Ransomware Variants Are Lurking “In the V-Shadows”

By Ryan Nolette
The man of many titles
- Security Operations Lead
- Senior Security Engineer
- Senior Threat Researcher
- Incident Response Consultant
• Who am I and what do I do?

• 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 V1

• Stopping this Ransomware threat
  • How to restore files encrypted using Shadow Volume Copies
  • How to prevent this infection with CryptoLocker V1
• My name is Ryan Nolette
  • I am currently the **Security Operations Lead** at Carbon Black
    – Manage Security Operations
    – Act as Senior Security Architect for Carbon Black
  • 10+ year veteran of IT, Incident Response, Threat Research, and Forensics
  • Carbon Black blog link

• **Responsibilities:**
  – Monitor Endpoint Events, Network Based Events, and Physical Security Events
  – User Education and Outreach
  – IT Oversight and Assistance
  – Security Oversight of Enterprise Projects
  – Incident Response
  – System Forensics
  – Vulnerability Scanning
  – Threat Research
  – ETC
Basically
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.
What is vshadow?

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.
Creating Shadows

Command

```
C:\>C:\Users\user\AppData\Local\Temp\vshadow.exe -p C:\
```

Output

```
QUERYING ALL SHADOW COPIES WITH THE SNAPSHOTSETID <458095b5-3d28-4d55-afd2-c5b916d0a>

* SNAPSHOT ID = {89c4339d-164b-4d0d-974f-7c844adaeff7} ...
  - Shadow copy Set: {458095b5-3d28-4d55-afd2-c5b916d0a}
  - Original count of shadow copies = 1
  - Original Volume name: \??\Volume<11e6f259-1536-11e5-824f-806e6f6e6963>\
    - Creation Time: 7/28/2015 12:31:03 PM
    - Shadow copy device name: \??\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
```
Mounting the shadow with the “mklink” Command

```
mklink /D C:\Windows\System32\msdc \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopies3\0
```

The malware is now mounted.
Starting the Malware

**Malware Process Running**

**Malware Application Running**

**Hiding the malware in MSDC**

```
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
```

```
Windows Task Manager

Task
C:\Windows\System32\msdc\malware.exe
```

```
Image File
Parent: cmd.exe(3232)
User: IKTHUSH\user
Started: 2:53:54 PM 7/28/2015
Comment: 
```

```
Malware Process Running
```

```
Malware Application Running
```

```
Hiding the malware in MSDC
```

```
```
Malware Running After Shadow is Deleted

Malware Process Running

Shadow Deleted

Malware process still running after shadow is deleted
Visibility

What happened?

What happened from the host point of view?
Sample detonated for this presentation

**MD5**  
c24605589c71eb4835f3ee2654812315  

**SHA1**  
B078772e826eaf2c736b96e7844f3828d2666b6f

**Initial location on the test system**  
C:\Users\master\Desktop\c24605589c71eb4835f3ee2654812315.b078772e826eaf2c736b96e7844f3828d2666b6f.exe

**Processes spawned:**  
- C:\Users\master\Downloads\PDMHSOFE\webpage-38715fa8845ad8844759960e8b8a34b3.zip.exe
- C:\Windows\syswow64\svchost.exe  
- C:\Windows\syswow64\vssadmin.exe
- C:\Users\master\Desktop\HELP_DECRYPT.TXT
- “C:\Program Files (x86)\Internet Explorer\iexplore.exe” -nohome
- “C:\Program Files (x86)\Internet Explorer\iexplore.exe” SCODEF:2184 CREDAT:14337

**Files Written:**  
- \Device\KsecDD
- C:\f1f94d81\f1f94d81.exe
- C:\Users\master\AppData\Roaming\f1f94d81.exe
- C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\f1f94d81.exe

**Files Read:**  
- C:\Windows\syswow64\svchost.exe
- C:\Windows\syswow64\vssadmin.exe
How did I know my system was infected?

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
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 *pathToCheck* HashAlgorithm
HashAlgorithm choices: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

```cmd
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.
```

VirusTotal

SHA256: eafe38f481344f23bb9d783fc21c734b2cd37d4a3f37e4a5a282fd739a87316b
File name: d0bfc139.vxe
Detection ratio: 44 / 56
Analysis date: 2015-08-01 10:57:35 UTC (9 months, 2 weeks ago)
What happens on the host from the host point of view
What happens on the host from the host point of view
What happens on the host from the host point of view

C:\> cd c:\f1f94d81

c:\f1f94d81> dir

Volume in drive C has no label.
Volume Serial Number is 1A55-965E

Directory of c:\f1f94d81

07/30/2015  04:00 PM       225,280 f1f94d81.exe

1 File(s)     225,280 bytes
0 Dir(s)     43,187,834,880 bytes free
What happens on the host from the host point of view

**Registry Key**

```
Computer\HKEY_USERS\S-1-5-21-175875322-2898002960-88455520-100 \Software\Microsoft\Windows\CurrentVersion\RunOnce
```

**Registry Values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ab (Default)</td>
<td>REG_SZ</td>
<td>(value not set)</td>
</tr>
<tr>
<td>ab *1f94d8</td>
<td>REG_SZ</td>
<td>C:\f1f94d81\f1f94d81.exe</td>
</tr>
<tr>
<td>ab *1f94d81</td>
<td>REG_SZ</td>
<td>C:\Users\master\AppData\Roaming\f1f94d81.exe</td>
</tr>
</tbody>
</table>
The more you read the angrier you get
How to detect this attack

1. IOC’s
   1. Hashes
   2. Filenames/paths
   3. Registry Values
   4. Network Connections

2. Behaviors
   1. Loading of Dependencies
   2. Process of Execution
   3. 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) = c5d2992c8cba0771f71fe4d7625a0b8b
- 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 fo mklink
  - `cmdline`:""C:\Windows\system32\cmd.exe" /c mklink /D"

- Look for vshadow being run
  - `process_name:vshadow.exe` AND `cmdline`:"-p C:"
Finding Vshadow Being Used

- path:device/harddiskvolumeshadowcopy*
- path:device/harddiskvolume*
Stopping this Ransomware threat

MALWARE

YOU SHALL NOT PASS

Don't Click on any suspicious Links
How to restore files encrypted using Shadow Volume Copies
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
How to prevent this infection

**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.