

## GNISREVER A POLYMORPHIC FILE-INFECTING RANSOMWARE



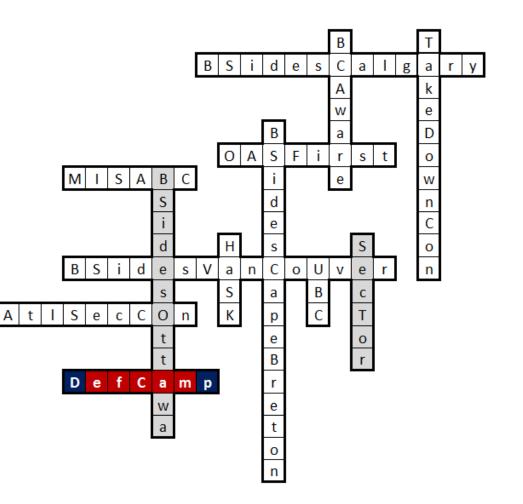
November 10-11, 2016 Raul Alvarez

© Copyright Fortinet Inc. All rights reserved.

#### About Me

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





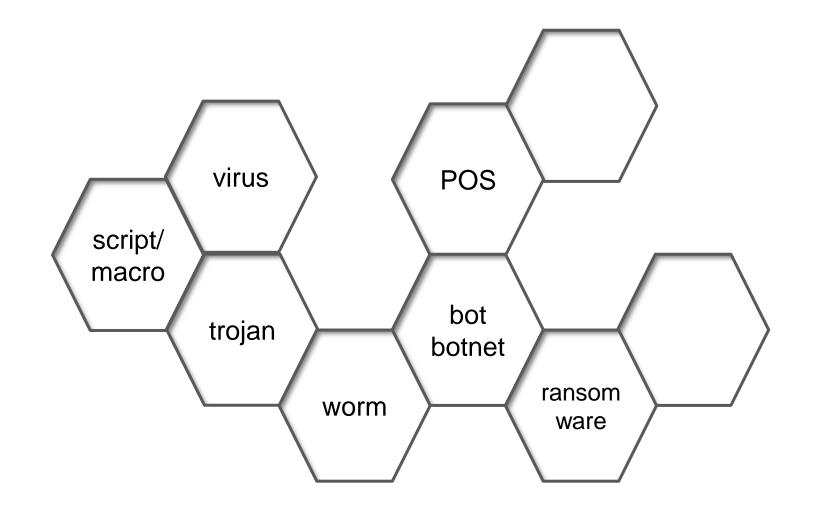


# **Malware Categories**





#### Malware Honeycomb



#### Virlock

POS virus script/ macro bot trojan botnet ransom worm ware

# Agenda





### 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





#### 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



#### A ransomware

A file infector

Uses on-demand polymorphic algorithm

Uses metamorphic algorithm

Locks your screen







#### 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 Online fine payments are processed by Royal Bank of Canada. After the payment is finalized enter Transfer ID below. Amount: Transfer ID: BTC 0.588 PAY FINE 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





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): 198tX7NmLg6o8qcTT2Uv9cSBVzN3oEozpv 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

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





View: Canadian Exchanges <u>International Exchanges</u>						
CaVirtex	Aaron Buys Gold Ltd					
https://www.cavirtex.com/home	aaronbuysgold.com					
(888)812-2525	Canada Wide 1.866.549.7747					
	Edmonton 780.628.6895					
Bitcoiniacs	947 Ordze Road Sherwood Park					
bitcoiniacs.com						
Waves Coffee, #100 - 900 Howe St. Vancouver	vault of Satoshi vaultofsatoshi.com					
BC V6Z 2M4 Canada	(855) 457-0101					
1 (877) 814-7460	(519) 757-0101					
contact@bitcoiniacs.com	340 Henry Street, Unit #16					
000000000000000000000000000000000000000	Brantford, Ontario					
QuadrigaCX	Canada, N3S 7V9					
quadrigacx.com						
Phone: 1-604-757-9660	Coin Clutch					
Email: contact@quadrigacx.com	coinclutch.com					
	Email: support@coinclutch.com					
QuickBT	Toll-Free: 1-800-704-0012					
quickbt.com/ca/						
1-888-QUICK-55 (784-2555) Tradebitcoin.com						
Payment BitCoin Information Bit	tCoin Exchanges BitCoin ATMs Internet Browser Notepad Network Connections					





BTM Locato	ors	Roboco ro	boco.in				
<u>Edmonton (</u> Fort Mcmur		BitCoin A	TM bitcoinatm.com				
Montreal (	(7)	CoinDesk	coindesk.com/bitcoi	.n-atm-map/			
<u>Vancouver</u> <u>Ottawa (2</u> )		BitCoin A	TM Map bitcoinatmma	ap.com			
<u>Quebec (3)</u> Sherwood F							
<u>Whistler (</u>	(1)						
<u>Winnipeg (</u> Alberta (1	·						
Saskatoon	(2)						
<u>Moncton (1</u> North Bay							
Toronto (2							
<u>Victoria (</u> <u>Halifax (</u> 1							
<u>Payment</u>	BitCoin	Information	<u>BitCoin Exchanges</u>	BitCoin ATMs	Internet Browser	<u>Notepad</u>	<u>Network Connections</u>





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

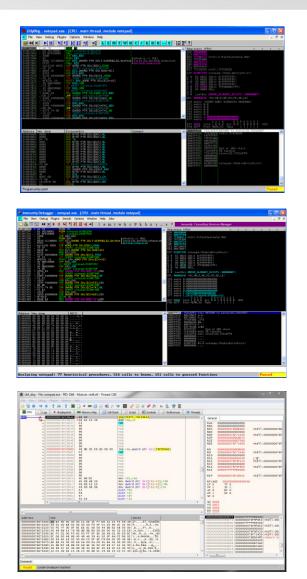
Payment BitCoin Information BitCoin Exchanges BitCoin ATMs Internet Browser Notepad Network Connections

# Just kidding!

FERTINET. FAST. SECURE. GLOBAL.

Confidential 19

#### **Debugging Tools**



#### ollydbg <u>http://www.ollydbg.de/</u>

immunity debugger http://www.immunityinc.com/p roducts/debugger/

> x64dbg http://x64dbg.com/



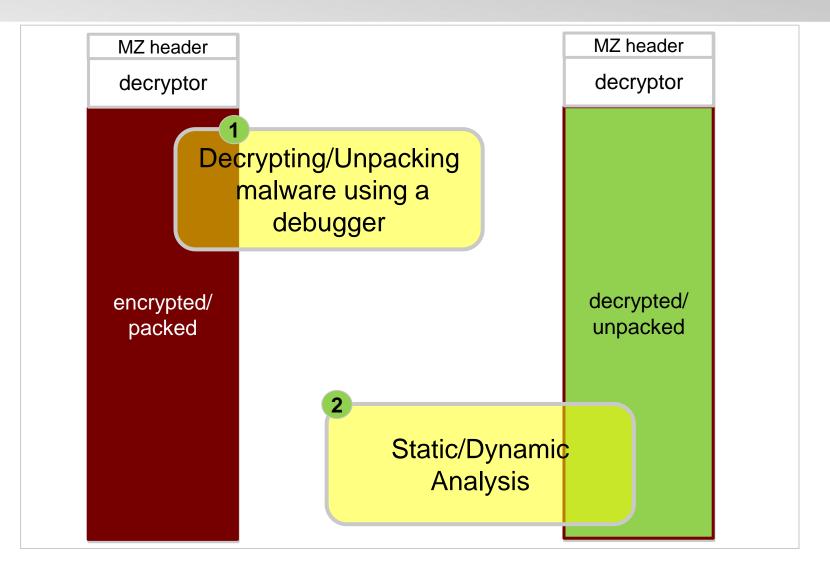
FAST. SECURE. GLOBAL.

# Virlock As A Common Malware





### **Common Reversing**



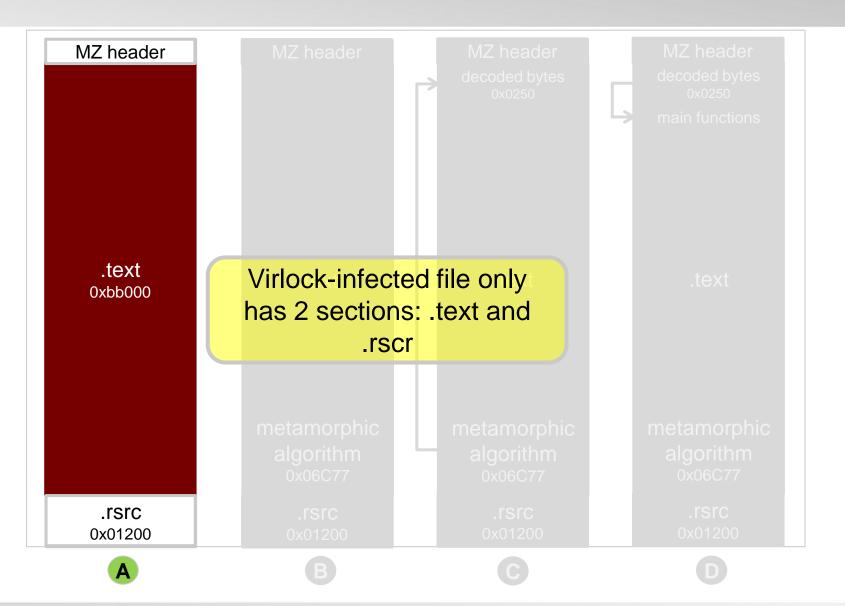


FAST. SECURE. GLOBAL.

