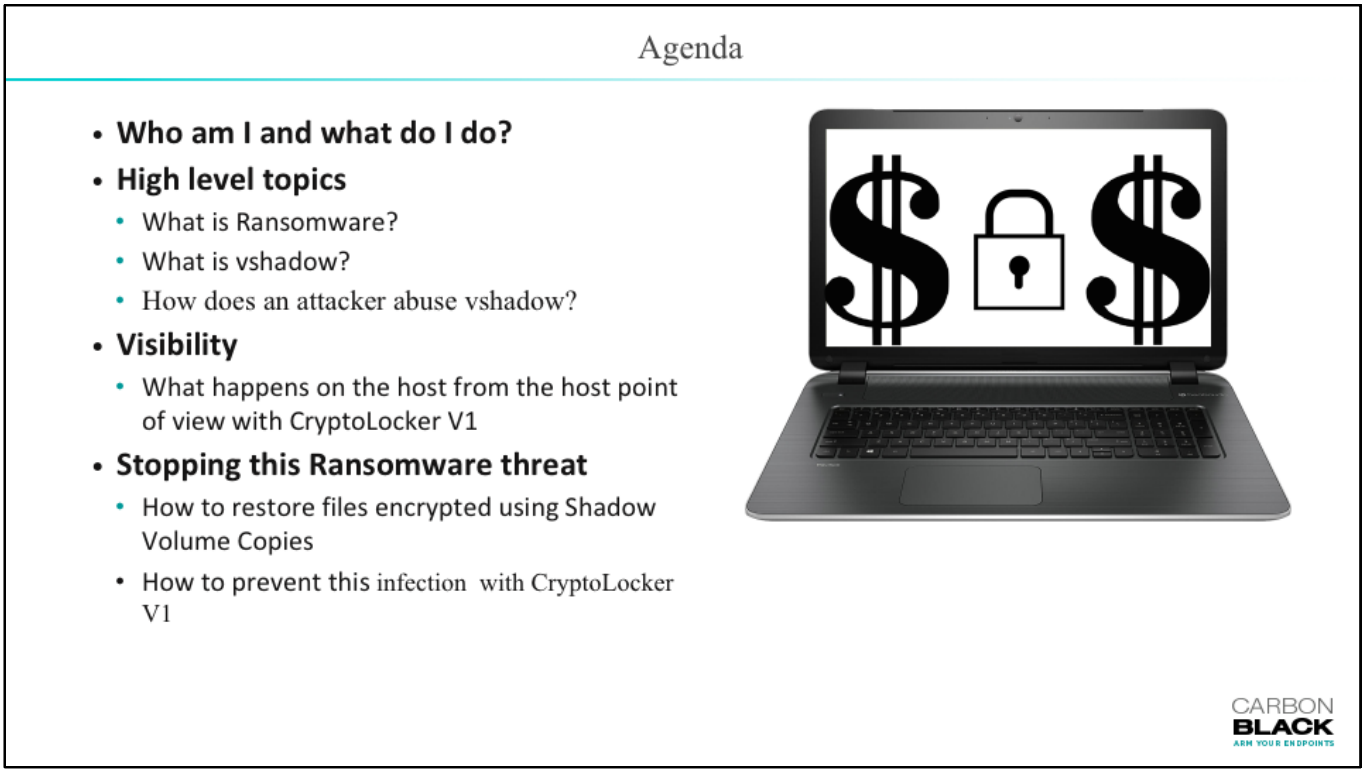
Ransomware Variants Are Lurking “In the V-Shadows”

By Ryan Nolette

The man of many titles

- Security Operations Lead
- Senior Security Engineer
- Senior Threat Researcher
- Incident Response Consultant

CARBON BLACK
ARM YOUR ENDPOINTS



Agenda

- **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

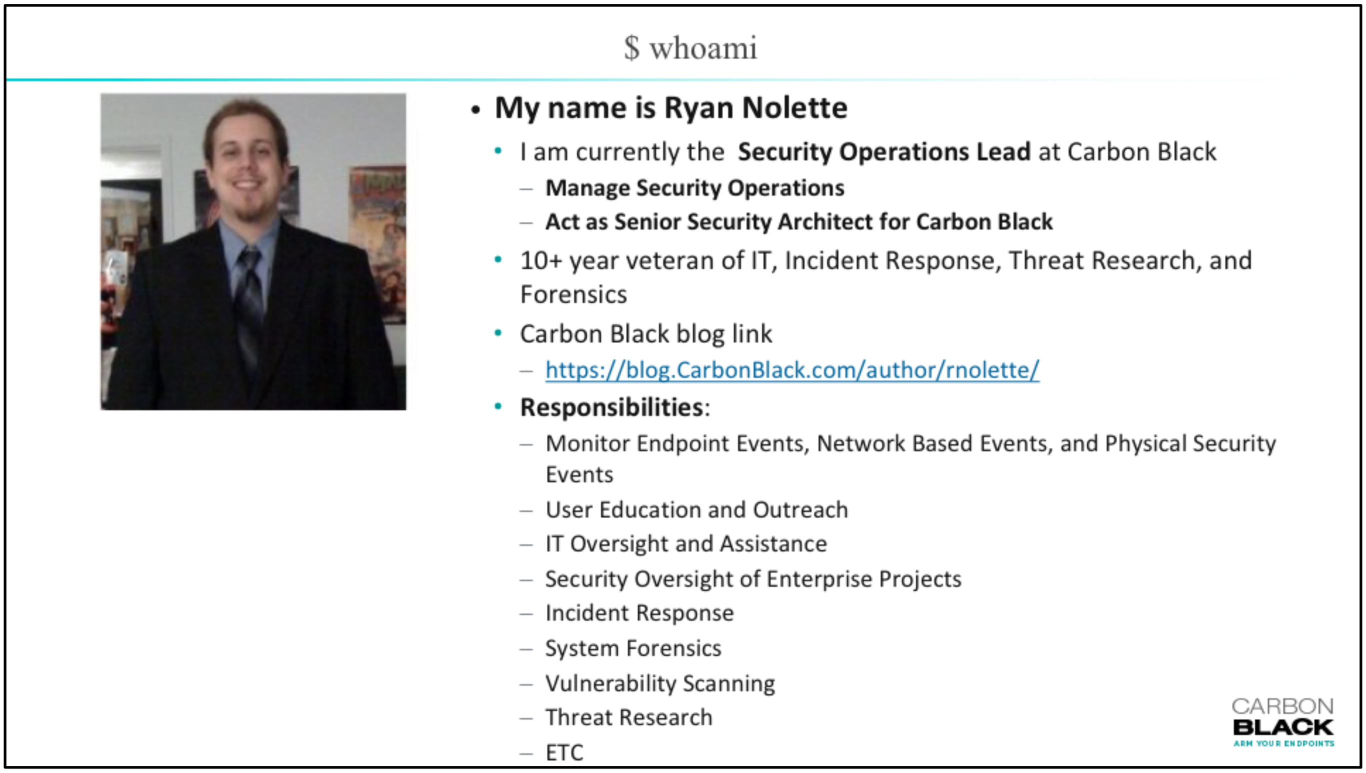
Hello everyone and welcome to my presentation. My name is Ryan Nolette and I currently run Security Operations for Carbon Black. As a disclaimer, I did use Carbon Black's products for this some of the visuals in this presentation but I promise no one in marketing, or HR for that matter, has seen my presentation what I am going to show you today.

Today I would like to talk about how attackers are abusing a legitimate windows utility, called vshadow, to hold your data hostage and how to defend your enterprise from this threat.

I will give you a quick overview of who I am and what I do. Then I will explain at a high level what ransomware is and what these attacks look like on a system. After that, I am going walk you through a growing trend of abusing volume shadow copies on systems to disallow users from restoring from backups. Finally, I will end with ways you can quickly and easily detect and respond to these kinds of attacks. If possible, please hold your questions for the end of the presentation. I cut a bunch of information to make time and if I am unable to get to your question at the end, please find me later on and I will be more than happy to try and answer your additional questions.

The specific variant I will be detailing in this presentation is Cryptolocker version 1. I only have time during this presentation to go in depth for 1 variant and will be focusing on Cryptolocker V1.

<next slide>



$ whoami

- **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
    - https://blog.CarbonBlack.com/author/rnolette/
  - **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

So who am I and why should you bother to pay attention to what I am saying?

I currently run Security Operations at Carbon Black and concentrate on the day to day SOC operations and security solutions required by the business.

