CryptNET Ransomware

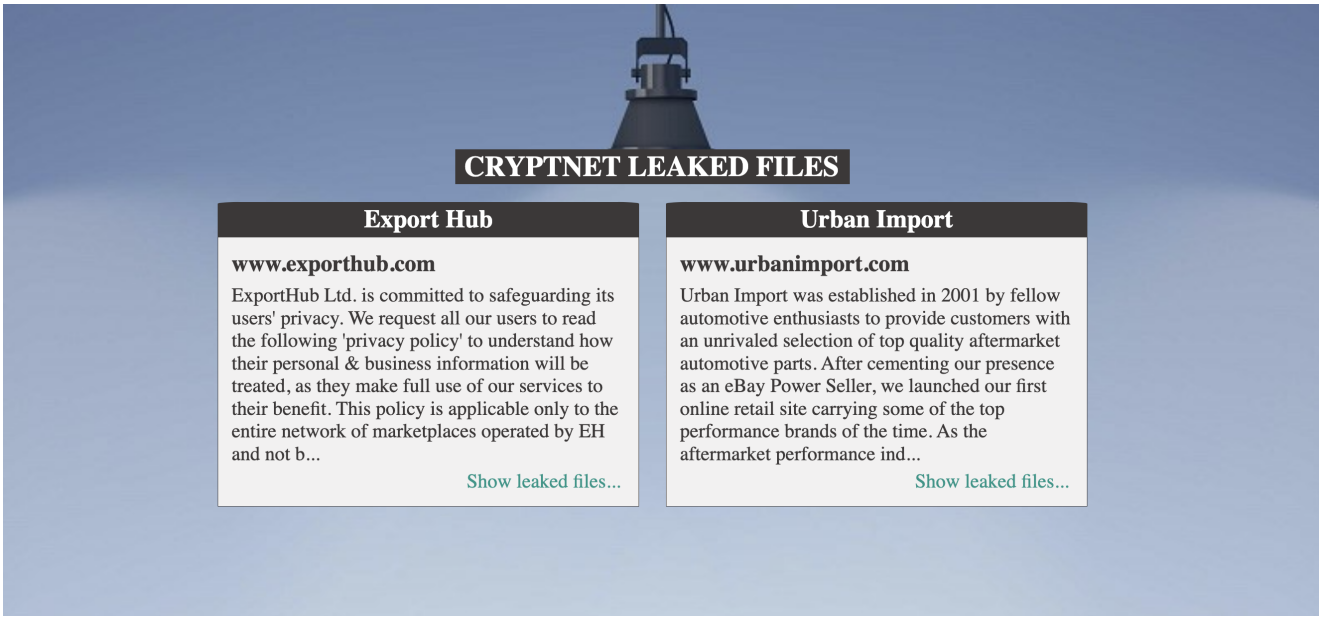
research.openanalysis.net/dotnet/cryptnet/ransomware/2023/04/20/cryptnet.html

OALABS Research April 20, 2023

Overview

This is a new .NET ransomware that was recently documented on Twitter by Zscaler ThreatLabz. This ransomware has a leaks site at `http[:]//blog6zw62uijolee7e6aqqnqaszs3ckr5iphzdzsazgrpvtqtjwqryid[.]onion/` and has atleast one victim.

According to Zscaler the ransomware is also protected using `.NET Reactor`



Example Ransom Note

```
*** CRYPTNET RANSOMWARE ***

--- What happened? ---
All of your files are encrypted and stolen. Stolen data will be published soon
on our tor website. There is no way to recover your data and prevent data leakage
without us
Decryption is not possible without private key. Don't waste your and our time to
recover your files.
It is impossible without our help

--- How to recover files & prevent leakage? ---
To make sure that we REALLY CAN recover your data - we offer FREE DECRYPTION for
warranty.
We promise that you can recover all your files safely and prevent data leakage. We
can do it!

--- Contact Us---
Download Tor Browser - https://www.torproject.org/download/ and install it
Open website:  http://cryptr3fmuv4di5uiczofjuypopr63x2gltlsvhur2ump4ebru2xd3yd.onion
Enter DECRYPTION ID:  xxxxxxxxxxxxxxxxxxxxxxxxxx
```

Sample

`2e37320ed43e99835caa1b851e963ebbf153f16cbe395f259bd2200d14c7b775` UnpacMe

References

NETReactorSlayer thanks washi for the tip :))

Analysis

- Files are encrypted with AES CBC using a generated 256 bit key and IV.
- The generated AES keys are encrypted using a hard coded RSA key and appended to the encrypted files.