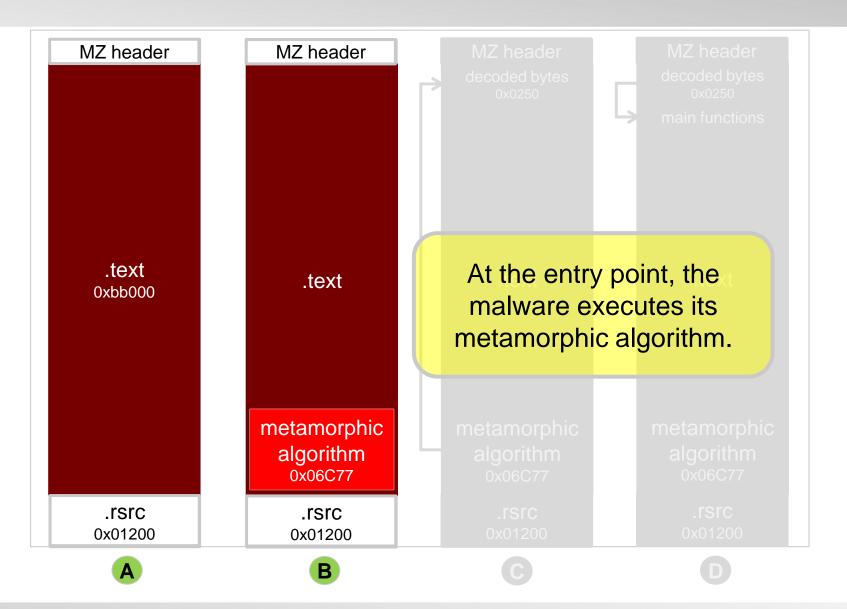
Confidential 22



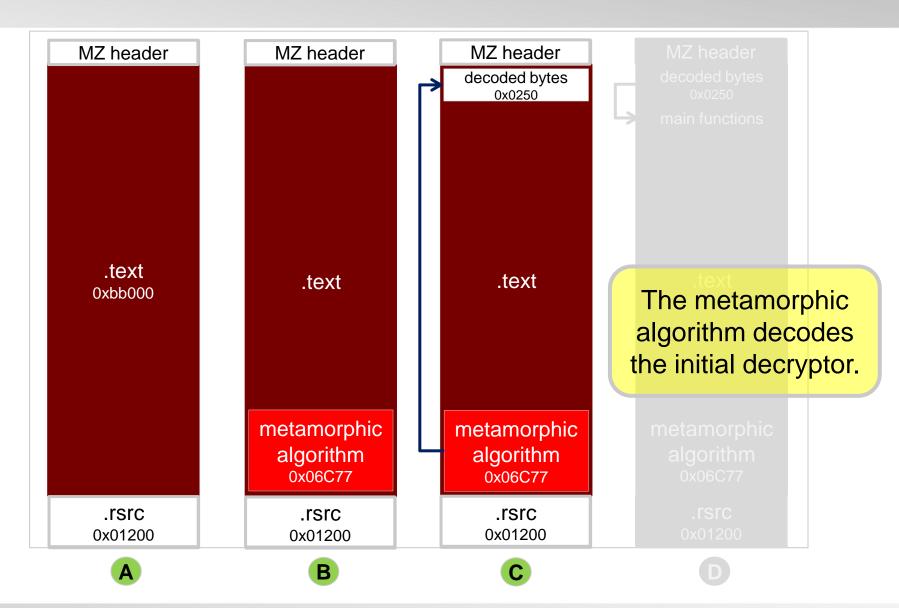




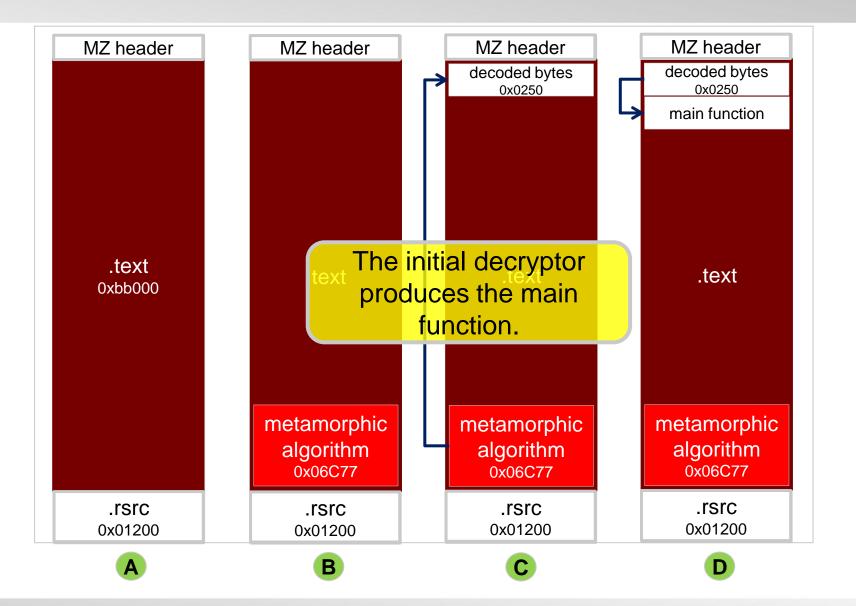




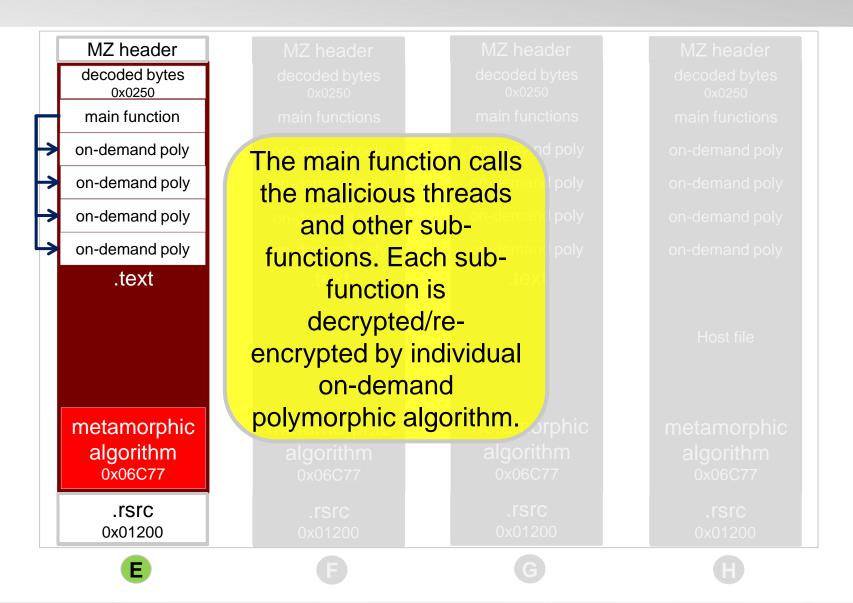




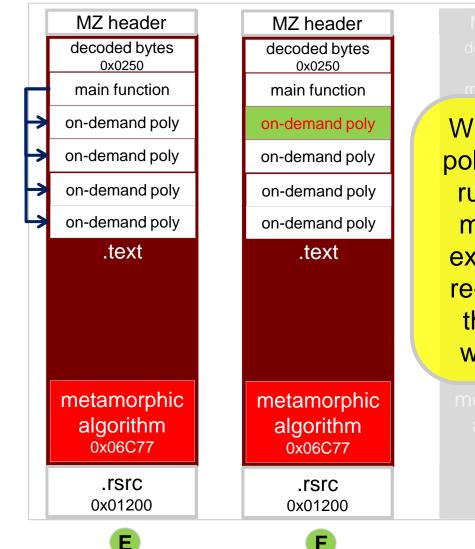


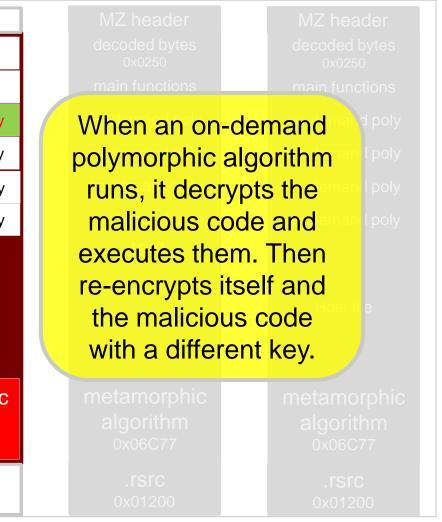


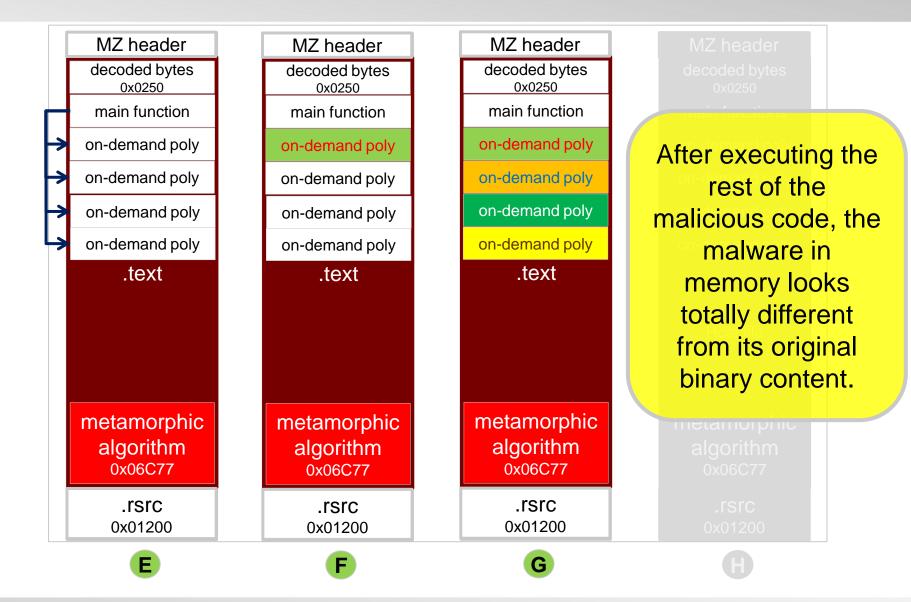






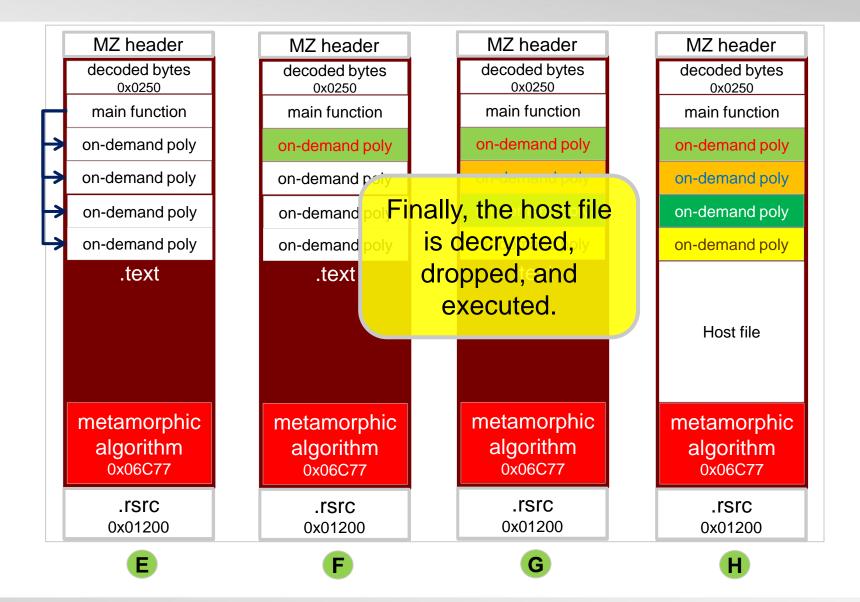












Metamorphic Algorithm





### Basics: Putting a value(0) in a register(EAX)

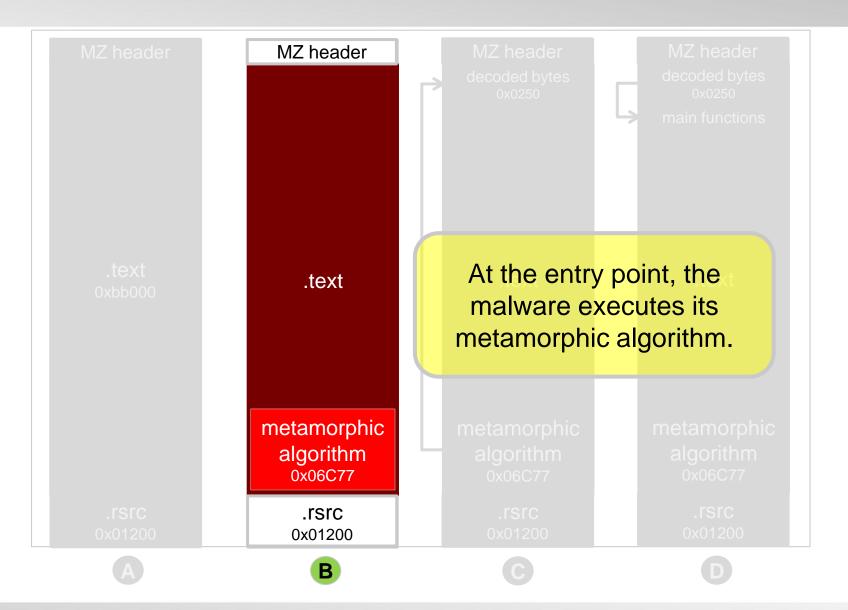
MOV EAX,0	EAX register gets 0 directly
XOR EAX,EAX	XORing the same register by itself also generates a zero value placed into a given register
SUB EAX,EAX	SUBtracting any register by itself also generates the same result.
MOV EAX, 0x10 ADD EAX, 0x10 SUB EAX, 0x20	EAX also gets 0

### **Metamorphic Algorithm**

### **Detection Limitation**

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







#### Metamorphic Algorithm (sample 1)

BF A9EB0000 MOV EDI, OEBA9 MOV ECX,6397A ADD EDI,708F6 B9 7A390600 81C7 F6080700 SUB ECX,0D4B34 81E9 344B0D00 81EF E3780000 SUB EDI,78E3 81E9 6EC30D00 SUB ECX, ODC36E The size of the 81EF 9C8D0B00 SUB EDI,088D90 81E9 4AA10A00 SUB ECX,0AA14A metamorphic code varies 81C7 73180300 ADD EDI,31873 81C1 83A00E00 ADD ECX,0EA083 **Entry Point** per infected file. 81C7 0B880600 ADD EDI,6880B SUB ECX, OCB440 81E9 40B40C00 81C7 EF340900 ADD EDI,934EF 81C1 5FBB0D00 ADD ECX, ODBB5F 81EF 8AD30700 SUB EDI,7D38A Approximately 28kb of 81E9 D24E0600 SUB ECX,64ED2 81EF CFB90D00 SUB EDI, ODB9CF code constitutes the 81E9 CD3D0B00 SUB ECX,0B3DCD 81EF 52C10A00 SUB EDI, OAC152 metamorphic algorithm 81E9 1E040D00 SUB ECX,0D041E 81EF 89360000 SUB EDI,3689 that generates the rest of 81C1 0B840600 ADD ECX,6840B ~ 28 kilobytes 81C7 40370B00 ADD EDI,0B3740 the malicious code, 81C1 C3AB0700 ADD ECX, 7ABC3 81EF 3FFD0C00 SUB EDI, OCFD3F including the polymorphic 81C1 05730100 ADD ECX,17305 81C7 83AD0700 ADD EDI,7AD83 algorithm. SUB ECX,0A9A14 81E9 149A0A00 81EF 85700C00 SUB EDI.0C7085 81C1 8A0D0B00 ADD ECX,0B0D8A 81EF B4D00A00 SUB EDI.OADOB4 81C2 5FF83800 |ADD EDX,38F85F 81EB 49CF436F SUB EBX, 6F43CF49 MOV DWORD PTR DS:[EDX],EBX 891A BA 55460B00 MOV EDX,084655 Call to the decrypted 81C2 FA830A00 ADD EDX, 0A83FA 81C2 4ADF0700 ADD EDX,7DF4A bytes at the start of the 81EA 9E190600 SUB EDX,6199E 81C2 29FC0A00 ADD EDX, 0AFC29 .text section. 81EA 55E00000 SUB EDX,0E055 81C2 31641E00 ADD EDX, 1E6431 FFD2