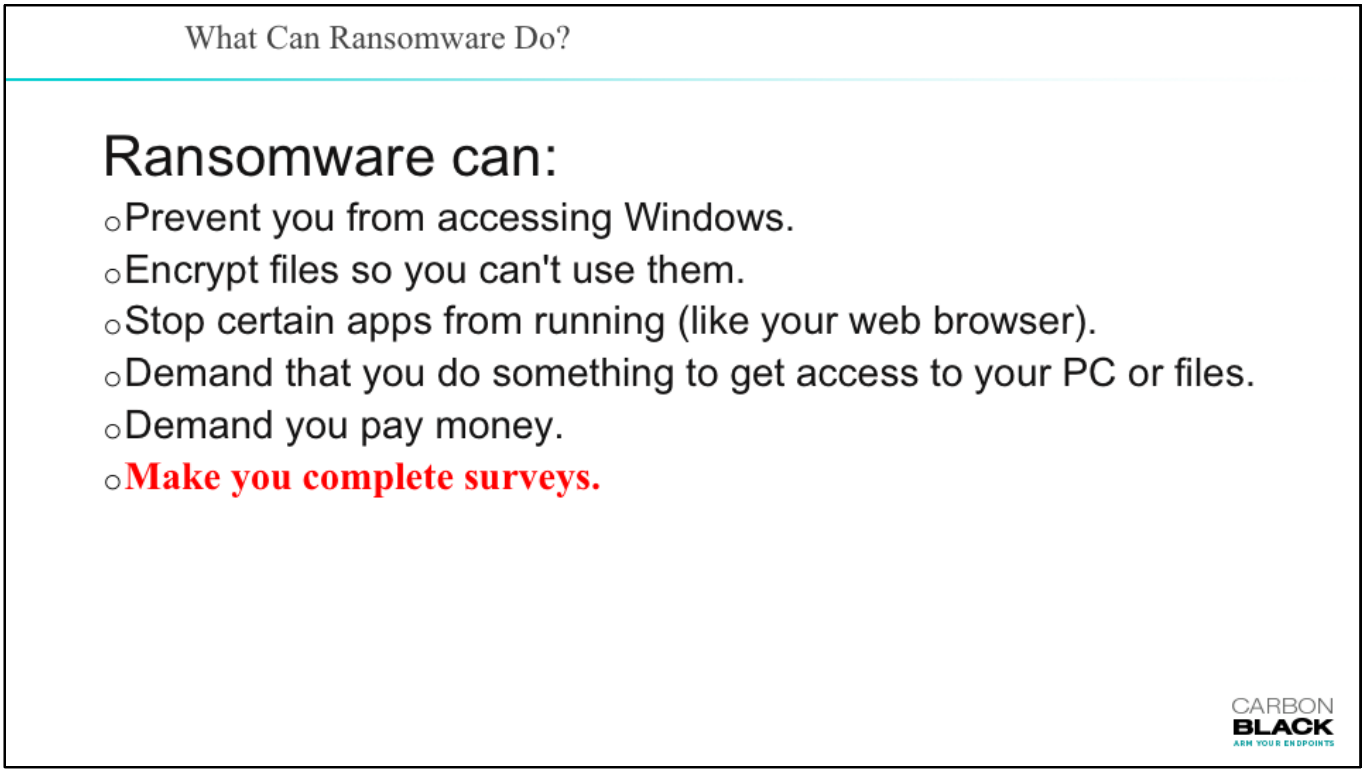
Before I took over SecOps I was a Senior Threat Researcher for Carbon Black and Senior Incident Response Consultant for external clients of Carbon Black.

You can see the long list of high level responsibilities but It can all be summed up pretty quickly... <next slide>

Basically

basically, I make sure that not only do we eat our own dogfood but that we also clean the messes left behind

<wait for laughs to finish then next slide>



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.**

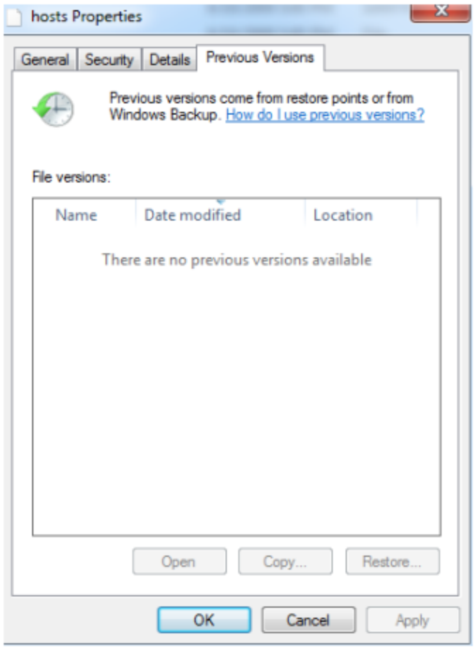
So what is Ransomeware and what can it do? If you type “What is Ransomware” into Google, you get the definition of “a type of malicious software designed to block access to a computer system until a sum of money is paid.” That pretty well sums it up.

The options are pretty numerous to be honest. The most common options are encrypting your files and not allowing you to use your system without paying the ransom.

But by far the most devious and evil thing I have ever seen ransomware do *pause* *click*

Make you complete surveys *shudder*
<next slide>

What is vshadow?



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

File versions:

Name	Date modified	Location
There are no previous versions available		

VShadow is a command-line tool that you can use to create and manage volume shadow copies.

Also known as

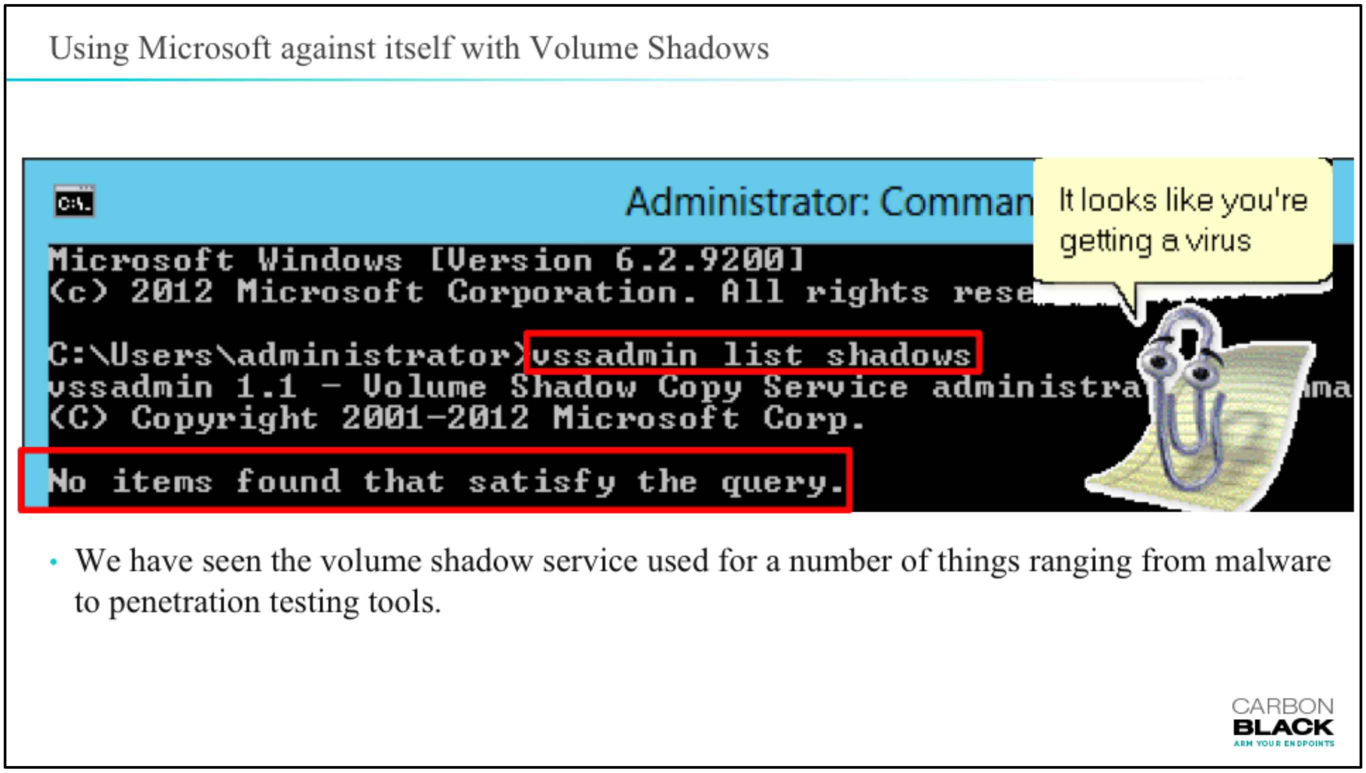
- Shadow Copy
- Volume Snapshot Service
- Volume Shadow Copy Service
- VSS

CARBON BLACK ARM YOUR ENDPOINTS

VShadow is a command-line tool that you can use to create and manage volume shadow copies. Shadow Copy is a technology included in Microsoft Windows that allows the taking of backup copies of computer files or volumes. These backups can be taken even when the files are in use. It is implemented as a Windows service called the “Volume Shadow Copy Service” or “VSS”.

What does that mean? This means the attackers now have a Microsoft signed binary to abuse.

I can see from some of your expressions that you can see why the removing of these files is beneficial to attackers. If you cannot recover from backups, you are at their mercy. <next slide>



Using Microsoft against itself with Volume Shadows

Administrator: Comman

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights rese

C:\Users\administrator>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administra                ma
(C) Copyright 2001-2012 Microsoft Corp.

