How to Protect Yourself from CryptoLocker Ransomeware Variants
Agenda

• High level topics
  – What is Ransomware?
  – What is vshadow?
  – How does an attacker abuse vshadow?

• Visibility
  – What happens on the host from the host point of view with CryptoLocker

• Stopping this Ransomware threat
  – How to prevent this infection with CryptoLocker V1
What Can Ransomware Do?

Ransomware can:
- Prevent you from accessing Windows.
- Encrypt files so you can't use them.
- Stop certain apps from running (like your web browser).
- Demand that you do something to get access to your PC or files.
- Demand you pay money.
- Make you complete surveys.
VShadow is a command-line tool that you can use to create and manage volume shadow copies.

Also known as
- Shadow Copy
- Volume Snapshot Service
- Volume Shadow Copy Service
- VSS
We have seen the volume shadow service used for a number of things ranging from malware to penetration testing tools.
Abusing Shadows

Create shadow

Mounting the shadow with the “mklink” Command

The malware is dropped into shadow and mounted
Starting the Malware

Hiding the malware in MSDC

Malware Application Running

Malware Process Running

Image File
Version: 0.0.0.0
Build Time: Tue Jul 28 14:43:34 2015
Path: C:\Windows\System32\msdc\malware.exe
Command line: malware.exe
Current directory: C:\Windows\System32\msdc\nAutostart Location: n/a
Parent: cmd.exe(3232)
User: IKTHUS\user
Started: 2:53:54 PM 7/28/2015
Comment: 

<table>
<thead>
<tr>
<th>Image Name</th>
<th>User Name</th>
<th>...</th>
<th>Memory (...)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audiog.exe</td>
<td>LOCAL SERVICE</td>
<td>00</td>
<td>10,188 K</td>
<td>Windows Audio Device Graph Isolation</td>
</tr>
<tr>
<td>lsmod.exe</td>
<td>SYSTEM</td>
<td>00</td>
<td>796 K</td>
<td>Local Session Manager Service</td>
</tr>
<tr>
<td>malware.exe</td>
<td>master</td>
<td>00</td>
<td>736 K</td>
<td></td>
</tr>
<tr>
<td>mscore.dll</td>
<td>SYSTEM</td>
<td>00</td>
<td>860 K</td>
<td>.NET Runtime Optimization Service</td>
</tr>
</tbody>
</table>
Malware Running After Shadow is Deleted

Malware Process Running

Shadow Deleted

Malware process still running after shadow is deleted
How did I know my system was infected?
What happens on the host from the host point of view

Search for all files created in last 30 days

Get-ChildItem -Path 'C:\' -Filter "*.exe" -Recurse | Where-Object { $_.CreationTime -gt (Get-Date).AddDays(-1) } | Select-Object Fullname,CreationTime | Out-File -FilePath c:\out.txt
Finding the application Hash

```
certUtil -hashfile pathToFileToCheck HashAlgorithm

HashAlgorithm choices: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512
```

```
C:\>cd Windows\System32

C:\Windows\System32> certUtil -hashfile cmd.exe MD5
MD5 hash of file cmd.exe:
f5 ae 03 de 0a d6 0f 5b 17 b8 2f 2c d6 84 02 fe
CertUtil: -hashfile command completed successfully.

C:\Windows\System32> certUtil -hashfile cmd.exe SHA256
SHA256 hash of file cmd.exe:
6f 88 fb 88 ff b0 f1 d5 46 5c 28 26 e5 b4 f5 23 59 8b 1b 83 78 37 7c 83 78 ff eb
c1 71 ba d1 8b
CertUtil: -hashfile command completed successfully.
```
What happens to the host from the host point of view?
How to detect this attack

- **IOC’s**
  - Hashes
  - Filenames/paths
  - Registry Values
  - Network Connections

- **Behaviors**
  - Loading of Dependencies
  - Process of Execution
  - Usage of rarely executed native tools

**Hashes**

- MD5 (vshadow-7-32.exe) = 3e1360a23ea5f9caf4987ccf35f2fcaf
- MD5 (vshadow-7-64.exe) = 576b379a59d094fb7b06c261a96034a6
- MD5 (vshadow-8-32.exe) = d0cd7ad91b2ff568275d497214ff185c
- MD5 (vshadow-8-64.exe) = 97fd0f3c05f1707544a9a6a0c896b43e
- MD5 (vshadow-8.1-32.exe) = d560c155b68121d98f8370e7deafbc4d
- MD5 (vshadow-8.1-64.exe) = c5d2992c8c8a0771f71fe4d7625a0b8b
- MD5 (vshadow-vista-64.exe) = 53d3e33ad31af6716559f29e889aca49
Finding Vshadow Being Used

- Detect loading of DLL and ignore werfault
  - modload:vss_ps.dll cmdline:"-p" -path:System32\werfault.exe

- Command line or batch file usage for mklink
  - cmdline:""C:\Windows\system32\cmd.exe" /c mklink /D"

- Look for vshadow being run
  - process_name:vshadow.exe AND cmdline:"-p C:\"

- path:device/harddiskvolumeshadowcopy*
- path:device/harddiskvolume*

Hiding the malware in Shadow
How to prevent this infection

The file paths that have been used by this infection and its droppers are:

- C:\f1f94d81\f1f94d81.exe
- C:\Users\master\AppData\Roaming\f1f94d81.exe
- C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\f1f94d81.exe
Block executable in %AppData%

Path: %AppData%\*.exe

Security Level: Disallowed

Block executable in %LocalAppData%

1. Path if using Windows XP: %UserProfile%\Local Settings\*.exe
2. Path if using Windows Vista/7/8: %LocalAppData%\*.exe
3. Security Level: Disallowed
4. Description: Don’t allow executables to run from %AppData%
How to prevent this infection

TODAY’S FORECAST: CLOUDY WITH A CHANCE OF BANHAMMER
Flag it, Tag it, and Bag it.

Ryan Nolette
Carbon Black

https://github.com/sonofagl1tch
https://www.carbonblack.com/author/ryan-nolette/

boston.healthprivacyforum.com | #hitprivacy