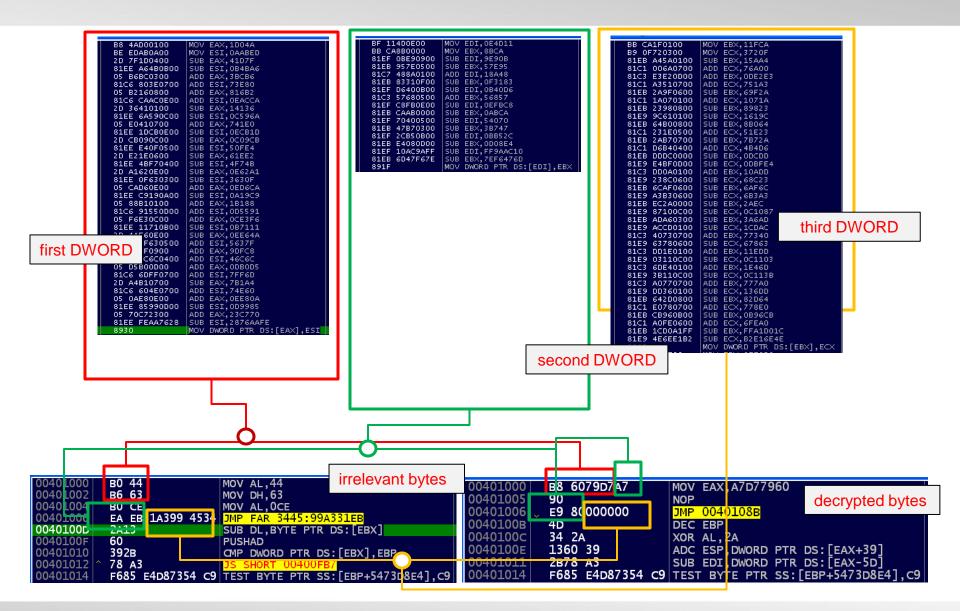


## Metamorphic Algorithm (sample 1)

BF A9EB0000 B3 7A390600         MOV EDI,0EBA9 MOV ECX,6397A A00 EDI,708F6 S1E9 344B0000 SUB ECX,004B34 S1E9 6C30000         SUB ECX,004B34 S1E9 6C30000           S1E9 4A410A00         SUB ECX,004B34 S1E9 94040000         SUB ECX,00436E S1E9 4040000         SUB EDI,70850 S1E9 4040000           S1C7 73180300         ADD EDI,31873 S1C1 83A00E00         ADD EDI,31873 S1C1 83A00E00         ADD EDI,31873 S1C1 83A00E00           S1C7 0580600         ADD ECX,00B85F S1E9 4044000         SUB ECX,00E85F S1E9 50000         SUB ECX,00B85F S1E9 52010A00           S1E9 1240600         SUB ECX,0041E S1E9 1240600         SUB ECX,00B85F S1E9 52010A00         SUB ECX,00B85F S1E9 52010A00           S1E9 1240600         SUB ECX,00A152 S1E9 1240600         SUB ECX,00B85F S1E9 1240000         SUB ECX,00B85F S1E9 1240000           S1E9 1240600         SUB ECX,00B85F S1E9 1240000         SUB ECX,00A11E S1E9 1240000         SUB ECX,0041E S1E9 1240000           S1E9 1240000         SUB ECX,0041E S1E9 1240000         SUB ECX,0041E S1E9 1240000         SUB ECX,0783 S121 1340000           S1E1 3120000         ADD ECX,74B23 S121 1340000         SUB ED1,0C7085 S121 1340000         SUB ECX,02084           S1E1 9100A0200         SUB ED1,0C7085 S121 5400000         SUB ECX,04904         SUB ECX,04904           S1E1 9100A0200         SUB ED1,0C7085 S121 5400000         SUB ECX,04904         SUB ECX,04904           S1E1 9100A0200         SUB ECX,04904 </th <th>B8         94E00200         MOV         EAX, 2E094           B8         E03F0800         MOV         EAX, 7BE03           B1E         G23F0800         MOV         EAX, 7BE03           B1E         G28BF020         SUB         EAX, 0CBF69           S1C3         G45A0000         SUB         EAX, 0CBF69           S1C3         G45A0000         SUB         EAX, 0C0729           S1C3         G44A0300         SUB         EAX, 0E8469           S1C3         G45A0000         SUB         EAX, 0E8469           S1C3         G45A0000         SUB         EAX, 0E8469           S1C3         G3870400         SUB         EAX, 0E8703           S1C3         G3870400         SUB         EAX, 0E8703           S1C3         G3730000         ADD         EAX, 0B704           S1C3         G3730000         ADD         EAX, 0B704           S1C3         G3730000         ADD         EAX, 0B704           S1C3         G4730000         <t< th=""><th>D SUB ESI,70F08 SUB ESI,8C43A SUB ESI,9E448 ADD ESI,0EE0B ADD ESI,0F0001 SUB EDX,10099 ADD ESI,08CA06 SUB EDX,79C6C ADD ESI,08CA06 SUB EDX,79C6C ADD ESI,083A07 SUB ESI,0853A0 ADD ESI,3771 SUB ESI,771 SUB ESI,7574 SUB ESI,7529 ADD ESI,7371 SUB ESI,7574 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 SUB ESI,0751F SUB ESI,19751F SUB ESI,19751F SUB ESI,19751F SUB ESI,19751F</th></t<></th>	B8         94E00200         MOV         EAX, 2E094           B8         E03F0800         MOV         EAX, 7BE03           B1E         G23F0800         MOV         EAX, 7BE03           B1E         G28BF020         SUB         EAX, 0CBF69           S1C3         G45A0000         SUB         EAX, 0CBF69           S1C3         G45A0000         SUB         EAX, 0C0729           S1C3         G44A0300         SUB         EAX, 0E8469           S1C3         G45A0000         SUB         EAX, 0E8469           S1C3         G45A0000         SUB         EAX, 0E8469           S1C3         G3870400         SUB         EAX, 0E8703           S1C3         G3870400         SUB         EAX, 0E8703           S1C3         G3730000         ADD         EAX, 0B704           S1C3         G3730000         ADD         EAX, 0B704           S1C3         G3730000         ADD         EAX, 0B704           S1C3         G4730000 <t< th=""><th>D SUB ESI,70F08 SUB ESI,8C43A SUB ESI,9E448 ADD ESI,0EE0B ADD ESI,0F0001 SUB EDX,10099 ADD ESI,08CA06 SUB EDX,79C6C ADD ESI,08CA06 SUB EDX,79C6C ADD ESI,083A07 SUB ESI,0853A0 ADD ESI,3771 SUB ESI,771 SUB ESI,7574 SUB ESI,7529 ADD ESI,7371 SUB ESI,7574 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 SUB ESI,0751F SUB ESI,19751F SUB ESI,19751F SUB ESI,19751F SUB ESI,19751F</th></t<>	D SUB ESI,70F08 SUB ESI,8C43A SUB ESI,9E448 ADD ESI,0EE0B ADD ESI,0F0001 SUB EDX,10099 ADD ESI,08CA06 SUB EDX,79C6C ADD ESI,08CA06 SUB EDX,79C6C ADD ESI,083A07 SUB ESI,0853A0 ADD ESI,3771 SUB ESI,771 SUB ESI,7574 SUB ESI,7529 ADD ESI,7371 SUB ESI,7574 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 ADD ESI,7371 SUB ESI,7529 SUB ESI,0751F SUB ESI,19751F SUB ESI,19751F SUB ESI,19751F SUB ESI,19751F
00401002         9C         POSHED           00401003         43         INC EBX           00401004         27         DAA           00401005         C5A495         ADE9925A           0040100C         DDD1         LDS ESP, FWORD           0040100C         27         JA SHORT 00401           0040100C         27         INC EX	00401005 00401006 E9 80 000401008 98 CWE 0040100C 0040100C 0040100C 0040100C 0040100C 0040100C 0040100C 005 005 005 005 005 005 005	decrypted bytes



## Metamorphic Algorithm (sample 2)



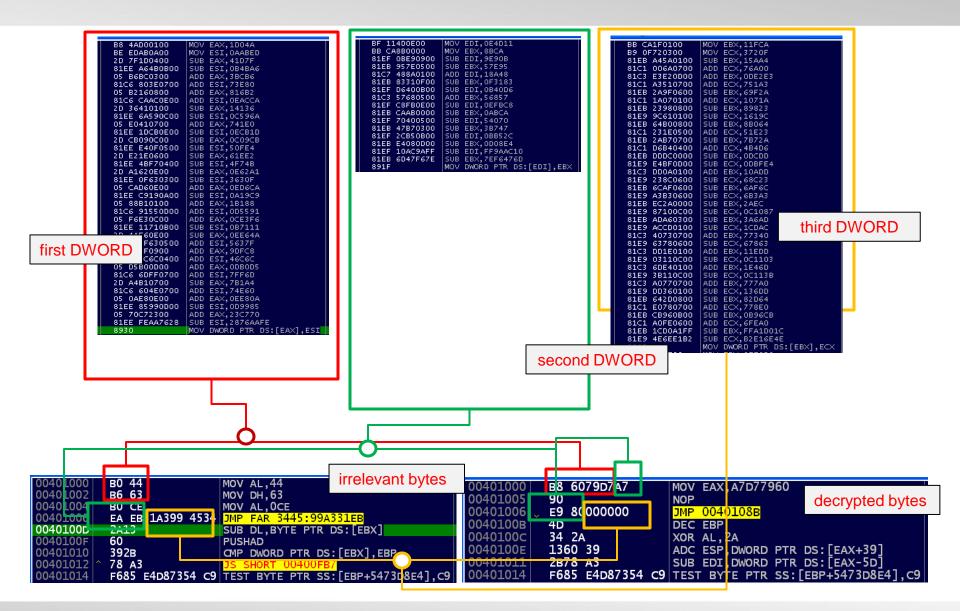


## Metamorphic Algorithm (sample 1)

BF A9EB0000 89 7A390600         MOV EDI,0EBA9 MOV ECX,6397A ADD EDI,708F6 81E9 34440000         SUB EDI,708F6 81E9 34440000           81E7 6250000         SUB EDI,70876           81E7 9250000         SUB EDI,70876           81E9 94A10A00         SUB EDI,70876           81E9 94A10A00         SUB EDI,088090           81E9 94A10A00         SUB EDI,088090           81E9 940100         SUB ECX,00414A           81C7 73180300         ADD EDI,31873           81C1 8780000         SUB ECX,00E85F           81E9 9404000         SUB ECX,00E85F           81E9 0240600         SUB ECX,004140           81C7 73180700         ADD ECX,00885F           81E9 0240600         SUB ECX,00412           81E9 0240600         SUB ECX,00412           81E9 0240600         SUB ECX,000412           81E9 1404000         SUB ECX,00412           81E9 1404000         SUB ECX,00412           81E9 1404000         SUB ECX,000412           81E9 1404000         SUB ECX,00418           81C7 40370800         ADD ECX,74803           81C7 40370800         ADD ECX,74803           81C7 40370800         ADD ECX,00414           81E9 14004000         SUB ECX,004314           9008000         SUB ECX,004314	B8         94E00200         MOV         EAX, 2E094           B8         E03F0800         MOV         EAX, 78E03           S1EE         62880100         SUE         EAX, 78E03           S1EE         62880100         SUE         EAX, 78E03           S1E         645A0000         ADD         EAX, 7763           S1E3         06470000         SUE         EAX, 000729           S1C3         06440300         ADD         EAX, 76504           S1C3         06440300         ADD         EAX, 76504           S1C3         06440300         ADD         EAX, 76504           S1C3         9670000         SUE         EAX, 000729           S1C3         9670000         SUE         EAX, 000729           S1C3         967000         SUE         EAX, 000729           S1C3         967000         SUE         EAX, 00070           S1C3         967000         ADD         EAX, 00704           S1C3         9770000         SUE         EAX, 000704           S1C3         9770000         ADD         EAX, 000704           S1C3         9770000         ADD         EAX, 000704           S1C3         973700000         ADD	BA         BAC0800         MOV         EDX, 8AC3A           BEE         BIEA         3AC00800         SUB         ESX, 70F08           BIEA         3AC00800         SUB         ESX, 70F08           BIEA         3AC40800         SUB         ESX, 70F08           BIEA         3AC40800         SUB         ESX, 70F08           BIEA         3AC40800         SUB         ESX, 70F08           BIEA         4830900         SUB         ESX, 70F08           BIEA         4830900         SUB         ESX, 70F08           BIC6         DBEE0000         ADD         ESX, 70F08           BIC6         DBEE0000         ADD         ESX, 70F08           BIC6         DBEC0000         ADD         ESX, 70F08           BIC6         DBC0000         SUB         EXX, 70F08           BIC6         DBC000         SUB         EXX, 70F08           BIC2         SAS0000         SUB         EXX, 75029           BIC4         SP31000
00401002         9C         POSHED           00401003         43         INC EBX           00401004         27         DAA           00401005         C5A495         ADE9925A           0040100C         DDD1         LDS ESP, FWORD           0040100C         27         JA SHORT 00401           0040100C         27         INC EX	00401005       90         00401006       E9         00401006       98         00401000       00401000         003F       00401000         00401000       22:2         00401010       22:2         005:[EBX_47],ESI       00401012	2F JA SHORT 0040103F



## Metamorphic Algorithm (sample 2)





## Metamorphic Algorithm (comparison)

first DWORD

BF A9EB0000 MOV EDI	I,OEBA9	B8 4AD0	0100 MON	/ EAX,1D04A	
B9 7A390600 MOV EC>	X,6397A	BE EDAB		/ ESI, OAABED	
	I,708F6	2D 7F1D		B EAX,41D7F	
81E9 344B0D00 SUB EC>	X,0D4B34	81EE A6		8 ESI,0848A6	
81EF E3780000 SUB ED1		05 8680		) EAX,3BCB6	
	X,ODC36E	81C6 80			
	I,0B8D9C			) ESI,73E80	
	X,0AA14A	05 B216		) EAX,816B2	
	I,31873	81C6 CA		) ESI,OEACCA	
	X,0EA083	2D 3641		B EAX,14136	
	I,6880B	81EE 6A		8 ESI,0C596A	·
	X,0CB440	05 E041		) EAX,741E0	
	1,934EF	81EE 1D		BESI,OECB1D	
		2D CB09		EAX,0C09CB	
	X,0DBB5F	81EE E4		BESI,50FE4	
	I,7D38A	2D E21E		8 EAX,61EE2	
	X,64ED2	81EE 4B		B ESI,4F74B	
	I,ODB9CF	2D A162		3 EAX,0E62A1	
	X, OB3DCD	81EE OF		8 ESI,3630F	
	I,0AC152	05 CAD6		) EAX,OED6CA	
	X,0D041E	81EE C9	190A00  SUE	8 ESI,0A19C9	
81EF 89360000 SUB ED		05 8881		) EAX,1B188	
	X,6840B	8106 91	550D00  AD0	) ESI,0D5591	
	I,0B3740	05 F6E3		) EAX,OCE3F6	
	X,7ABC3	81EE 11	710800  SUB	3 ESI,087111	
	I,OCFD3F	2D 4AE6	0E00  SUB	B EAX, OEE64A	
	×,17305	81C6 7F	630500 ADD	) ESI,5637F	
	I,7AD83	05 C8DF	0900 ADD	) EAX,9DFC8	
	X,0A9A14	8106 60	6C0400   ADD	) ESI,46C6C	
	I,0C7085	05 D5B0	ODOO ADD	) EAX,ODBOD5	
	×,0B0D8A	8106 60	FF0700 ADD	ESI.7FF6D	
	I,OADOB4	2D-A481	200 / EU	EAX.78184	
	×,2BAOD		4E 1707	EAX]	
	I,OEFF25	OS VAEN		-AAL	
	X,0E400A	81EE 85	990000 99000	EST.009955	, — — –
81C7 501D0F00 ADD ED1	I,OF1D50	05 7007	2300 ADD	EAX,23C770	
81E9 8D380400 SUB EC		81EE FE	AA7628 SUE	8 ESI,2876AA	
		8930	MO\		DS:[EAX],ESI
MOV [E					
810FV048€COV  S_0-e0.					
81C1 8ABB0800 ADD ECX	X,8BB8A		Sa	mple 2	
	I,FFA4B8FC		Ja		
81E9 568EBF5A SUB EC	X,5ABF8E56				
890F MOV DW0	OŔD PTR DS:[EDI],ECX				
Sample	1				
Campie					