No items found that satisfy the query.
```

- We have seen the volume shadow service used for a number of things ranging from malware to penetration testing tools.

Some variants of the CryptoLocker ransomware family are known for deleting all volume shadow copies to prevent restoring from backup.
The ransomware does this by executing a delete shadows /all command.

I have observed various techniques utilizing volume shadows. Lately it has been utilized for avoiding detection and for anti-analysis.

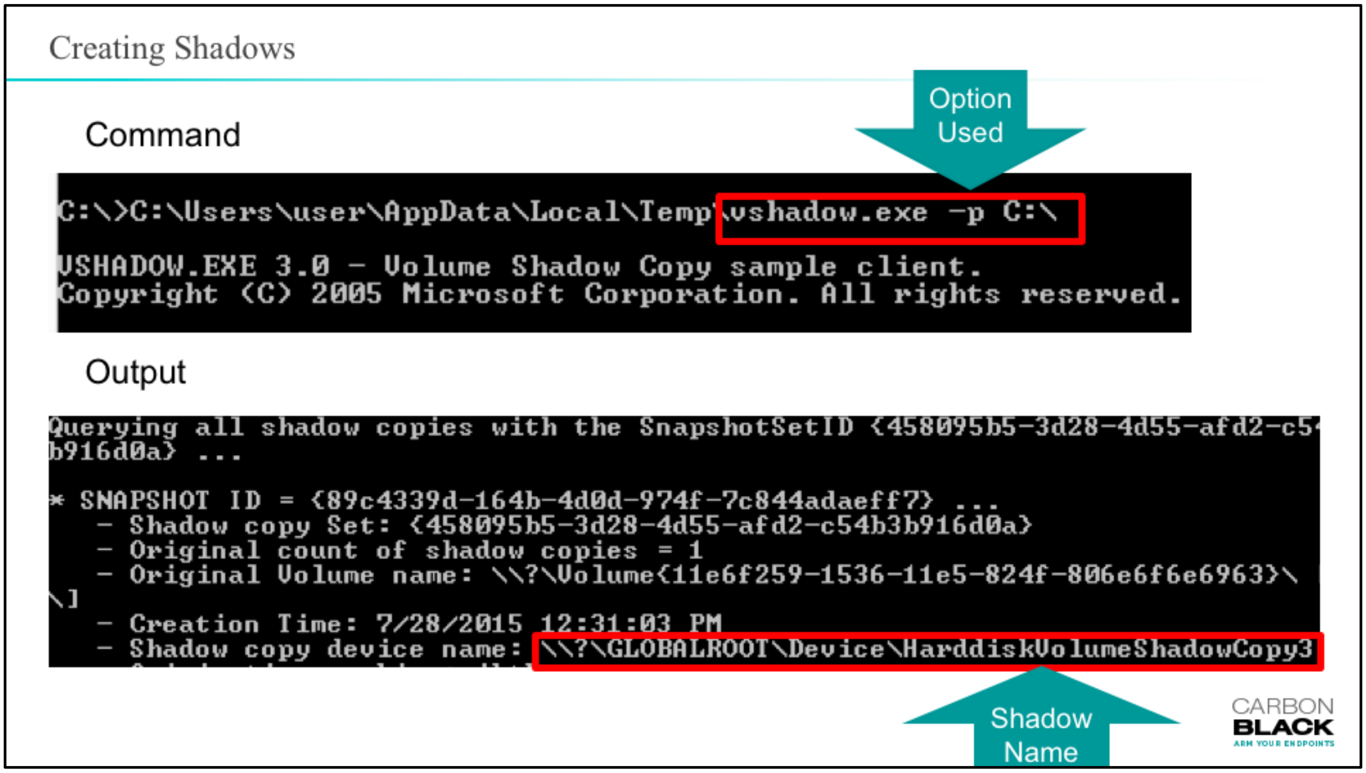
The technique I am going to show you consists of:

1. attackers dropping their malware on the file system via whatever infection mechanism they choose
2. then create a volume shadow
3. “mount” the shadow and execute the malware
4. Then unmount and delete the shadow

What is unique about this technique is that even after the unmounting and deleting of the shadow, the executed malware will still run.

<click>
Now that we have laid some ground work, let’s break something muuuhahahaha

<next slide>



Creating Shadows

Command

Option Used

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

VSHADOW.EXE 3.0 - Volume Shadow Copy sample client.
Copyright (C) 2005 Microsoft Corporation. All rights reserved.
```

Output

```
Querying all shadow copies with the SnapshotSetID {458095b5-3d28-4d55-afd2-c5
b916d0a} ...

* SNAPSHOT ID = {89c4339d-164b-4d0d-974f-7c844adaeff7} ...
   - Shadow copy Set: {458095b5-3d28-4d55-afd2-c54b3b916d0a}
   - 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
```

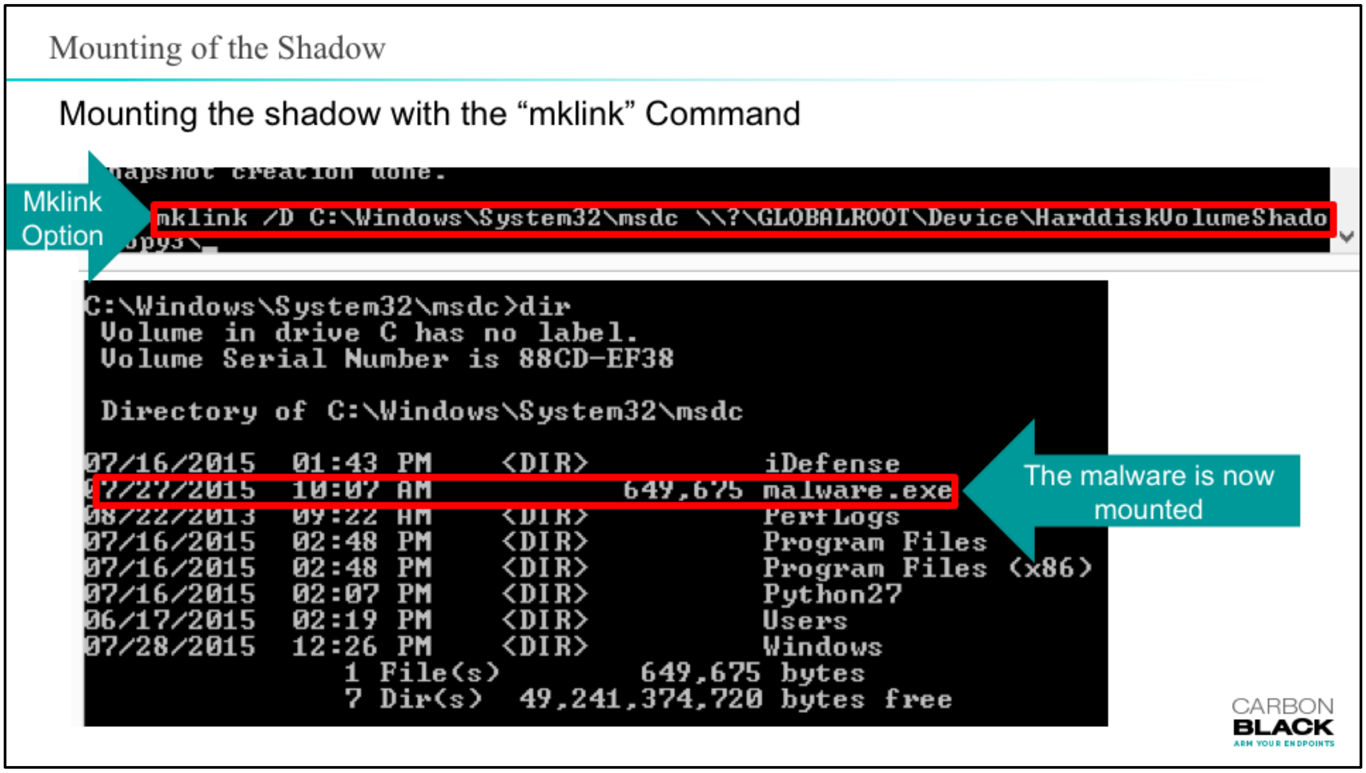
Shadow Name

CARBON BLACK ARM YOUR ENDPOINTS

On Windows XP, the Vssadmin tool doesn't have the ability to create persistent shadows on the system. Starting with the Windows Vista SDK, Microsoft supplied a binary called Vshadow to allow this.

Once the Vshadow executable is on the victim, attackers can use it to create a persistent shadow. And by persistent, I mean survives between reboots. To create a persistent shadow attackers utilize the "-p" option and point it toward the location on the file system they want to create a shadow of.

In the above example, the attackers are creating a persistent shadow of the full C: drive. This will run for a few seconds and end with the output seen above.
Keep note of the "Shadow copy device name."
(\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3) as it will be used to mount the shadow in the following attack
<next slide>



Mounting of the Shadow

Mounting the shadow with the “mklink” Command

Mklink Option

```
napshot creation done.
mklink /D C:\Windows\System32\msdc \\?\GLOBALROOT\Device\HarddiskVolumeShado
opy3\_
```

```
C:\Windows\System32\msdc>dir
 Volume in drive C has no label.
 Volume Serial Number is 88CD-EF38

 Directory of C:\Windows\System32\msdc

07/16/2015  01:43 PM    <DIR>          iDefense
7/27/2015   10:07 AM           649,675 malware.exe
08/22/2013  09:22 AM    <DIR>          PerfLogs
07/16/2015  02:48 PM    <DIR>          Program Files
07/16/2015  02:48 PM    <DIR>          Program Files (x86)
07/16/2015  02:07 PM    <DIR>          Python27
06/17/2015  02:19 PM    <DIR>          Users
07/28/2015  12:26 PM    <DIR>          Windows
               1 File(s)        649,675 bytes
               7 Dir(s)  49,241,374,720 bytes free
```

The malware is now mounted

Now that the shadow with the malware has been created, it must be mounted. This is done using the “mklink” command.

Here the attackers are creating a symbolic link directory in System32 to a directory called “msdc.” The symlink directory points to the shadow copy of the C drive created earlier.

The malware was placed at the root of the shadow after it was created. A directory listing of C:\Windows\System32\msdc reveals the malware on the normal filesystem but living inside the shadow filesystem.