RSA Key

```
"<RSAKeyValue>
<Modulus>8TO8tQQRyFqQ0VShtSpLkDqtDVsrxS8SfdOsqRAj8mWF7sVoGzyZMcv501DF6iZUdKYsFDlaSMnu
ckG9+MJmD2ldZwU/0H6Xztkta1BkJWSO2qHg2JAGDp9ZsFGP1wDR9oRb1w7wtBe7Db3wf7q848+qKPWiTP/2R
/jlR4evW73M65Jdo9uOzQnbmvw+blsloXeszuYlW2nCcwQ7WarzAK29UmM9ZHS0/lqzU0KHNU+DvyfGwmMJgt
b2HN6GFGXq9Z0n3dNBCQVzdUl2G/7fLAMoFbJeExn5USZdFHr2ygheTilo/shmfq7tcPCZM8C4zqBtb0Nbct0
f/M48+H920Q==</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>"
```

File Extension Targets

```
.myd .ndf .qry .sdb .sdf .tmd .tgz .lzo .txt .jar .dat .contact .settings .doc .docx
.xls .xlsx .ppt .pptx .odt .jpg .mka .mhtml .oqy .png .csv .py .sql .indd .cs .mp3
.mp4 .dwg .zip .rar .mov .rtf .bmp .mkv .avi .apk .lnk .dib .dic .dif .mdb .php .asp
.aspx .html .htm .xml .psd .pdf .xla .cub .dae .divx .iso .7zip .pdb .ico .pas .db
.wmv .swf .cer .bak .backup .accdb .bay .p7c .exif .vss .raw .m4a .wma .ace .arj .bz2
.cab .gzip .lzh .tar .jpeg .xz .mpeg .torrent .mpg .core .flv .sie .sum .ibank
.wallet .css .js .rb .crt .xlsm .xlsb .7z .cpp .java .jpe .ini .blob .wps .docm .wav
.3gp .gif .log .gz .config .vb .m1v .sln .pst .obj .xlam .djvu .inc .cvs .dbf .tbi
.wpd .dot .dotx .webm .m4v .amv .m4p .svg .ods .bk .vdi .vmdk .onepkg .accde .jsp
.json .xltx .vsdx .uxdc .udl .3ds .3fr .3g2 .accda .accdc .accdw .adp .ai .ai3 .ai4
.ai5 .ai6 .ai7 .ai8 .arw .ascx .asm .asmx .avs .bin .cfm .dbx .dcm .dcr .pict .rgbe
.dwt .f4v .exr .kwm .max .mda .mde .mdf .mdw .mht .mpv .msg .myi .nef .odc .geo
.swift .odm .odp .oft .orf .pfx .p12 .pl .pls .safe .tab .vbs .xlk .xlm .xlt .xltm
.svgz .slk .tar.gz .dmg .ps .psb .tif .rss .key .vob .epsp .dc3 .iff .opt .onetoc2
.nrw .pptm .potx .potm .pot .xlw .xps .xsd .xsf .xsl .kmz .accdr .stm .accdt .ppam
.pps .ppsm .1cd .p7b .wdb .sqlite .sqlite3 .db-shm .db-wal .dacpac .zipx .lzma .z
.tar.xz .pam .r3d .ova .1c .dt .c .vmx .xhtml .ckp .db3 .dbc .dbs .dbt .dbv .frm .mwb
.mrg .txz .mrg .vbox .wmf .wim .xtp2 .xsn .xslt
```

Services To Kill

```
BackupExecAgentBrowser veeam VeeamDeploymentSvc PDVFSService BackupExecVSSProvider
BackupExecAgentAccelerator vss sql svc$ AcrSch2Svc AcronisAgent
Veeam.EndPoint.Service CASAD2DWebSvc CAARCUpdateSvc YooIT memtas sophos veeam
DefWatch ccEvtMgr SavRoam RTVscan QBFCService Intuit.QuickBooks.FCS YooBackup
BackupExecAgentBrowser BackupExecRPCService MSSQLSERVER backup GxVss GxBlr GxFWD
GxCVD GxCIMgr VeeamNFSSvc BackupExecDiveciMediaService SQLBrowser
SQLAgent$VEEAMSQL2008R2 SQLAgent$VEEAMSQL2012 VeeamDeploymentService
BackupExecJobEngine Veeam.EndPoint.Tray BackupExecManagementService SQLAgent$SQL_2008
BackupExecRPCService zhudongfangyu sophos stc_raw_agent VSNAPVSS QBCFMonitorService
VeeamTransportSvc
```

Processes To Kill

```
sqlwriter sqbcoreservice VirtualBoxVM sqlagent sqlbrowser sqlservr code steam zoolz
agntsvc firefoxconfig infopath synctime VBoxSVC tbirdconfig thebat thebat64
isqlplussvc mydesktopservice mysqld ocssd onenote mspub mydesktopqos CNTAoSMgr
Ntrtscan vmplayer oracle outlook powerpnt wps xfssvccon ProcessHacker dbeng50 dbsnmp
encsvc excel tmlisten PccNTMon mysqld-nt mysqld-opt ocautoupds ocomm msaccess
msftesql thunderbird visio winword wordpad mbamtray
```

Shadow Copies Destroyed

```
vssadmin delete shadows /all /quiet & wmic shadowcopy delete
bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default}
recoveryenabled no
wbadmin delete catalog -quiet
```

Files Excluded From Encryption

```
iconcache.db
autorun.inf
thumbs.db
boot.ini
bootfont.bin
ntuser.ini
bootmgr
bootmgr.efi
bootmgfw.efi
desktop.ini
ntuser.dat
```

Directories Excluded From Encryption

```
windows.old
windows.old.old
amd
nvidia
program files
program files (x86)
windows
$recycle.bin
documents and settings
intel
perflogs
programdata
boot
games
msocach
```