## Metamorphic Algorithm (comparison)

second DWORD

B8 94E00200	MOV	EAX,2E094	
BB E03F0B00	MOV.	EBX,0B3FE0	
05 03BE0700	ADD.		
81EB 62B80100	SUB	EBX,1B862	
2D 69BF0C00	SUB	EAX. OCBF69	
81C3 645A0000	ADD	EBX,5A64	
2D 08770000	SUB	EAX,7708	
81EB 14080300	SUB	EBX,30814	
20 29070000	SUB	EAX,0D0729	
81C3 0D440300	ADD	EBX.3440D	
05 E9840E00	ADD	EAX, OE84E9	
81EB 0A300F00	SUB	EBX, OF300A	
2D D4650700	SUB	EAX,765D4	
81C3 693F0E00	ADD	EBX,0E3F69	
2D D3870400	SUB	EAX, 487D3	
81C3 B4A00E00	ADD	EBX, OEAOB4	
05 0AB70B00	ADD	EAX, OBB70A	
81C3 92FD0D00	ADD	EBX, ODFD92	
05 A5FA0500	ADD	EAX, 5FAA5	
81C3 33730000	ADD	EBX,7333	
2D B4F00D00	SUB	EAX, ODFOB4	
81C3 0D820300	ADD	EBX,3820D	
2D D4C00000	SUB	EAX, OCOD4	
81C3 80420B00	ADD	EBX,0B4280	
20 53780800	SUB	EAX, 87853	
81C3 FF040D00	ADD	EBX,0D04FF	
2D AA650900	SUB	EAX, 965AA	
81EB 3F330A00	SUB	EBX, OA333F	
2D 74560000	SUB	EAX,5674	
81EB 450A0000	SUB	EBX, OA45	
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	
20 20460800	SUB	EAX,084620	
81EB C8800C00	SUB	EBX,0C80C8	
05 0BD30000	ADD	EAX, OD30B	
81EB A9270A00	SUB		
05 92A80200	ADD	EAX, 2A892	
81EB ABEED200	SUB	EBX, ZEEAB	
05 E1542809	400	FAX. 54F1	
MOV	10.5	$-\Lambda V$	
	1 1 2		
81EB 24AC0400	<b>HIB</b>	EBX 4AC2	
	CUD	EAX FERGER	

SUB EAX, FF862576 ADD EBX,80E74D05 MOV DWORD PTR DS:[EAX],EBX 81C3 054DE780

### BF 114D0E00 MOV EDI, 0E4011 MOV EBX, 8BCA BB CA8B0000 81EF 0BE90900 SUB EDI,9E90B 81EB 957E0500 SUB EBX,57E95 ADD EDI,18A48 81C7 488A0100 81EB 83310F00 SUB EBX,0F3183 81EF D6400B00 SUB EDI,0840D6 81C3 57680500 ADD EBX,56857 81EF C8FB0E00 SUB EDI, OEFBC8 MOV [EDI],EBX 81EF 10AC9AFF SUB EDI, FF9AAC10 81EB 6D47F67E SUB EBX,7EF6476D MOV DWORD PTR DS:[EDI],EBX 891F

Sample 2

FERTIDET.

2D 762586FF

8918

FAST, SECURE, GLOBAL,

Sample 1

## Metamorphic Algorithm (comparison)

third DWORD

BA         BA         BA         CONSTR         BB         CA1F0100         MOV         EEX, 11FCA           BE         83080700         MOV         ECX, 7083         B9         0F720300         MOV         ECX, 3720F           B1EA         3AC00800         SUB         EDX, 8C03A         B1EB         A45A0100         SUB         EEX, 15AA4           81EA         3AC40800         SUB         ESI, 70F08         B1C1         006A0700         ADD         ECX, 76A00           81EA         14540800         SUB         ESI, 1F81E         B1C1         106A0700         ADD         ECX, 76A00           81EA         48480900         SUB         EDX, 94848         B1C1         1A070100         ADD         ECX, 1071A           81C6         0EEC0000         ADD         EDX, 106805         B1C1         1A070100         ADD         ECX, 1071A           81C6         0E00000         ADD         ESI, 0F0001         B1E8         23980800         SUB         ECX, 1619C           81C4         6690700         SUB         EDX, 10099         B1E8         44800800         SUB         ECX, 1619C           81C4         6670700         SUB         EDX, 106607         B1C1         231E050
81EA 3AC00800       SUB EDX, 8C03A       B3 00720500       BUB CX, 37207         81EE 080F0700       SUB ESI, 70F08       81EB A45A0100       SUB EEX, 76A00         81EA 3AC40800       SUB ESI, 70F08       81C1 006A0700       ADD ECX, 76A00         81EE 1EF80100       SUB ESI, 1F81E       81C1 006A0700       ADD ECX, 75IA3         81EA 48480900       SUB EDX, 94848       81C1 1A070100       ADD ECX, 1071A         81C6 0BEE0000       ADD ESI, 0EE0B       81C1 1A070100       ADD ECX, 1071A         81C6 0BEE0000       ADD ESI, 0F0D1       81EB 23980800       SUB EDX, 94848         81C6 0BCA0000       ADD ESI, 0F0D1       81EB 23980800       SUB EEX, 89823         81C6 0BCA0000       ADD ESI, 0F0D1       81EB 64B00800       SUB EEX, 89823         81C6 0CA0800       ADD ESI, 0F0AD1       81EB 24870700       SUB EEX, 88064         81EA 629C0700       SUB EDX, 79C6C       81EB 24870700       SUB EEX, 7872A         81EA 629C0700       SUB EDI, 96FE2       81C1 06840400       ADD ECX, 6823         81EA 2380000       SUB ESI, 37674       81C3 D00A0100       SUB EEX, 6AF6C         81EA 249500700       SUB ESI, 7371       81EB 6480000       SUB EX, 6AF6C         81EA 2500500       SUB ESI, 7371       81EB 6480000       SUB EX, 6AF6C
81EE       080F0700       SUB       ESI, 70F08       SUB       SUB       ESI, 70F08         81EA       3AC40800       SUB       EDX, 8C43A       81C1       006A0700       ADD       EEX, 76A00         81EA       3AC40800       SUB       EDX, 8C43A       81C3       E3220D00       ADD       EEX, 76A00         81E4       48480900       SUB       EDX, 94848       81C1       A3510700       ADD       ECX, 75A3         81C6       0BEE0000       ADD       ESI, 1F81E       81C1       1A070100       ADD       ECX, 1071A         81C6       0BEE0000       ADD       ESI, 0F0001       81EB       23980800       SUB       EBX, 89823         81C6       D1000F00       ADD       ESI, 0F0001       81EB       64800800       SUB       EBX, 89823         81C6       D6CA0800       ADD       ESI, 0F0001       81EB       64800800       SUB       ESX, 89823         81C6       D6CA0800       ADD       ESI, 0F0001       81EB       81EB       64800800       SUB       EX, 88064         81C6       D6CA0800       ADD       ESI, 0RCAD6       81E1       231E0500       ADD       ECX, 51E23         81C6       D6CA08000       SU
81EA 3AC40800       SUB EDX, 8C43A       81C1 00080700       ADD ECX, 78A00         81EE 1EF80100       SUB EDX, 1F81E       81C3 E3E20000       ADD ECX, 751A3         81EA 48480900       SUB EDX, 94848       81C1 A3510700       ADD ECX, 751A3         81C2 05680000       ADD ESI, 0EE08       81C1 1A070100       ADD ECX, 1071A         81C4 01000F00       ADD EDX, 006805       81EB 23980800       SUB EBX, 89823         81C6 01000F00       ADD ESI, 0F0001       81EB 23980800       SUB EBX, 89823         81C6 06CA0800       ADD ESI, 0F0001       81EB 64B00800       SUB EBX, 88064         81C4 07360A00       ADD ESI, 0F0001       81EB 23980800       SUB EBX, 88064         81C4 07360A00       ADD ESI, 08CAD6       81C1 231E0500       ADD ECX, 48406         81EA 62670700       SUB EDX, 79C6C       81C1 D6840400       ADD ECX, 48406         81EA 62670700       SUB EDX, 96FE2       81C1 D6840400       ADD ECX, 48406         81E2 74760300       SUB ESI, 0853A0       81E9 238C0600       SUB ECX, 68C23         81E4 29500700       SUB ESI, 37674       81C3 D00A0100       ADD EX, 68C23         81C4 71730000       ADD EX, 75D29       81E9 238C0600       SUB EX, 68C23         81C6 71730000       ADD EX, 75D29       81E9 A3830600       SUB EX,
81EE       1EF 80100       SUB       EST, 1F81E       81C3       ASLC3       ASLC3000       ADD       EEX, 751A3         81C4       48480900       SUB       EDX, 94848       81E8       2A9F0600       SUB       EBX, 69F2A         81C4       DECX, 006805       81C1       1A070100       ADD       ECX, 1071A         81C4       D1000F00       ADD       EST, 0F00D1       81E9       99C610100       SUB       EEX, 88823         81C4       D6CA0800       ADD       EST, 0F00D1       81E9       9C610100       SUB       EEX, 1619C         81C4       D6CA0800       ADD       EST, 0F00D1       81E9       G64B00800       SUB       EEX, 88064         81C4       D6CA0800       ADD       EST, 0F00D1       81E9       C610100       SUB       EEX, 1619C         81C4       D6CA0800       ADD       EST, 0F00D1       81E9       C4B00800       SUB       ECX, 1619C         81C4       D6CA0800       ADD       EST, 0F06C       81C1       D640000       SUB       ECX, 51E23         81C4       D67360A00       ADD       EST, 0A3607       81C1       D640000       SUB       EEX, 0DDD         81E4       E26F0900       SUB
81EA       48480900       SUB       EDX, 94848       81C1       ABS10100       ADD       ECX, 751A3         81C6       0BEE0000       ADD       EST, 0EE0B       81C1       1A070100       ADD       ECX, 1071A         81C2       0568000       ADD       EST, 0EE0B       81C1       1A070100       ADD       ECX, 1071A         81C2       0568000       ADD       EST, 0F00D1       81EB       23980800       SUB       EBX, 89823         81E4       9900100       SUB       EDX, 10099       81EB       64800800       SUB       EEX, 7872A         81C4       050700       SUB       EDX, 79C6C       81C1       231E0500       ADD       ECX, 1071A         81C4       050700       SUB       EDX, 10099       81EB       64800800       SUB       EEX, 7872A         81C4       6050700       SUB       EDX, 79C6C       81C1       231E0500       ADD       ECX, 48406         81E4       E26F0900       SUB       EDX, 96FE2       81EB       DD0C0000       SUB       EEX, 0DDFD         81E2       24760300       SUB       EST, 37674       81C3       DD0A0100       ADD       EX, 68C23         81E4       29500700       SUB
81C6       OBEE0000       ADD       ESI, 0EE0B       SUC1       1A070100       ADD       ECX, 1071A         81C2       05680D00       ADD       EDX, 0D6805       81C1       1A070100       ADD       ECX, 1071A         81C4       01000F00       ADD       ESI, 0F00D1       81E8       23980800       SUB       EDX, 1619C         81C4       0900100       SUB       EDX, 10099       81E9       9C610100       SUB       EDX, 1619C         81C4       0900100       SUB       EDX, 10099       81E8       64B00800       SUB       EBX, 88064         81C4       06CA0B00       ADD       ESI, 0BCAD6       81E1       231E0500       ADD       ECX, 1619C         81C4       06CA0B00       ADD       ESI, 0BCAD6       81E2       31E0500       ADD       ECX, 1619C         81C4       06CA0B00       ADD       ESI, 0BCAD6       81E1       231E0500       ADD       ECX, 1619C         81C4       07360A00       ADD       ESI, 0A3607       81E1       231E0500       ADD       ECX, 484D6         81C4       23500900       SUB       EDX, 96F22       81E8       DDC0000       SUB       EDX, 0DEF4         81E2       23500700 <td< th=""></td<>
81C2       05680D00       ADD       EDX,006805       81EB       23980800       SUB       EDX,89823         81C6       D1000F00       ADD       ESI,0F00D1       81EB       23980800       SUB       EDX,89823         81C4       D9000100       SUB       EDX,10099       81EB       23980800       SUB       EDX,88823         81C4       D6CA0800       ADD       ESI,0BCAD6       81EB       64800800       SUB       EDX,51623         81C6       07360A00       ADD       ESI,0A3607       81EB       2AB70700       SUB       EBX,7872A         81C6       07360A00       ADD       ESI,0853A0       81EB       DDC0000       SUB       EBX,0DCDD         81C2       3A500900       SUB       ESI,37674       81C3       DD0A0100       ADD       EX,6823         81EA       295D0700       SUB       EDX,75D29       81EB       6CAF0600       SUB       EX,6823         81C6       71730000       ADD       ESI,7371       81E9       A3B30600       SUB       EX,683A3         81EA       29C0500       SUB       ESI,75D29       81EB       ECA0000       SUB       EX,683A3         81E4       1CF10400       SUB       EDX,4F1
81C6       D1000F00       ADD       EST,0F00D1       81E9       25380800       SUB       ECX,1619C         81EA       9900100       SUB       EDX,10099       81EB       64800800       SUB       EDX,88064         81C6       D6CA0800       ADD       EST,08CAD6       81E9       92610100       SUB       ECX,1619C         81C4       D6CA0800       ADD       EST,08CAD6       81E9       23800800       SUB       EDX,7872A         81C6       07360A00       ADD       EST,043607       81E1       D6B40400       ADD       ECX,484D6         81C2       3A500900       SUB       EDX,96522       81E8       DDDC0000       SUB       EBX,0DCDD         81C2       3A500900       SUB       EST,37674       81E9       238C0600       SUB       ECX,68C23         81E4       29500700       SUB       EDX,75029       81E8       6CAF0600       SUB       EBX,6AF6C         81E4       29500700       SUB       EDX,7371       81E8       6CAF0600       SUB       EX,6B3A3         81E4       29C00500       SUB       EDX,4F11C       81E9       A3830600       SUB       EX,6AF6C         81E4       29C00500       SUB       ED
81EA 99000100       SUB EDX, 10099       81EB 64B00800       SUB EDX, 88064         81C6 D6CA0B00       ADD ESI, 0BCAD6       81EB 64B00800       SUB EBX, 88064         81C6 07360A00       ADD ESI, 0A3607       81EB 2AB70700       SUB EBX, 7B72A         81C6 07360A00       ADD ESI, 0A3607       81EB 2AB70700       SUB EBX, 7B72A         81C4 23500900       SUB EDX, 96FE2       81EB DDDC0000       SUB EBX, 00CDD         81C2 3A500900       ADD EDX, 9503A       81E9 E4BF0D00       SUB ECX, 68C23         81EA 29500700       SUB EDX, 75029       81EB 6CAF0600       SUB EBX, 6AF6C         81C4 71730000       ADD ESI, 7371       81E9 A3B30600       SUB EBX, 6AF6C         81E4 29CD0500       SUB EDX, 415A9       81E9 87100C00       SUB EBX, 6AF6C
81C6       D6CA0B00       ADD       ESI,0BCAD6       81C1       231E0500       ADD       ECX,51E23         81C4       6C9C0700       SUB       EDX,79C6C       81EB       2AB70700       SUB       EDX,7B72A         81C6       07360A00       ADD       ESI,0A3607       81EB       2AB70700       SUB       EDX,7B72A         81C4       23600900       SUB       EDX,96F22       81EB       DDC0000       SUB       EBX,0DCDD         81C2       3A500900       ADD       EDX,9503A       81E9       E48F0000       SUB       ECX,0BFE4         81E4       29500700       SUB       ESI,37674       81C3       DD0A0100       ADD       ESX,6AF6C         81E4       29500700       SUB       EDX,75D29       81EB       6CAF0600       SUB       EBX,6AF6C         81C4       71730000       ADD       ESI,7371       81E9       23820600       SUB       EX,6B3A3         81E4       29500500       SUB       EDX,415A9       81EB       ECA0000       SUB       EX,6B3A3         81E4       29500500       SUB       EDX,415A9       81E9       2382000       SUB       EX,6B3A3         81E5       81C6       71730000       SUB
81EA 6C9C0700       SUB EDX,79C6C       81EB 2AB70700       SUB EDX,7872A         81C6 07360A00       ADD ESI,0A3607       81EB 2AB70700       SUB EEX,7872A         81EA E26F0900       SUB EDX,96FE2       81EB DDDC0000       SUB EBX,0DCDD         81E2 3A500900       ADD EDX,9503A       81E9 E4BF0D00       SUB EEX,0DBFE4         81E2 74760300       SUB ESI,37674       81C3 DD0A0100       ADD ECX,68C23         81E4 29500700       SUB EDX,75D29       81E9 238C0600       SUB EEX,68F6C         81E4 1CF104400       SUB EDX,4F11C       81E9 A3B30600       SUB EEX,6B3A3         81E4 29CD0500       SUB EDX,415A9       81E9 A000000       SUB EEX,00877
81C6       07360A00       ADD       ESI, 0A3607       S1C1       D6B40400       ADD       ECX, 4B4D6         81EA       E26F0900       SUB       EDX, 96FE2       S1EB       DDDC0000       SUB       EBX, 0DCDD         81C2       3A500900       ADD       EDX, 9503A       S1E9       E48F0D00       SUB       ECX, 0DBFE4         81E2       74760300       SUB       ESI, 37674       S1E9       238C0600       SUB       ECX, 68C23         81E4       295D0700       SUB       EDX, 75D29       S1EB       6CAF0600       SUB       ECX, 6823         81E4       1CF10400       SUB       EDX, 4F11C       S1E9       A3B30600       SUB       EX, 2AEC         81E4       29CD0500       SUB       EDX, 415A9       S1E9       S1E9       S1B000       SUB       EX, 0C10
81EA E26F0900       SUB EDX,96FE2       81C1 D6840400       ADD ECX,48408         81EE A0530B00       SUB ESI,0853A0       81EB DDDC0000       SUB EEX,0DCDD         81C2 3A500900       ADD EDX,9503A       81E9 E4BF0000       SUB EEX,0DBFE4         81EE 74760300       SUB ESI,37674       81C3 DD0A0100       ADD EBX,10ADD         81EA 295D0700       SUB EDX,75029       81EB 6CAF0600       SUB EEX,68C23         81EA 1CF10400       SUB EDX,4F11C       81E9 A3B30600       SUB EEX,6B3A3         81EE 29CD0500       SUB ESI,5C029       81E9 87100C00       SUB EEX,0C1087         81EA A9150400       SUB EDX,415A9       81E9 A3B30000       SUB EEX,0C1087
81EE       A0530B00       SUB       ESI,0B53A0       81EB       EAB,0DEFE4         81C2       3A500900       ADD       EDX,9503A       81E9       E4BF0000       SUB       ECX,0DBFE4         81EE       74760300       SUB       ESI,37674       81E9       238C0600       SUB       ECX,68C23         81EA       295D0700       SUB       EDX,75D29       81EB       6CAF0600       SUB       EBX,6AF6C         81E4       CF10400       SUB       EDX,4F11C       81E9       A3B30600       SUB       EBX,2AEC         81E4       29CD0500       SUB       EDX,415A9       81E9       81E9       81E9       CAD000
81C2       3A500900       ADD       EDX, 9503A       81C3       DD0A0100       ADD       EBX, 10ADD         81EE       74760300       SUB       ESI, 37674       81C3       DD0A0100       ADD       EBX, 10ADD         81EA       29500700       SUB       EDX, 75029       81EB       6CAF0600       SUB       EBX, 6AF6C         81C4       71730000       ADD       ESI, 7371       81E9       A3B30600       SUB       ECX, 6B3A3         81E4       29CD0500       SUB       EDX, 4F11C       81E9       81E9       87100C00       SUB       ECX, 00107         81E4       A9150400       SUB       EDX, 415A9       81E9       81E9       81E8       ECX, 001087
81EE       74760300       SUB       ESI,37674       81E9       238C0600       SUB       ECX,68C23         81EA       29500700       SUB       EDX,75D29       81EB       6CAF0600       SUB       EDX,68C23         81E4       29500700       ADD       ESI,7371       81E9       A3B30600       SUB       EDX,68C23         81E4       1CF10400       SUB       EDX,4F11C       81E9       EDX,46B3A3         81E4       29C0500       SUB       ESI,5CD29       81E9       81E9       81E9       238C0600         81E4       A9150400       SUB       EDX,415A9       81E9       238C0600       SUB       ECX,0C1087
81EA 29500700       SUB EDX,75029       81EB 6CAF0600       SUB EBX,6AF6C         81C6 71730000       ADD ESI,7371       81E9 A3B30600       SUB ECX,6B3A3         81EA 1CF10400       SUB EDX,4F11C       81EB EC2A0000       SUB EBX,2AEC         81EE 29CD0500       SUB ESI,5CD29       81E9 87100C00       SUB ECX,0C1087         81EA A9150400       SUB EDX,415A9       81EB AD60300       SUB EBX,3A6AD
81C6       /1/30000       AUD ES1,7371       81E9 A3B30600       SUB ECX,6B3A3         81EA       1CF10400       SUB EDX,4F11C       81EB EC2A0000       SUB EBX,2AEC         81E2       29CD0500       SUB ES1,5CD29       81E9 87100C00       SUB ECX,0C1087         81EA       A9150400       SUB EDX,415A9       81E8 AD660300       SUB EEX,0C1087
81EA         1CF10400         SUB         EBX, 4F11C         81EB         EC2A0000         SUB         EBX, 2AEC           81EE         29CD0500         SUB         ESI, 5CD29         81E9         87100C00         SUB         ECX, 0C1087           81EA         A9150400         SUB         EDX, 415A9         81EB         AD460300         SUB         EBX, 346AD
81EE 29CD0500 SUB ESI,5CD29 81E9 87100C00 SUB ECX,0C1087 81EA A9150400 SUB EDX,415A9 81EB AD460300 SUB ECX,0C1087
81EA A9150400  SUB EDX,415A9   81EB ADA60300  SUB EBX.346AD
81C2 FB760A00 ADD EDX,0A76FB 81C3 40730700 ADD EBX,77340
81EE EF350A00 SUB ESI,0A35EF 81E9 63780600 SUB ECX,67863
81C2 CF0C0D00 ADD EDX,0D0CCF 81C3 DD1E0100 ADD EBX,11EDD
MOV [EDX], ESI 8169 03110C00 8163 00110000 8163 00110000 8169 03110000 8169 03110000 8109 00000 8109 00000 8109 00000 8109 00000 8109 00000 800 00000 800 00000 800 00000 800 0000 800 00000 800 00000 800 0000 800 00000 800 00000 800 00000 800 0000 800 0000 8000000 800 0000 800 00000 800 0000 800 000000000 800 0000000000
81C5 80240100 ADD 25X, 12480 81E9 3B110C00 SUB ECX, 0C113B
SIEA IFSIBSFF ISUB EUX, FFBSSIIF
81EE 436AF467 SUB ESI,67F46A43
MOV DWORD PTR DS: [EDX], ESI MOV [EBX], ECX
Samula 1
Sample 1
81EB 1CD0A1FF SUB EBX, FFA1D01C
81E9 4E6EE1B2 SUB ECX, B2E16E4E
890B MOV DWORD PTR DS:[EBX],ECX
Sample 2