Once the symlink has been created the contents of the shadow are accessible via normal file system operations like the directory listing we did above.
<next slide>

Starting the Malware

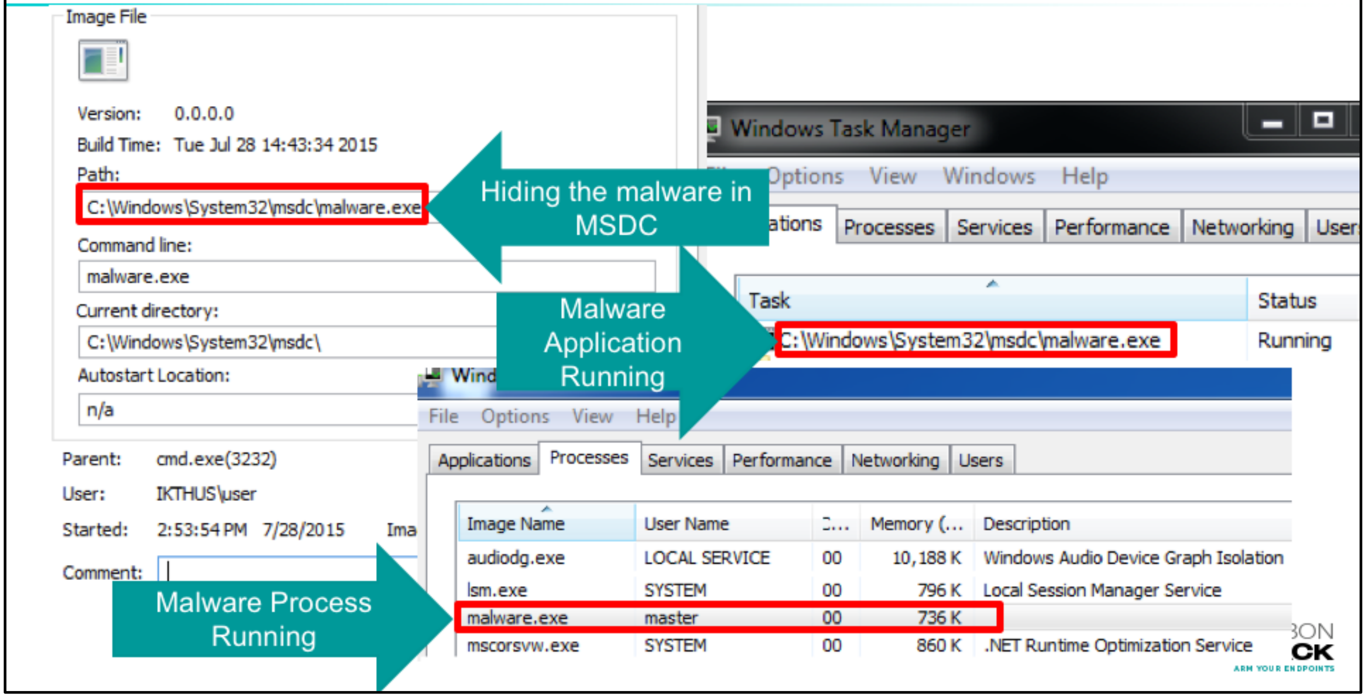


Image File

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\

Autostart Location:

n/a

Parent: cmd.exe(3232)

User: IKTHUS\user

Started: 2:53:54 PM 7/28/2015

Comment:

Hiding the malware in MSDC

Malware Application Running

Malware Process Running

Task	Status
C:\Windows\System32\msdc\malware.exe	Running

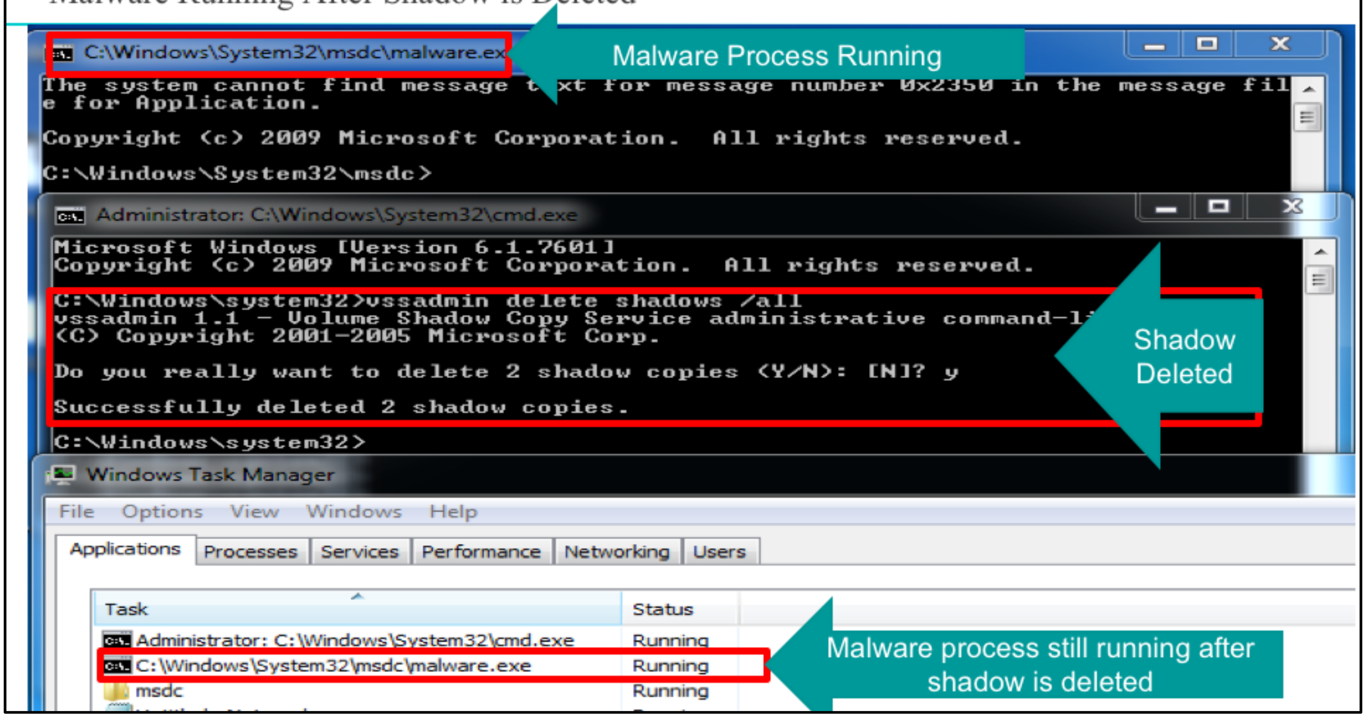
Image Name	User Name	C...	Memory (...	Description
audiodg.exe	LOCAL SERVICE	00	10,188 K	Windows Audio Device Graph Isolation
lsm.exe	SYSTEM	00	796 K	Local Session Manager Service
malware.exe	master	00	736 K	
mscorsvw.exe	SYSTEM	00	860 K	.NET Runtime Optimization Service

Once the file system setup is in place, the malware is started just like any other executable.

When the malware is started and shown in a tool like process explorer it shows that it is running from C:\Windows\System32\msdc

that path doesnt look too suspicious at first glance does it?
<next slide>

Malware Running After Shadow is Deleted



C:\Windows\System32\msdc\malware.ex
Malware Process Running
Administrator: C:\Windows\System32\cmd.exe
Shadow Deleted
Windows Task Manager
File Options View Windows Help
Applications Processes Services Performance Networking Users
Malware process still running after shadow is deleted

```
The system cannot find message text for message number 0x2350 in the message fil
e for Application.

Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32\msdc>
```

