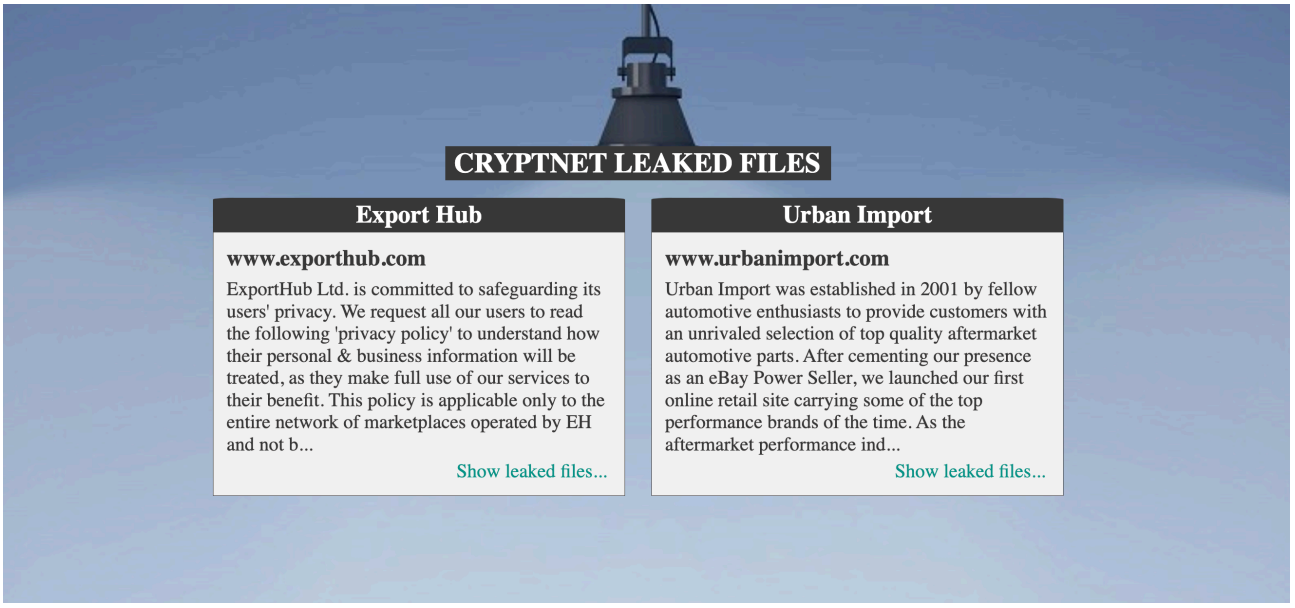
CryptNET Ransomware

Published: 2023-04-20 · Archived: 2026-04-05 19:21:49 UTC

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:  xxxxxxxxxxxxxxxxxxxxxxxxx
```

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>8TO8tQQRyFqQ0VShtSpLkDqtDVsrxS8SfdOsqRAj8mWF7sVoGzyZMcv501DF6iZUdKYsFDlaSMnuckG9+MJmD2l
```

File Extension Targets

```
.myd .ndf .qry .sdb .sdf .tmd .tgz .lzo .txt .jar .dat .contact .settings .doc .docx .xls .xlsx .ppt .pptx .od
```

Services To Kill

```
BackupExecAgentBrowser veeam VeeamDeploymentSvc PDVFSService BackupExecVSSProvider BackupExecAgentAccelerator
```

Processes To Kill

```
sqlwriter sqbcoreservice VirtualBoxVM sqlagent sqlbrowser sqlservr code steam zoolz agntsvc firefoxconfig infop
```

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
```

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