Sample 2

## Metamorphic Algorithm (detection)

00401000 00401002 00401003 00401004 00401005 0040100c 0040100c 00401010 00401012 00401015	0C 41 9C 43 27 C5A495 ADE9925A DDD1 77 2F 2E:41 8773 B9 884E F8	OR AL,41 PUSHFD INC EBX DAA LDS ESP,FWORD PTR SS:[EDX*4+EBF FST ST(1) JA SHORT 0040103F INC ECX XCHG DWORD PTR DS:[EBX-47],ESI MOV BYTE PTR DS:[ESI-8],CL ple 1	00401000 00401002 00401004 00401006 0040100F 0040100F 00401010 00401012 00401014		SUB DL,BYTI PUSHAD CMP DWORD H JS SHORT 00	E PTR DS:[EBX] PTR DS:[EBX],EBP	·],c9
00401000 00401005 00401006 00401006 00401006 00401006 00401010 00401012 00401015	90 E9 80000000 98 DDD1 F 77 2F 2E:41	OV EAX,F3A53A05 OP MP 0040108B WDE ST ST(1) A SHORT 0040103F NC ECX CHG DWORD PTR DS:[EBX-47],ESI OV BYTE PTR DS:[ESI-8],CL	00401000 00401005 00401006 0040100B 0040100C 0040100E 00401011 00401014	B8 6079D7A7 90 E9 80000000 4D 34 2A 1360 39 2B78 A3 F685 E4D87354	NDP JMP 0040 DEC EBP XOR AL.2		+39] -5D] 3D8E4],C9
		MOV EAX NOP JMP 0040					

## Demo – Metamorphic Algorithm





## Virlock As A File Infector

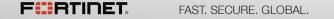




**Cleaning: How To Clean An Infected File** 

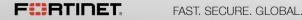
## **Basics**:

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

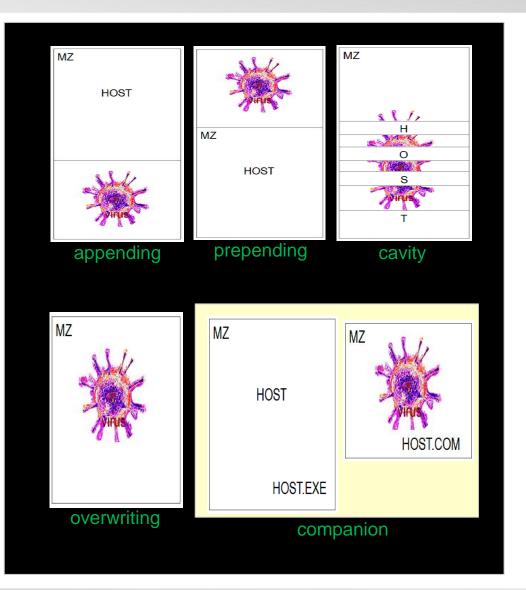


## Basics:

- Appending
- Prepending
- Cavity
- Overwriting
- Companion



## **Different Kinds Of File Infectors**



MZ	
VIFUS	
MZ	
ENCRYPTED HOST	
virlock	



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**

MZ header	MZ header	MZ header	MZ header
decoded bytes 0x0250			decoded bytes 0x0250
main function			main function
> on-demand poly			on-demand poly
> on-demand poly	on-demand p-i		on-demand poly
-> on-demand poly	on-demand Fina	ally, the host file	on-demand poly
> on-demand poly		s decrypted,	on-demand poly
.text	.text C	dropped, and executed.	Host file
			metamorphic algorithm
			0x06C77
			. <b>rsrc</b> 0x01200
B	B	G	Н