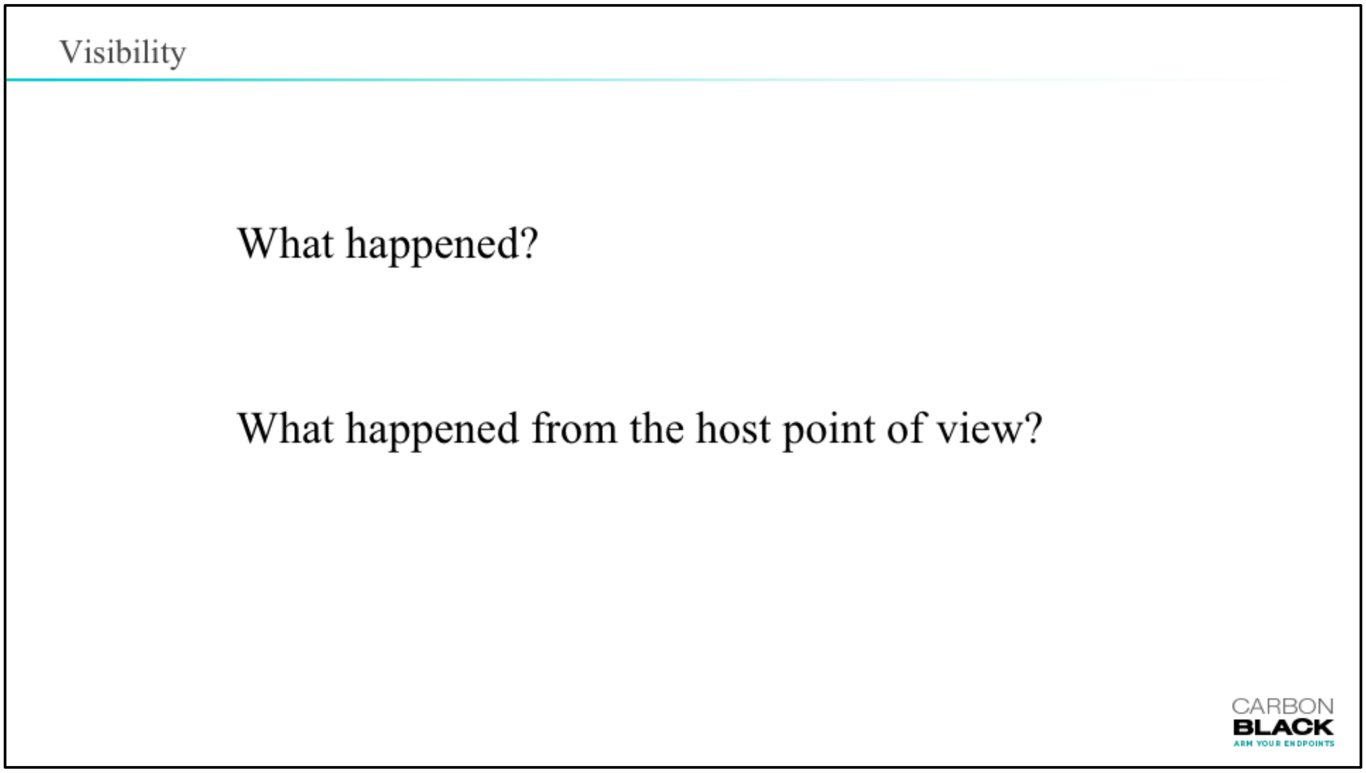
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>vssadmin delete shadows /all
vssadmin 1.1 - Volume Shadow Copy Service administrative command-li
(C) Copyright 2001-2005 Microsoft Corp.

Do you really want to delete 2 shadow copies (Y/N): [N]? y

Successfully deleted 2 shadow copies.

C:\Windows\system32>
```

Task	Status
Administrator: C:\Windows\System32\cmd.exe	Running
C:\Windows\System32\msdc\malware.exe	Running
msdc	Running

Once the malware is started, the attackers can unmount and delete the shadow and the malware continues to run.

the attacker wants to remove as much forensic evidence as possible so they would unmount the directory and delete the shadow with Vssadmin

As demonstrated, this technique is a nice hiding mechanism that throws in a little anti-forensics with it.
<next slide>



Visibility

What happened?

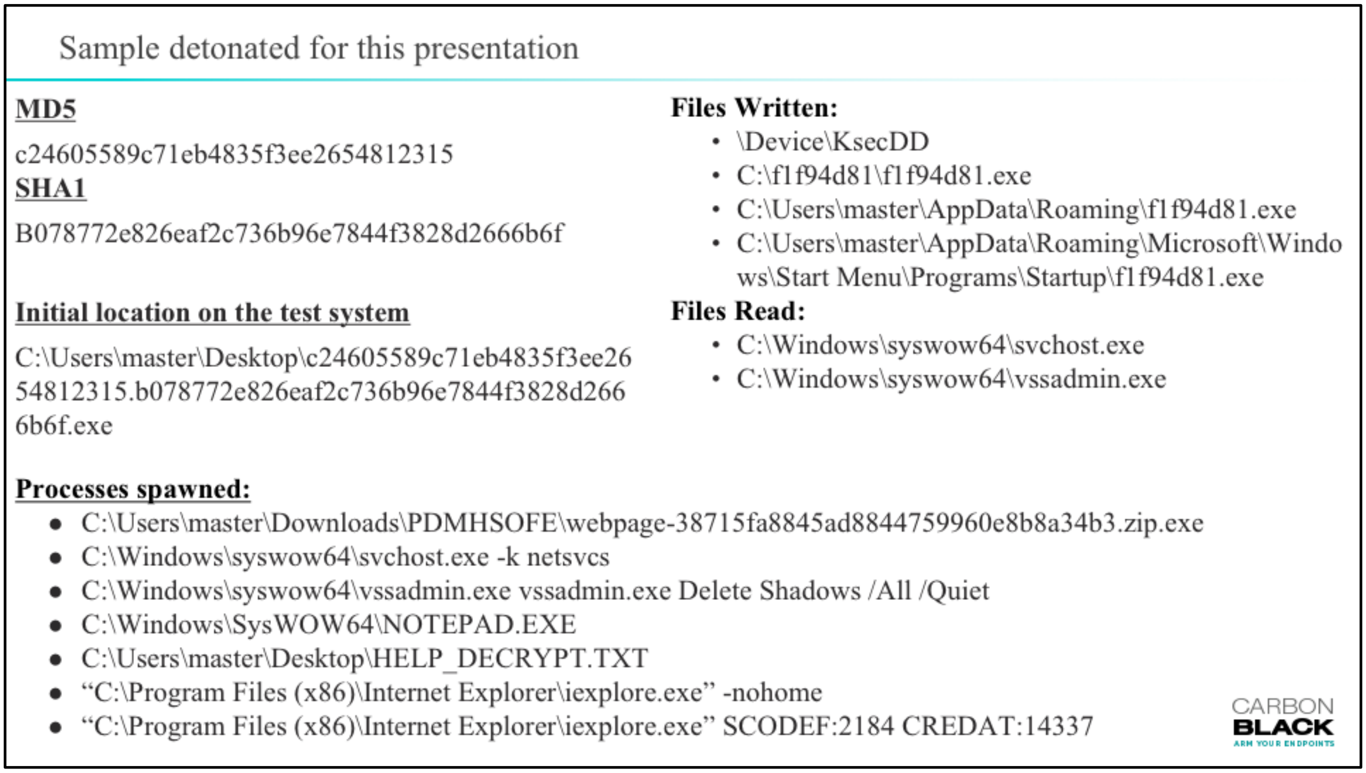
What happened from the host point of view?

CARBON
BLACK
ARM YOUR ENDPOINTS

Now that we have gone over a high level explanation of Ransomeware and the recent examples of abusing vshadow, let's talk about visibility.

Visibility is a key requirement of detection and preventions. I like to say, if you can't see it, how can you alert on it? And If you can't alert on it, how can you stop it?

Let's answer a few questions:
What really happened on the host?
What happens on the host from the host point of view?
<next slide>



Sample detonated for this presentation

MD5

c24605589c71eb4835f3ee2654812315

SHA1

B078772e826eaf2c736b96e7844f3828d2666b6f

Initial location on the test system

C:\Users\master\Desktop\c24605589c71eb4835f3ee2654812315.b078772e826eaf2c736b96e7844f3828d2666b6f.exe

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

Processes spawned:

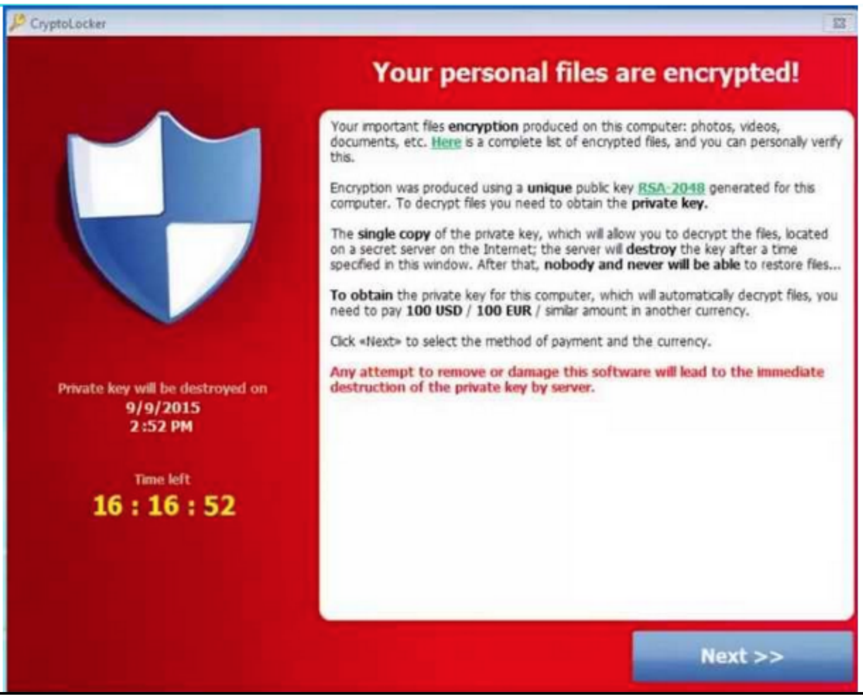
- C:\Users\master\Downloads\PDMHSOFE\webpage-38715fa8845ad8844759960e8b8a34b3.zip.exe
- C:\Windows\syswow64\svchost.exe -k netsvcs
- C:\Windows\syswow64\vssadmin.exe vssadmin.exe Delete Shadows /All /Quiet
- C:\Windows\SysWOW64\NOTEPAD.EXE
- C:\Users\master\Desktop\HELP_DECRYPT.TXT
- “C:\Program Files (x86)\Internet Explorer\iexplore.exe” -nohome
- “C:\Program Files (x86)\Internet Explorer\iexplore.exe” SCODEF:2184 CREDAT:14337

No you do not have to memorize this slide…..but there will be a test later…

Since we detonated this malware on purpose in a sandbox, we already know what to look for based on the original filename. In the real world, we don’t have that luxury.

<next slide>

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.

Private key will be destroyed on
9/9/2015
2:52 PM

Time left
16 : 16 : 52

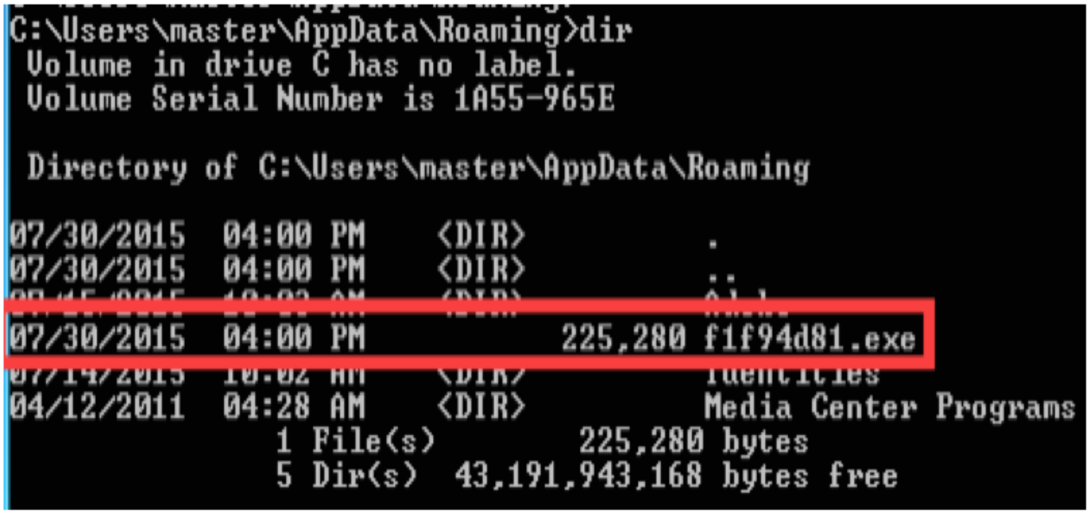
This was my first hint that the infection worked. Unfortunately the AV installed on the demo system didn’t catch it even though virustotal shows that my vendor had a signature for this malware.

Speaking of virustotal…
<next slide>

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
```



```
C:\Users\master\AppData\Roaming>dir
 Volume in drive C has no label.
 Volume Serial Number is 1A55-965E

 Directory of C:\Users\master\AppData\Roaming

07/30/2015  04:00 PM    <DIR>          .
07/30/2015  04:00 PM    <DIR>          ..
07/30/2015  04:00 PM           225,280 f1f94d81.exe
07/14/2015  10:02 AM    <DIR>          Identities
04/12/2011  04:28 AM    <DIR>          Media Center Programs
               1 File(s)        225,280 bytes
               5 Dir(s)  43,191,943,168 bytes free
```

