system is already locked?

Steps:

- Reboot the system on safe mode
- Remove the malware entry on the startup registry
- Then go back to eradication stage

Demo – Unlocking Virlock

Wrap Up

- For reversing:
  - ✓ Set a breakpoint at the end of metamorphic algorithm
  - ✓ Copy the decrypted code from memory
- For detection:
  - ✓ Get patterns from the decrypted code
- For cleaning:
  - ✓ Remove the entries from the registry keys
  - ✓ Extract the host file

Mulțumesc!

FORTINET


FORTINET