## Cleaning: Extracting The Host File From Virlock

	Address Hey dump		ASCLL
EBX = initial key SUB ESI,8 MOV EBX,DWORD PTR DS:[initial_key] XOR DWORD PTR DS:[ESI].EBX MOV EBX,DWORD PTR DS:[ESI] ADD ESI,4 XOR EDI,EDI MOV EDY,EDY	0042C1C3       )E       73       A7       57         0042C1D3       )E       73       A7       57         0042C1E3       )E       73       A7       57         0042C203       )G       EF       7B       4C         0042C223       )C       EA       EC       54         0042C233       PD       DD       AC       92         0042C233       A5       49       AA       D2         0042C233       A5       49       AC       92         0042C233       A6       49       F7       12         042C233       A6       49       A	9B         FA         A7         D7         82         F3         BB         57         85           82         F3         AC         57         87         73         B9         17         87           9E         73         AC         57         9E         B3         58         68         9E           9E         73         A7         57         9E         73         A7         57         9E           9E         73         A7         57         9E         73         A7         57         9E           9E         73         A7         57         9E         73         A7         57         9E           9E         73         A7         57         9E         73         A7         57         9E           9E         73         A7         57         9E         73         A1         57         9E           9C         04         AF         39         9E         20         D4         1F         8B           07         2F         FF         8C         56         2B         3F         4C         8B           03         68	B3       BF       97       !!▲.à¢       ?! €≤¬Wà ¬ù         33       34       Ø1       cs; ±€       340; s; ±c,340         73       89       57          °WR       ?WR:s,1±c,340         73       87       57       Rs°WR       ?WR:s <sup>2</sup> WRs <sup>2</sup> WRs <sup>2</sup> WR         73       A7       57       Rs°WR       ?WR:s <sup>2</sup> WRs <sup>2</sup> WRs <sup>2</sup> WR         73       A7       57       Rs <sup>2</sup> WR       ?WR:s <sup>2</sup> WRs <sup>2</sup> WRs <sup>2</sup> WR         73       A7       57       Rs <sup>2</sup> WR       ?WR:s <sup>2</sup> WRs <sup>2</sup> WRs <sup>2</sup> WR         73       A7       57       Rs <sup>2</sup> WR       ?WR:s <sup>2</sup> WRs <sup>2</sup> WRs <sup>2</sup> WR         73       A7       57       Rs <sup>2</sup> WR       ?WR:s <sup>2</sup> WRs <sup>2</sup> WR       dP         29       7D       4B       0p <sup>2</sup> >>9R       L\$Ti>>>K         68       BA       DF       ûn(L       '1U+?LEh         B         3B       7C       BC       fj/ª       in Pà(o-è; 1î       F         69       BD       A         not + r(x!#Rs <sup>2</sup> WR </td J       J         93       B       SA        !m <sup>2</sup> /       ?2       J       J         94       75       Si       NI¬m <sup>2</sup> WI       R <sup>2</sup> <t< th=""></t<>
MOV ECX, EBX	0042C2C3 9E 73 A7 57 0042C2D3 EC 63 A7 57	9E 73 F3 46 9E 73 F4 57 9F 9E 73 A7 57 9E 73 9F 57 DD	F3 B3 F3 Rs≌WRs≤FRs¢Wf≤ ≤ B3 E5 D7 ∞c≌WRs≏WRsfW  σ
MOV EBX, DWORD PTR DS: [ESI]	Adduese It		
ROR EBX,CL MOV DWORD PTR DS:[ESI],EBX	ESI = loca	ation of the encrypted Dec	ryptionKey
ADD ESI,4	0 042C1H3 0 042C1B3 90 00 03 00	00 00 04 00 00 00 FF FF 00	00 B8 00 É♥ ♥ ₹
INC EDI CMP EDI,EDX	XORing E	BX with dword in [ESI]	
JNE SHORT loop_here	generates	the DecryptionKey	3 69 73   17 - 0=! = @L=! This
	0042C213 62 4E 20 72	<u></u>	20 6D 6F be rul in DOS mo
	0042C233 0042C233 0042C243	3X = DecryptionKey	00 ה- 75 מפי. 172 E8 70 36 הה. קראים 100 המים E8 70 36 ה F8 AD 08 55 - קראים 115 - קראים 10
Decrypts the HOST file	6642C253 EBX = the	e next DWORD	E8 41 0B €2490 Að62"902Að E8 40 0B X20102á-12,902Lð
	0042C273 F E E 40 13 0042C283 E1 E8 40 15	EG ES ES 18 BD ES 39 14 EG	E8 2E 14 ≤호,¶αΣά-ČΣ∕¶αΣ.¶ E8 28 37 βΣθΣαΣΣ↑ <sup>1</sup> Σ9¶αΣ<7
	0042C293 EB E8 25 14 0042C2A3 E6 E8 2F 14	E0 E8 28 37 EA E8 24 14 E0 E0 E8 52 69 63 68 2E 14 E0	E8 E9 12 62%9x2<7R2\$9x20‡ E8 00 00 u2/9x2Rich.9x2
	0042C2B3 88 88 88 88 88 0042C2C3 88 88 88 88	00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4 <u>C 01 06</u>	00 00 00 00 52 90 PE L©+ Ré
	0042C2D3 C8 41 00 00	00 00 00 00 00 00 E0 00 0E	01 0B 01 4A 💦 🛪 70050

## Cleaning: Extracting The Host File From Virlock

	Address	Hoy dumy							ASCII
DecryptionKey	0042C193 0042C1A3 0042C1B3	OF DO AD	17 82 57 9E	FA A7 F3 A0 73 A6 73 B7	; 57 8' 57 9)	7 73 B9 E B3 58	57 85 B3 17 87 33 68 9E 73 57 9E 73	34 01 89 57	‼.A.ࢷ≏  é≤sWà ıù çs¦ ‡é≤24Wçs¦‡ç34©    ≏WRs≏WR }hRsëW Rs≏WRsηWRs≦WRs≏W
Original Host	0042C1D3 0042C1E3 0042C1E3 0042C1F3 0042C203	9E 73 A7 30 70 A7 96 EF 7B	579E Fadc 4007	73 A7 73 A7 00 AF 2F FF	2 57 91 2 57 91 7 39 91	E 73 A7 E 73 E1 E 20 D4	57 9E 73 57 9E F3 1F 8B 29 4C 45 68	A7 57 64 50 7D 4B	Rs≌WRs≌WRs≌WRs≌W Rs≌WRs≌WRs€WR≤dP Øp≏>9R =₹ï>>K ûn{L•⁄_ îV+îLEh  ■
Filename	0042C213 0042C223 0042C233 0042C233 0042C243	C6 6A 2F C7 EA EC 7D DD AC A4 09 AC	CB 03 54 1D D2 A6 92 A6	68 EF 71 AF C9 AC 09 B2	0D 8 17 9 52 A 55 A	5 7 E 7: EI 6 C HJ	52 A6 Ø9	8C 55	ran <sup>≜</sup> raR≏raR≏i;Z ño%de≏o∭Uñi R≏oîU
SUB ESI,8 MOV EBX,DWORD PTR DS:[initial_key] XOR DWORD PTR DS:[ESI],EBX MOV EBX,DWORD PTR DS:[ESI]	0042C253 0042C263 0042C273 0042C283 0042C283 0042C293	A5 49 AA A4 09 B2 A2 49 AC	D2 A6 92 A6 12 A6	09 77 49 8F 49 8F 49 9T	750 B: 750 B: 51 B:	1 49 AC E 89 AC 1 09 A9	92 A6 49 52 A6 C9 12 A6 49	74 55 AC 52 6D 5A	ÑI¬∏≏OwÜñק∩ñÜñ₽OwÜ ñO∭∩≏IâP∭Ił∦E≏ItU óI¾E≏IâP≟ił₩P≃F%2R ≏I≈‡≏I¥Q©ot‡≏ImZ ≊C∞#2I¥Q©ot‡≏EmZ
ADD ESI,4 XOR EDI,EDI MOV ECX,EBX	0042C273 0042C2A3 0042C2B3 0042C2C3 0042C2C3	A6 49 F7 A4 09 AE A7 89 AC 9E 73 A7 9E 73 A7 FC 63 A7	D2 A6 57 9E	C9 F3 73 A7	4D 80 57 91 46 91	6 E9 AC E 73 A7 E 73 F4	92 A6 49 57 9E 73	A7 57 A7 57 B3 F3	ñ0xd£≏ImZñIx(m≏0++S ≏ë≵am≏n≓XM&8t¥£≏I≏W Rs≏WRs≤WRs≤WRs≏W Rs≏WRs≤FRs WH≤I≤ ∞c≏WRs≤WRszWHIo†I
MOV EBX, DWORD PTR DS: [ESI]	00100000	20 00 111	01 72		01 77	. 10 /1	01 00 00	20 21	
XOR EBX,ECX ROR EBX.CL	Address	Hox dump	<u> </u>						ASCII
ROR EBX,CL MOV DWORD PTR DS:[ESI],EBX	0042C193	9E 73 A7		24 02		0 00 72	00 6F 00	<u> </u>	Rs≌W <b>_\$8</b> proc
ADD ESI,4	0042C1H3 0042C1B3	65 00 78 90 00 03	00 70 00 00				00 65 00 FF 00 00	4D 5A B8 00	exp.exe MZ
INC EDI	0042C1C3	00 00 00	00 00	00 40	000	0 00 00	00 00 00	00 00	Č Č
CMP EDI, EDX	0042C1D3	00 00 00						00 00	40 B-
JNE SHORT loop_here	0042C1E3 0042C1F3	00 00 00  BA 0E 00		00 00 CD 21			01 00 00 21 54 68	0E 1F 69 73	t© ∏v   月 - 0=!q©L=!This
	0042C203	20 70 72		72 61		0 63 61	6E 6E 6F	74 20	program cannot
	0042C213	62 65 20		6E 20		E 20 44	4F 53 20	6D 6F	be run in DOS mo
	0042C223 0042C233	64 65 2E 8E BB 2E	E 0D 0D E 14 E0					6A 75	de. <i>₽₽</i> ⊙\$ju <u>~                                    </u>
Decrypts the	0042C243	EB E8 21	) 14 EØ	E8 21 E8 55		C E8 28	Decryp	ted Ho	ost File ∞(¶xoio
HOST file	0042C253 0042C263	EE E8 34 EA E8 55		E8 41 E8 A0					1 ΩΩU11αQā⊷τ፬,¶α፬L♂
TIOOT IIIC	0042C273	F3 E8 20	;14 EØ	E8 A8	0 1C 8	Ø E8 2F	14 EØ E8	2E 14	<b>≤፬,¶α፬</b> ά⊢Ç፬∕¶α፬.¶
	0042C283	E1 E8 40	15 EØ	E8 E8 E8 28			14 E0 E8		βδ@δαδδ↑ <sup>11</sup> δ9¶αδ(7
	0042C293 0042C2A3	EB E8 25 E6 E8 21		E8 28 E8 52			14 E0 E8 14 E0 E8		δ፬%¶α፬<7Ω፬\$¶α፬θ‡ μ፬/¶α፬Rich.¶α፬
	0042C2B3	00 00 00	00 00	00 00	0 00 0	0 00 00	00 00 00	00 00	
	0042C2C3 0042C2D3	00 00 00 C8 41 00		00 50 00 00			01 06 00 00 0E 01		PE L©⊕ RÉ ĽA αΠΘδΘ