CARBON BLACK
ARM YOUR ENDPOINTS

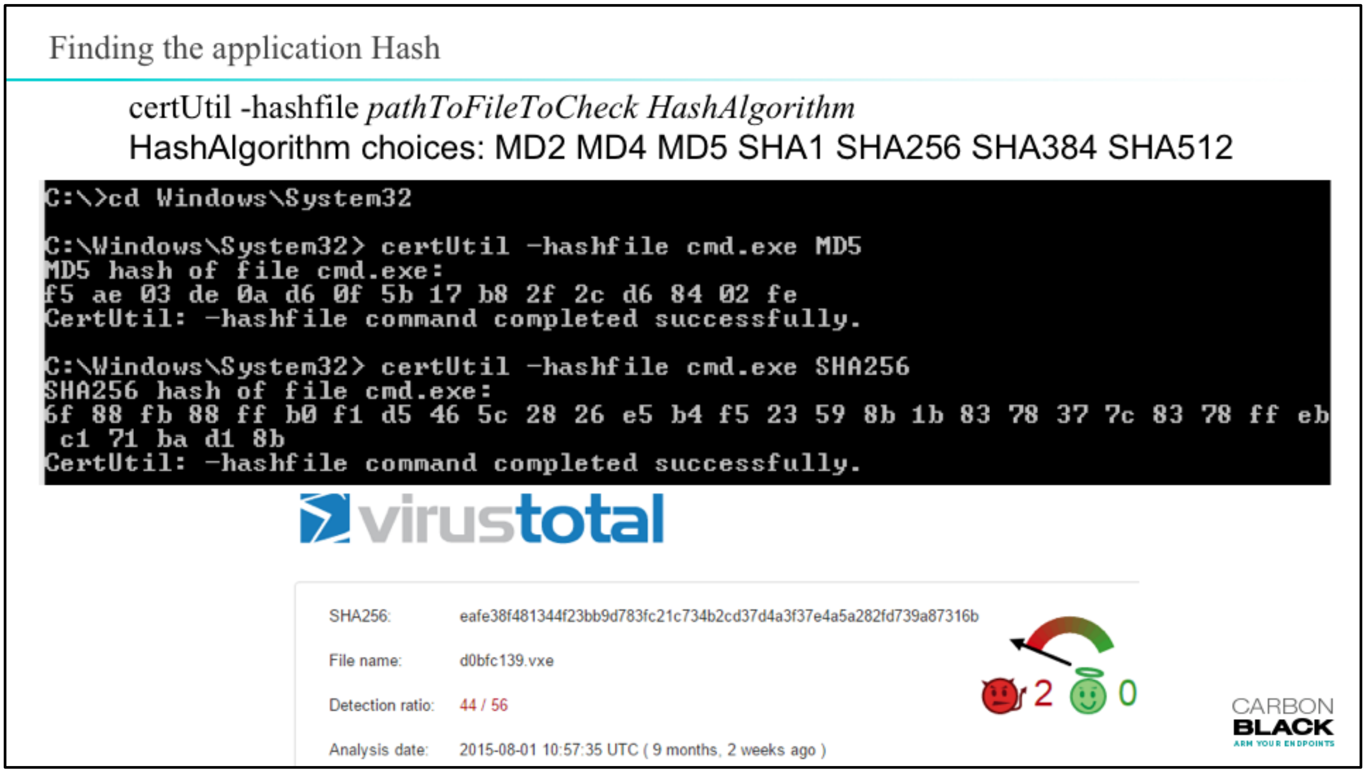
The first thing this malware does is delete itself from the original location it was executed from and create a new binary in the user's appdata roaming directory.

How do I know this? Because on the suspected compromised computer I ran a powershell query to find all new files created in the past 24 hours.

From this list I was able to quickly find randomly generated executable files in strange directories like appdata.

This is extremely common among Trojan malwares and is the first place I check for newly created directories and binaries because it is so common.