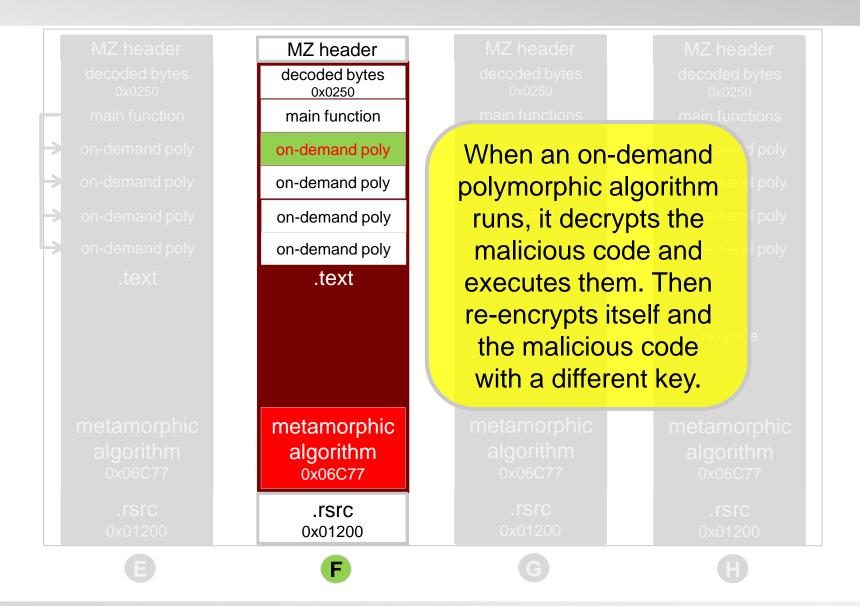


# Virlock As A Polymorphic Malware



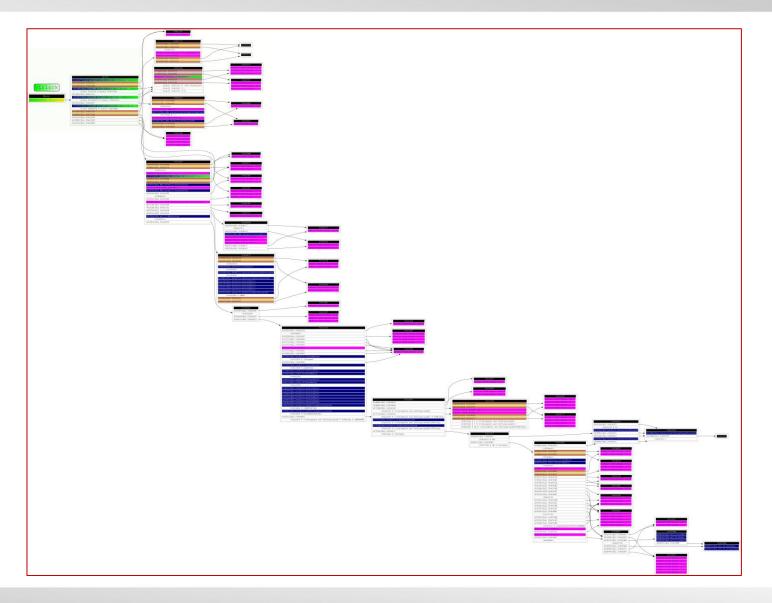


## **Reversing Stages**

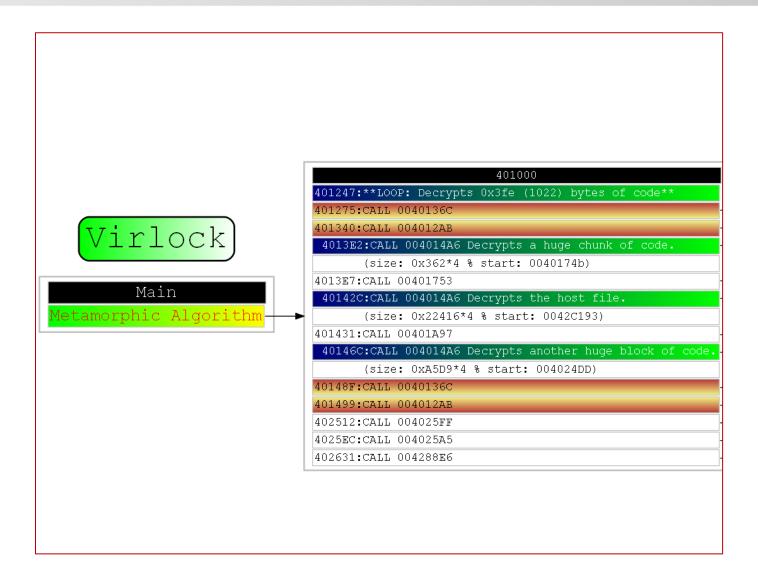


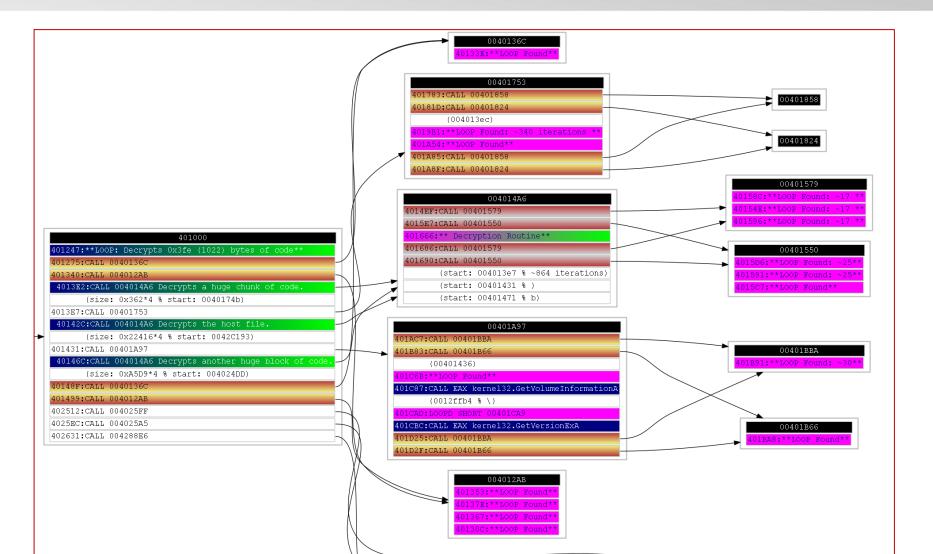










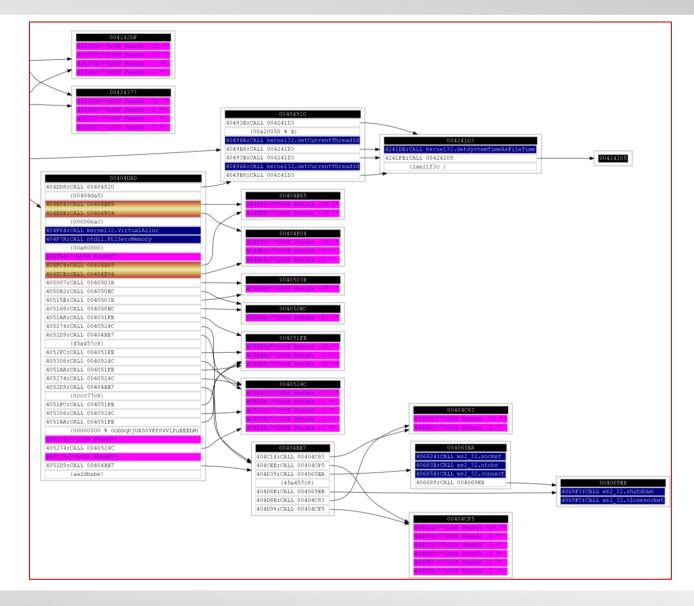


### C:CALL 00428979 (00402636) 94C2:CALL 00428979 653:CALL EAX kernel32.VirtualAl 10402545 0267F:CALL EAX kernel32.VirtualAllo 4026C8:CALL 004025FF 5FD:\*\*LOOP Found: (004bbe64) 4026D2:CALL 004025A5 GEC:REP MOVS BYTE PTR ES: [EDI], BYTE PTR DS: [ESI 40271B:CALL 004027BF 40282B:CALL 00402791 402874:CALL 0042B05E 402879:CALL 00423F79 288A:CALL ws2\_32.WS (00000101) 4028E3:CALL 00428569 42B086:CALL 0042B117 0042B117 (00402879) B14C:\*\*LOOP Found: 42B182:CALL 0042B160 2B1DC:CALL EAX kernel32.VirtualAlloc B1F2:LOOPD SHORT 0042B1EE B231:\*\*LOOP Found: ~181 \*\* 2B216:\*\*LOOP Found: ~367 \*\* 42B251:CALL 0042B117 B1A3:\*\*LOOP Found: 428258:CALL 00428160 423F9F:CALL 0042407B 42403F:CALL 00424006 0042407B (0040287e) 24061:\*\*LOOP Found: 24072:\*\*LOOP Found CALL kernel 000040) CALL ADVAPI32.SetSecurityD 411F:CALL kernel32.VirtualAllo 4138:CALL kernel32.VirtualAllo 00424006 CALL kernel32.VirtualAll LL kernel32.Virt 24095:\*\*LOOP Found: ~2 ALL kernel32.Get (00423f4a % TEMP) 4241BD:CALL 0042407B 4241C7:CALL 00424006 004285BC 42858F:CALL 004285BC (004028e8) 428664:CALL 004285F7 630:\*\*LOOP Found: 4286D7:CALL 00424525 28682:\*\*LOOP Found:



FAST. SECURE. GLOBAL.







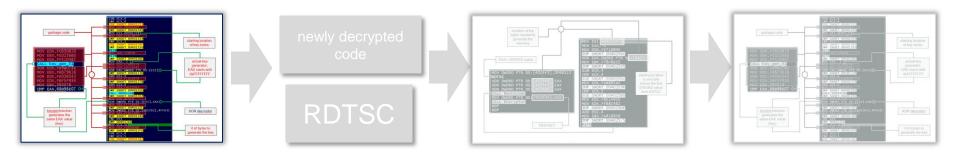
FAST. SECURE. GLOBAL.

# **On-Demand Polymorphic Algorithm**





- 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



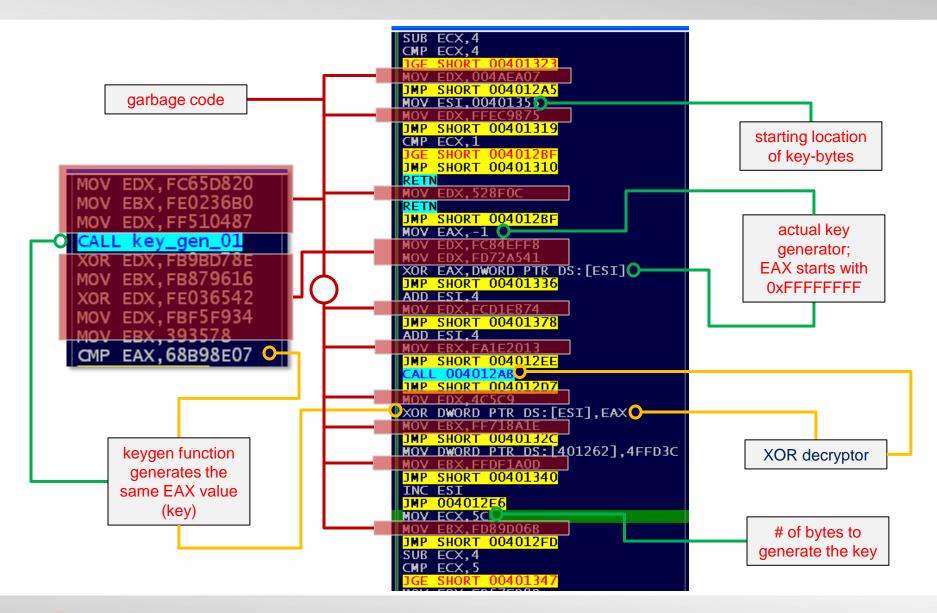


## Decryptor

## Features:

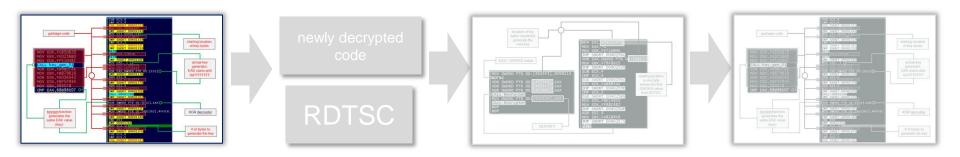
- Uses garbage code
- Keygen function for redundancy check
- Uses XOR to generate the key
- Uses XOR to decrypt a block of code

Decryptor



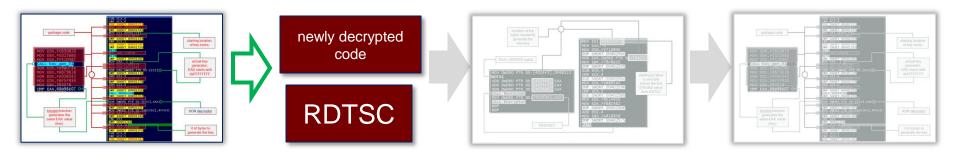


- Uses Decryptor to decrypt a block of code using an old key
- Executes the newly decrypted code
- Uses RDTSC (Read Time-Stamp Counter) to generate a new dword value
- Uses NewKeyGenerator to generate new key
- Uses Encryptor to encrypt the same block of code using the new key

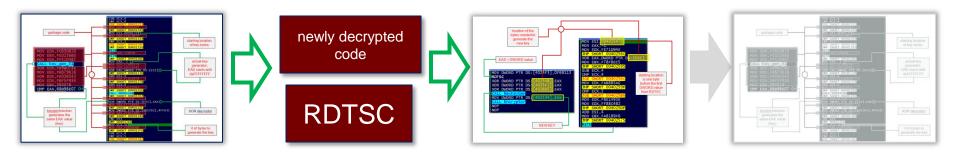




- Uses Decryptor to decrypt a block of code using an old key
- Executes the newly decrypted code
- Uses RDTSC (Read Time-Stamp Counter) to generate a new dword value
- Uses NewKeyGenerator to generate new key
- Uses Encryptor to encrypt the same block of code using the new key



- 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

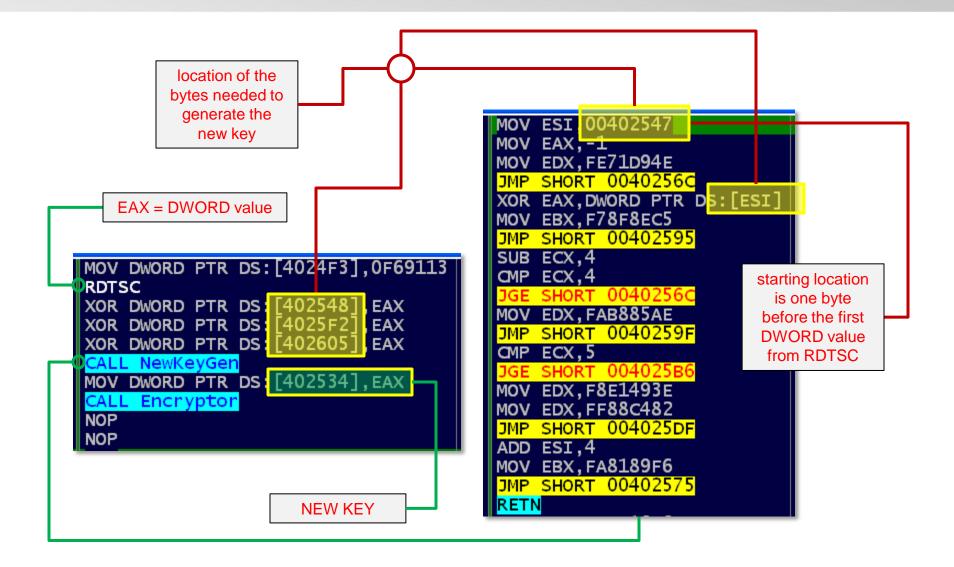




- **RDTSC** generates a new dword value
- Saves it in different memory locations
- The memory locations are within the memory range that contains key bytes
- Generates new key by XORing the key bytes
- Saves the new key to the original location of the old key used in the Decryptor

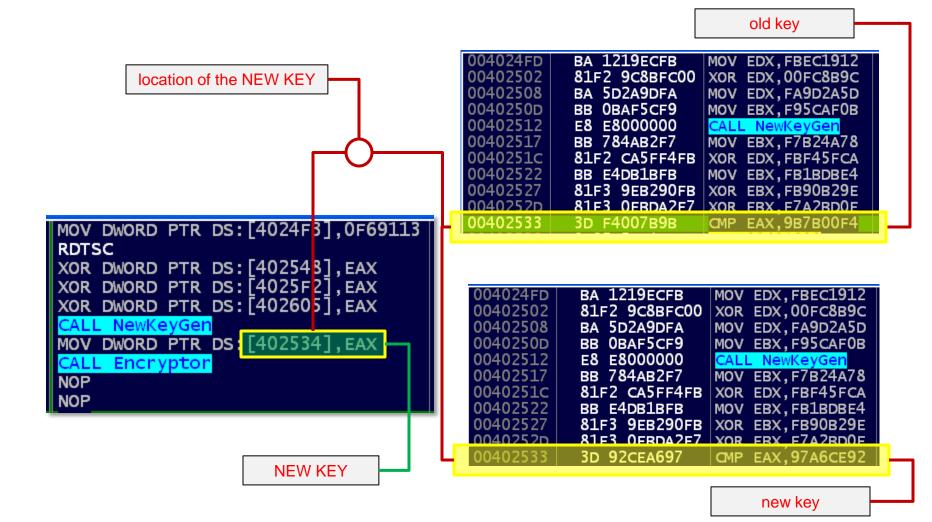
## NewKeyGenerator







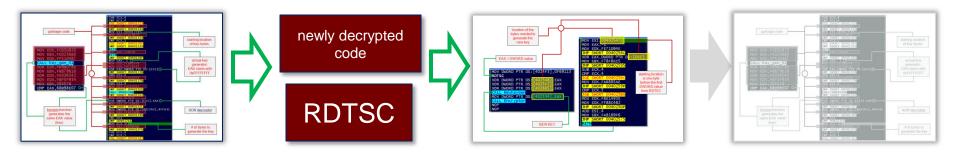
## **NewKeyGenerator**



FERTINET. FAST. SECURE. GLOBAL.