<next slide>



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.
```

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)

CARBON BLACK
ARM YOUR ENDPOINTS

While in the process of researching different ways to hash files, I discovered that windows has a native hashing feature built into certUtil.

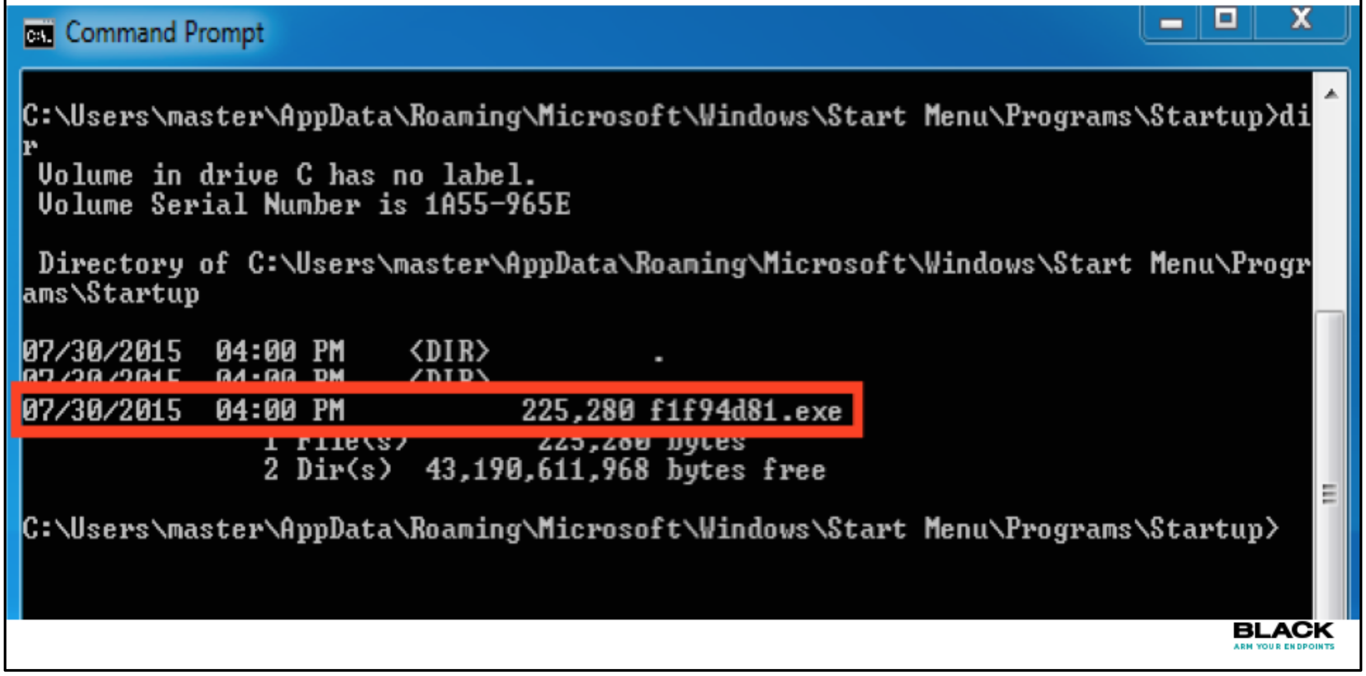
Using this tool I can programmatically hash every file on a system and then upload that hash list to virustotal for a quick check for known malware.

When I did this for the binary, I found that it has a virustotal score of 44/56.

We should probably look into what this binary did right?

<next slide>

What happens on the host from the host point of view



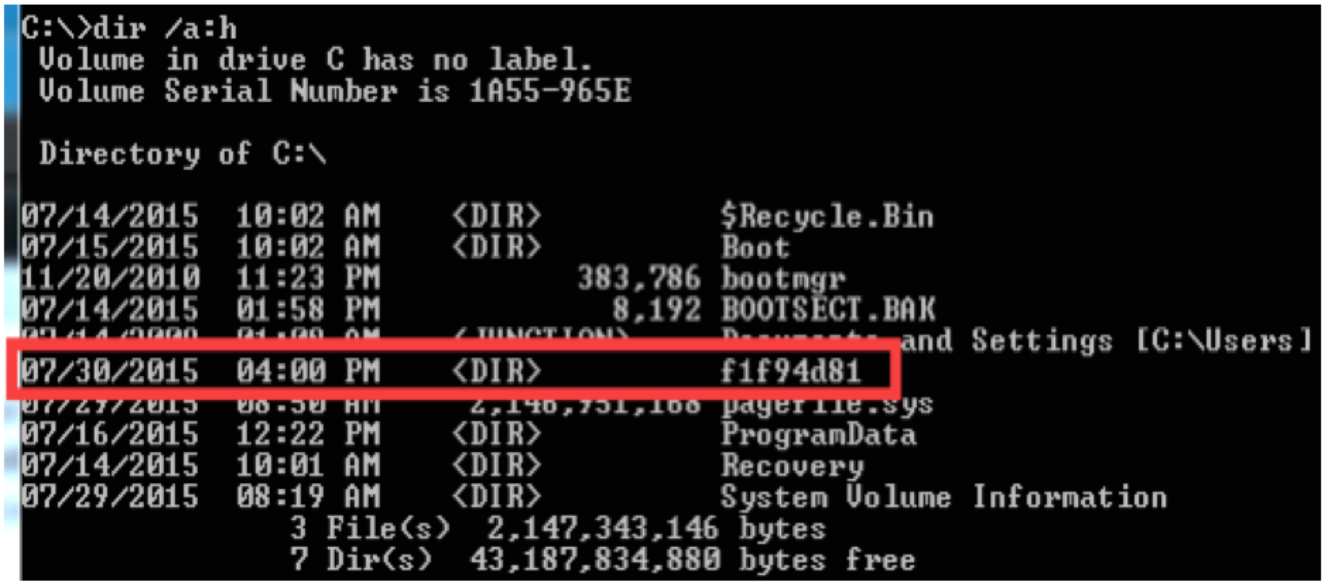
```
C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>di
r
 Volume in drive C has no label.
 Volume Serial Number is 1A55-965E

 Directory of C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Progr
ams\Startup

07/30/2015  04:00 PM    <DIR>          .
07/30/2015  04:00 PM    <DIR>          ..
07/30/2015  04:00 PM           225,280 f1f94d81.exe
               1 File(s)        225,280 bytes
               2 Dir(s)  43,190,611,968 bytes free

C:\Users\master\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

Next the malware creates a persistence mechanism by copying itself to the user's startup programs directory.

This is a common technique and is a location that should always be checked for new binaries.

<next slide>

What happens on the host from the host point of view



```
C:\>dir /a:h
 Volume in drive C has no label.
 Volume Serial Number is 1A55-965E

 Directory of C:\

07/14/2015  10:02 AM    <DIR>          $Recycle.Bin
07/15/2015  10:02 AM    <DIR>          Boot
11/20/2010  11:23 PM           383,786 bootmgr
07/14/2015  01:58 PM             8,192 BOOTSECT.BAK
07/14/2009  01:08 AM    <JUNCTION>     Documents and Settings [C:\Users]
07/30/2015  04:00 PM    <DIR>          f1f94d81
07/29/2015  08:30 AM     2,146,951,168 pagefile.sys
07/16/2015  12:22 PM    <DIR>          ProgramData
07/14/2015  10:01 AM    <DIR>          Recovery
07/29/2015  08:19 AM    <DIR>          System Volume Information
               3 File(s)  2,147,343,146 bytes
               7 Dir(s)  43,187,834,880 bytes free
```

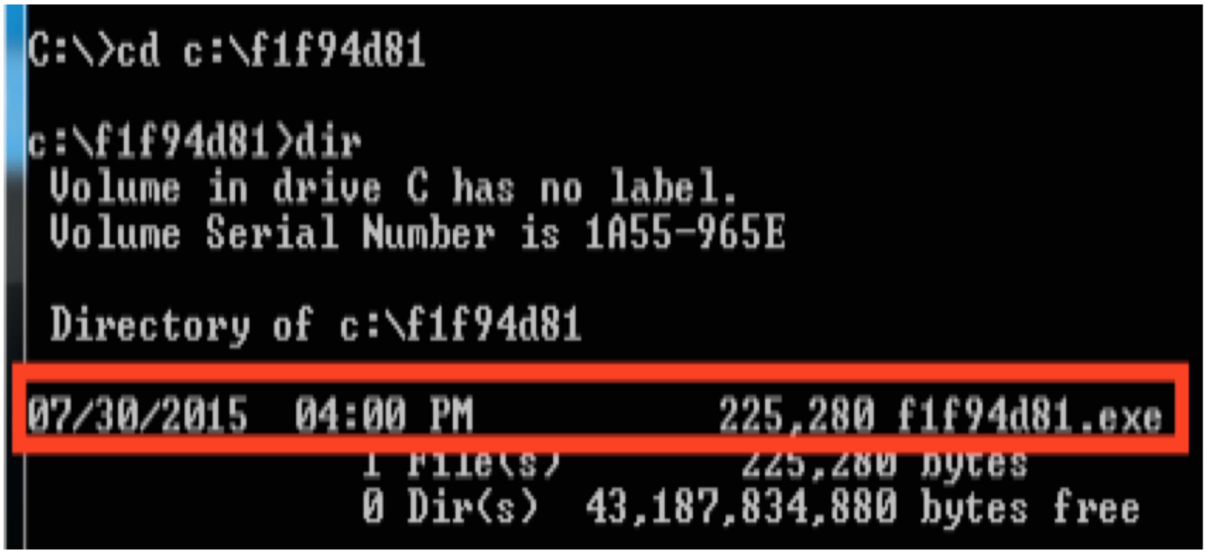
CARBON BLACK
ARM YOUR ENDPOINTS

The third action this malware takes is to create a hidden folder in the root directory of the files system.

You can see that the folder was created within seconds of the original binary being deleted and the other two binaries being written to the filesystem.

<next slide>

What happens on the host from the host point of view

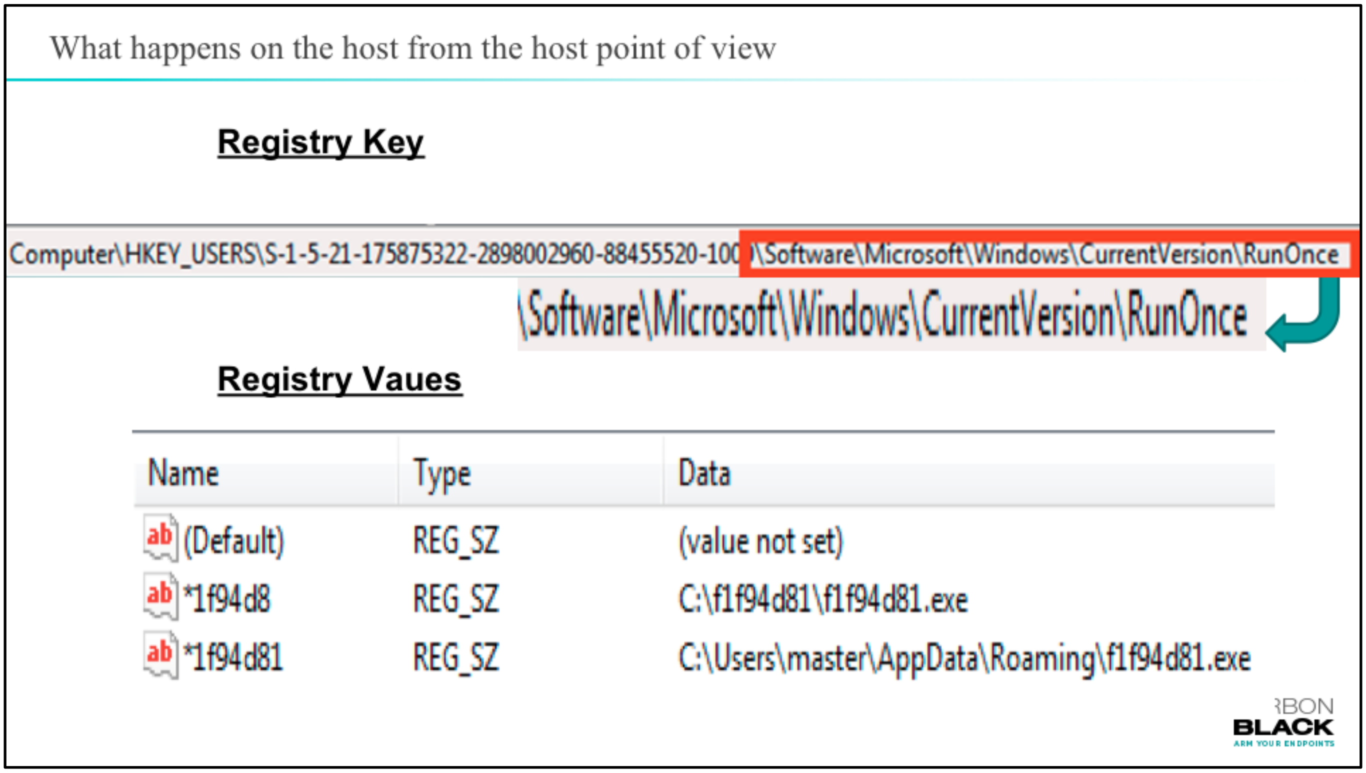


```
C:\>cd c:\f1f94d81

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
```

Inside this new file is yet another copy of the binary.