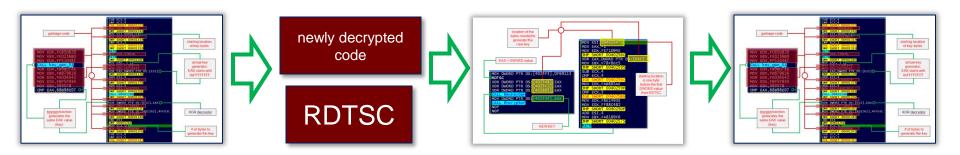
## Implementation

- 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



## 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

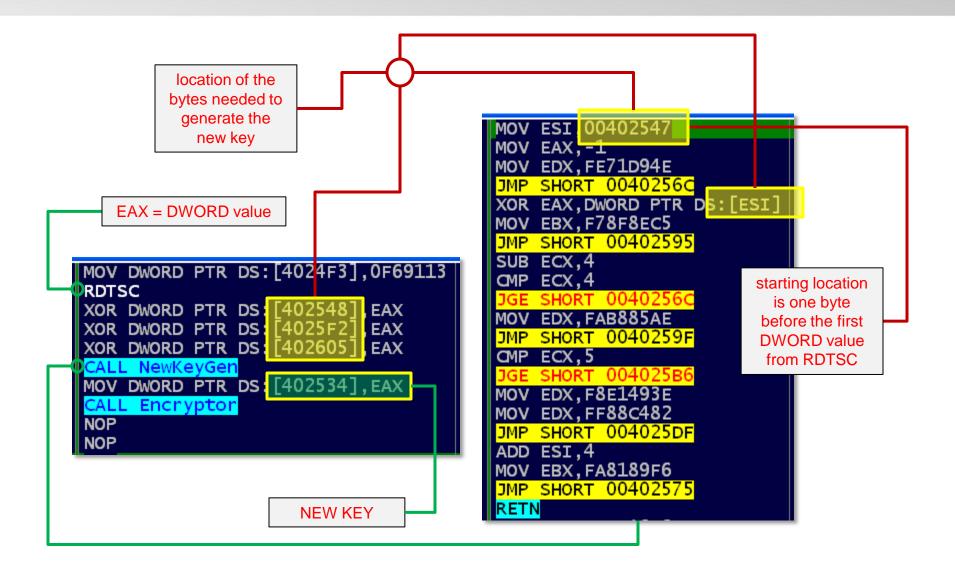
Address	Hex dumn										ASCII	~				
00402631 00402641	1C BØ 19 B4 68 7B	99 F4 8B F4	C7 7E 00 13	64 E2 98 F0			A F4 1 F4	00 A1		F1 ØF	-∭4Ör  ~dr@{ür {±  h{ïr ‼¢≡ {±ríí*		1C	в0	19	99
00402651 00402661	B6 00 84 DD BC 39	4B 57 9B 32	29 C7 06 7B	D9 F4 DD 16	FA		F F4 E 58	00 02	FØ 7B	AE F1	äKW>     r  {f  = «   ⊔9¢2⊕{ = ·   K⊠{t		F4	C7	7E	64
00402671 00402681	B4 68 7B 57 31 C7	8B F4 D9 F4	00 2B	F1 F4 27 B6			)F B6 )E F4	00 10	84 3B	4B 9B	]h(î[ +±[íí≉] äK W1  '[úB']] ÷R[▶;¢					
00402691	57 2D C7	D9 F4	C7 7E	AE 48	3 42	7B I	E 58	02	7B	5Ĉ			<b>E2</b>	40	7B	9A
004026A1 004026B1	F1 FF 6D 65 F6 7B	DB F4 94 C5	31 7E	9B F4 D3 D1			8 DØ 14 F1	40 F2	7B 5E	88 DB	± m r <c r  ~'nψ@<ê<br="">e÷&lt;ö+1~╙╤@&lt;¬±≥^</c>		F4	00	7B	F1
004026C1 004026D1		9E <u>D2</u> ØA <b>FF</b>	40 7B FF 90	73 Cf 90 F			4 57 D BC	<u>34</u> 42		DB 8B	encrypted with OLD					* *
	3D 31 BC		8B 0D	35 B	42	ÖÖ İ	3 44	81	3D	ЙЙ						
Address	Hex dump	_		_			_	-	-		ASCII					
00402631	E8 BØ 62	02 00	C7 Ø5	FF 16		00 0	1 00	00		6A			E8	в0	62	02
00402641 00402651		10 00 D0 A3	00 68 29 BC	00 04 42 00		00 6 00 0		A1 00		94 35	2∭08   2 = 6 8 j Ch ⊨ h ♦ j í rö B 4ú>4B ¦  ♦ ï5			Ъ	02	02
00402661	29 BC 42	00 C6	06 00	46 E2	FA	B8 4	5 AC	02	00	6A	> <sup>⊔</sup> B ⊨t FΓ aE‰B j		00	<b>C7</b>	05	FF
00402671 00402681	A3 31 BC	10 00 42 00	00 50 A3 39	6A 00 BC 42	00		4 42	00 10	40	D0 00	0h ▶ Pj íröB <sup>Π</sup> ú1⊔B ú9⊔B ì <b>4</b> ▶0		16	40	00	01
00402691 004026A1		42 00 40 00	C7 05 00 00	35 BC 00 00		00 4 05 F	5 AC	02 40	00 00	C7 13	ú–⊔B  \$5⊔BE&B   &0   \$454BE&B		110	40	00	0T
004026B1	91 F6 00	ØF 31	31 05	48 25	40	õõ 3		F2		40			00	00	00	6A
004026C1 004026D1	00 E8 CE	05 <u>26</u> FE <b>FF</b>	40 00 FF 90	E8 32 90 FC	: 8B	35 2	D BC	42	00		decrypted code	9				
004026E1	3D 31 BC	42 00	8B ØD	35 BC	: 42	00 F	3 A4	81	3D	00						
Address	Hex dump										ASCII	~				
00402631		E2 9D	9C EE	1F 8F	1B	EB E	1 9D	5B		8A 74	uδëΓ¥£€▼ï←δβ¥[δè 3δ≡¥[âαΰ[δ襷1t		75	EB	89	E2
00402641 00402651	DF 5B 14	FØ 9D 30 3E	5B 83 72 57	EØ 99 A2 91		EB 8 EB E	A 9D 4 9D		_	D5	Ε¶Ø>rWó¥ΓδΣ¥Ε`F			_		
00402661		ЕО 5В FO 9D	5D EB 5B BB	A6 7E 8A 9T	A1 FA	53 A 31 7	5 31 4 DF	59 5B		8A 30	-1 τ⊢α[]δ≌△íSñ1¥δè ]3δ≡¥[ŋ襷1t∎[¶0]		9D	9C	EE	<b>1F</b>
00402681	3E 6A 57	A2 9D	F8 D2	5C DI	5B	<u>66</u> E	5 9D	4B	AB	ĒØ	>jWó¥⁰π\■[fσ¥K½α >vWó¥£€ F!↓δÑ1¥δ'		88	<b>1</b> B	EB	<b>E1</b>
00402691 004026A1	3E 76 57 98 A4 FD	A2 9D A0 9D	9C EE 5B EB	D5 21 E0 91	19 90	EBA EE1	5 31 3 B9	59 1B		27 F3	ÿñ²á¥[δα¥£€!!¦ €δ≤∣					
004026B1 004026C1	ØC AD EB 9D 6A EE	2C AC E5 BB	6A EE 1B EB	A8 B8 CC AF		EB D				АØ Ай	¥וֹס, אַןּכּנִק+סִקּטֶּרןוֹאַ ¥.וכּסק+סו⊳אװיזויס, אַ		<b>9</b> D	5B	EB	<b>8</b> A
004026D1	9D 75 53	63 FF	FF 90	90 FC	8B	35 2	D BC	42	ØØ	8B	encrypted with NEV					
004026E1	3D 31 BC	42 00	8B ØD	35 BC	42	ың қ	3 A4	81	3D	00						

#### Detection

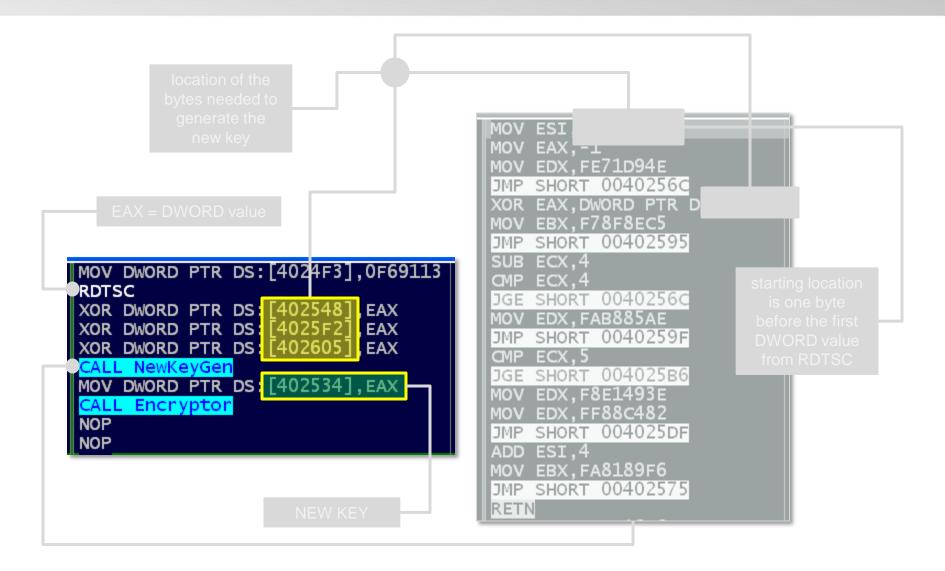
Address       Hex. dumn         00402631       00402641         00402651       00402651         00402661       00402671         00402681       00402681         00402681       00402681         00402661       00402681         00402661       00402681         00402661       00402681         00402681       00402681         00402661       00402681         00402661       00402681         00402661       00402681         00402661       00402681         00402661       00402681         00402661       00402681         00402661       FF FF 90 90 FC 8B 35 2D BC 42 00 8B         ercypted with OLD KEY	1C F4 E2 F4		19 7E 7B 7B	64 9A
Address       Hex dump       ASCII         00402631       E8 B0 62 02 00 C7 05 FF 16 40 00 01 00 00 06 A       00 40 00 6A       00 40 2641         00402641       40 68 00 10 00 00 68 00 04 00 00 6A       00 A1 DA 94         00402651       42 00 FF D0 A3 29 BC 42 00 B9 00 04 00 00 8B 35       B       -40 20 B         00402661       29 BC 42 00 C6 06 00 46 E2 FA B8 45 AC 02 00 6A       00 H > 1 + + + + + + + + + + + + + + + + + +	E8 00 16 00	B0 C7 40 00	62 05 00 00	02 FF 01 6A
Address       Hax dump       ASCII         00402631 $00402631$ $00402641$ $00402641$ 00402661 $00402661$ $00402661$ $10^{2} \times 10^{2} \times 1$	75 9D 8B		89 EE EB	1F



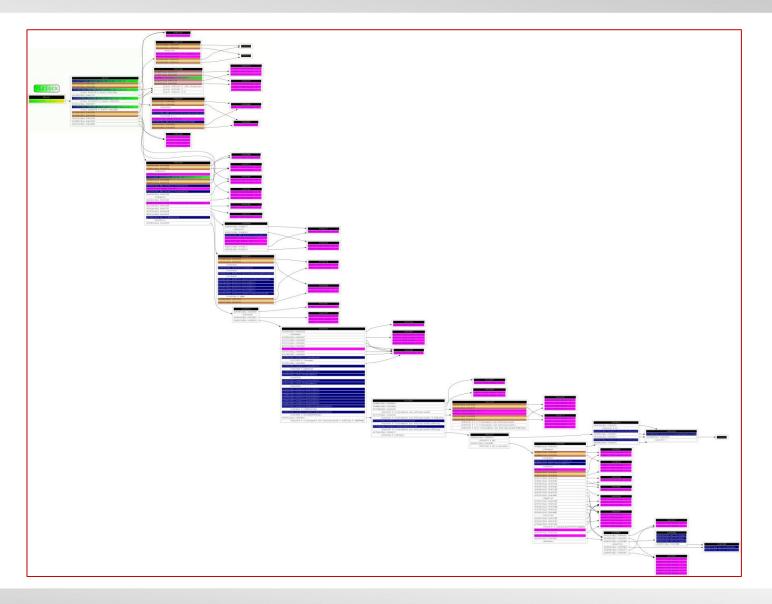
#### Detection



## Detection



## **Dynamic Routine Execution Map**





## Virlock As A Ransomware





## **Visible Signs of Infection**









#### 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 Online fine payments are processed by Royal Bank of Canada. After the payment is finalized enter Transfer ID below. Amount: Transfer ID: BTC 0.588 PAY FINE 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





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): 198tX7NmLg6o8qcTT2Uv9cSBVzN3oEozpv 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

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





View: Canadian Exchanges <u>Inter</u>	rnational Exchanges								
CaVirtex	Aaron Buys Gold Ltd								
https://www.cavirtex.com/home	aaronbuysgold.com								
(888)812-2525	Canada Wide 1.866.549.7747								
	Edmonton 780.628.6895								
Bitcoiniacs	947 Ordze Road Sherwood Park								
bitcoiniacs.com									
Waves Coffee, #100 - 900 Howe St. Vancouver	vault of Satoshi vaultofsatoshi.com								
BC V6Z 2M4 Canada	(855) 457-0101								
1 (877) 814-7460	(55) 457-0101								
contact@bitcoiniacs.com	340 Henry Street, Unit #16								
000000000000000000000000000000000000000	Brantford, Ontario								
QuadrigaCX	Canada, N3S 7V9								
quadrigacx.com									
Phone: 1-604-757-9660	Coin Clutch								
Email: contact@quadrigacx.com	coinclutch.com								
	Email: support@coinclutch.com								
QuickBT	Toll-Free: 1-800-704-0012								
quickbt.com/ca/									
1-888-QUICK-55 (784-2555) Tradebitcoin.com									
Payment BitCoin Information Bit	tCoin Exchanges BitCoin ATMs Internet Browser Notepad Network Connections								





BTM Locato	ors	Roboco ro	boco.in				
<u>Edmonton (</u> Fort Mcmur		BitCoin A	TM bitcoinatm.com				
Montreal (	(7)	CoinDesk	coindesk.com/bitcoi	.n-atm-map/			
<u>Vancouver</u> <u>Ottawa (2)</u>		BitCoin A	TM Map bitcoinatmma	ap.com			
<u>Quebec (3)</u> Sherwood F							
<u>Whistler (</u>	(1)						
<u>Winnipeg (</u> Alberta (1	·						
Saskatoon	(2)						
<u>Moncton (1</u> North Bay							
Toronto (2							
<u>Victoria (</u> <u>Halifax (</u> 1							
<u>Payment</u>	BitCoin	Information	<u>BitCoin Exchanges</u>	BitCoin ATMs	Internet Browser	<u>Notepad</u>	<u>Network Connections</u>





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

## **Eradication**





## **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:
  - $\checkmark$  Get patterns from the decrypted code
- For cleaning:
  - ✓ Remove the entries from the registry keys
  - ✓ Extract the host file

# Mulțumesc!