It seems like the malware author is afraid of these binaries being found and creates backup plans for their backup plans.

That kind of paranoia isn't healthy.
<next slide>



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
```

```
\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Registry Vaues

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab *1f94d8	REG_SZ	C:\f1f94d81\f1f94d81.exe
ab *1f94d81	REG_SZ	C:\Users\master\AppData\Roaming\f1f94d81.exe

Next up, the malware starts creating registry values so it can be started in the background each time the user logs in.

I can infer their intent because the “Run” and “RunOnce” keys are run each time a new user logs in and would start this malware again upon login.

These keys are for background services such as remote registry service and are run only once per boot.
<next slide>

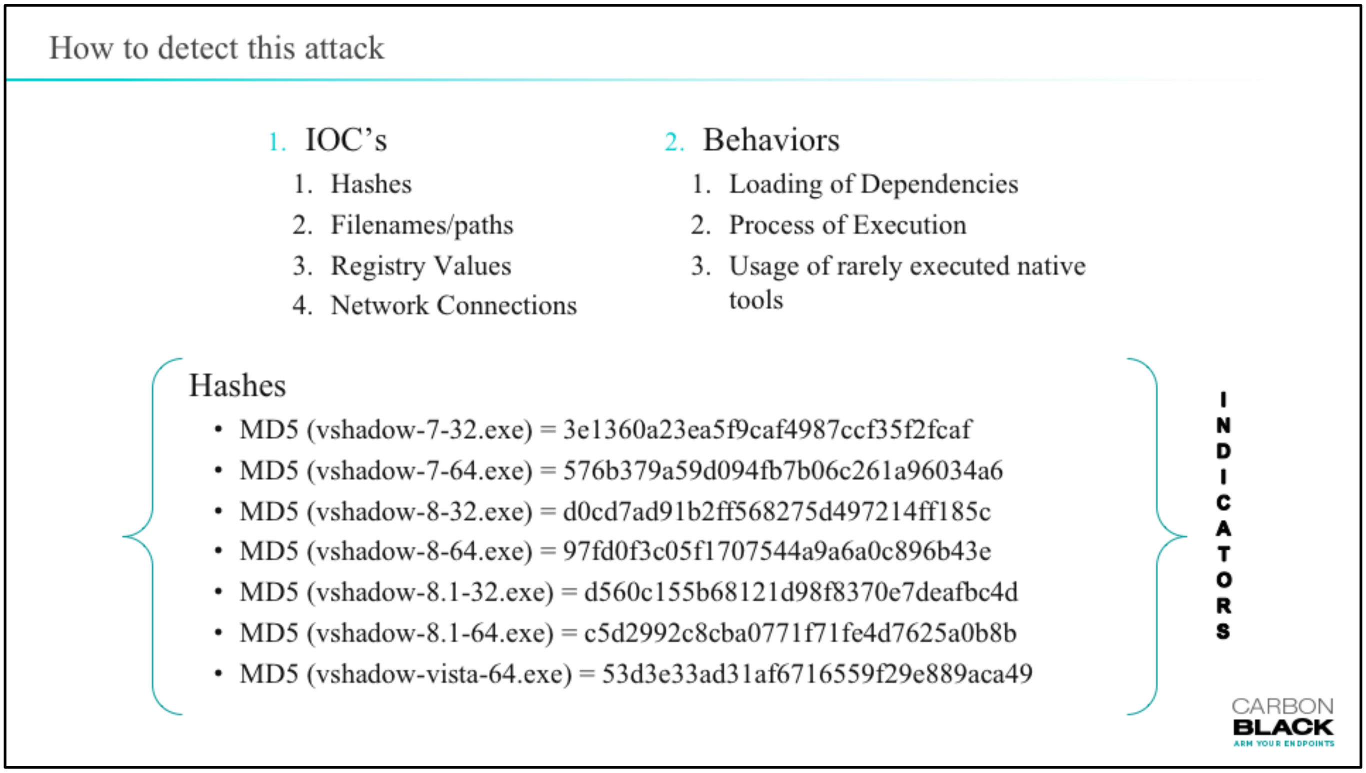
The more you read the angrier you get

My Computer\HKEY_CURRENT_USER\Software\CryptoLocker\Files

CARBON BLACK
ARM YOUR ENDPOINTS

This is what I have been referring to as the “pissed list” because the longer the list, the more you're pissed.

<next slide>



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

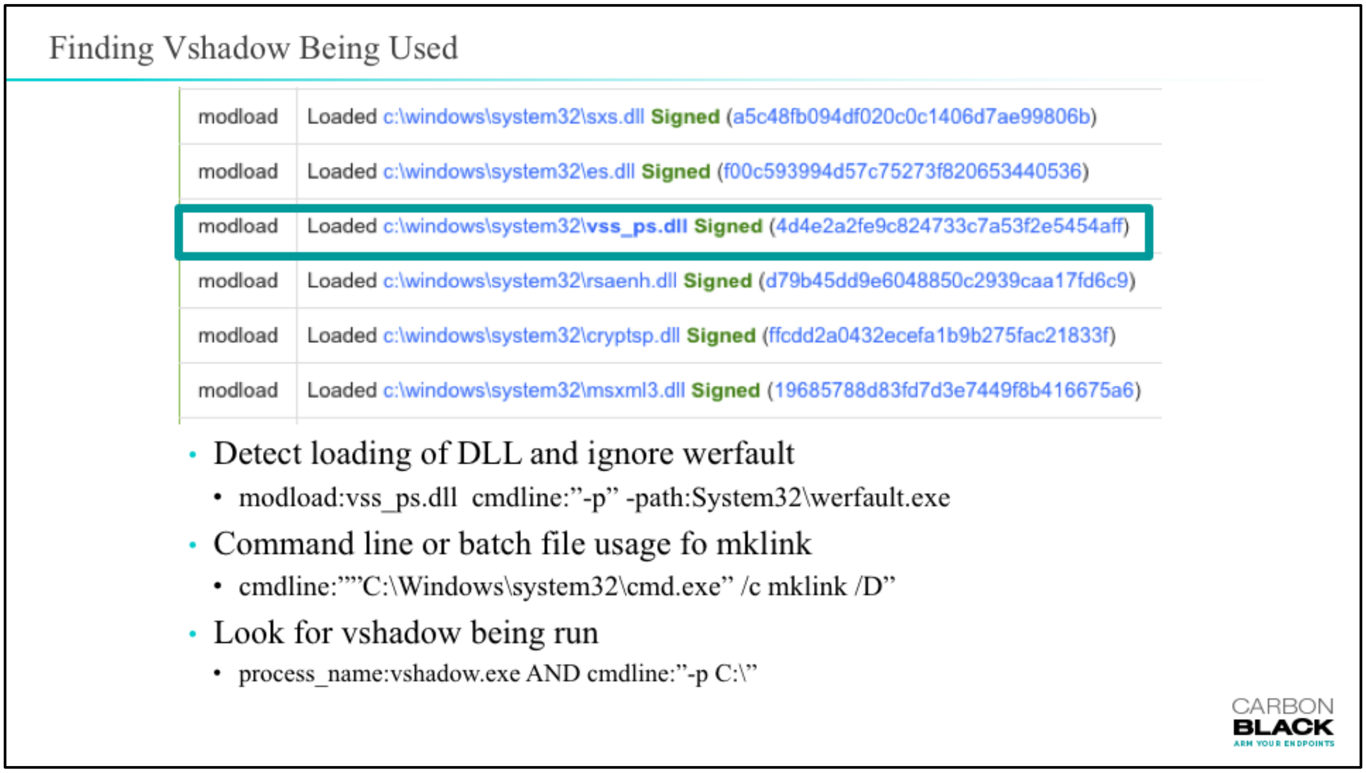
Hashes

- 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

Next question is “how do I detect this type of attack?”

I tried to stick to indicators that could be used in various tools.

Our first method for finding use of the Vshadow tool is looking for hashes. Each version of the SDK will have the Vshadow tool in it and will have an x86 and 64bit version.
<next slide>



Finding Vshadow Being Used

modload	Loaded c:\windows\system32\sxs.dll **Signed** (a5c48fb094df020c0c1406d7ae99806b)
modload	Loaded c:\windows\system32\es.dll **Signed** (f00c593994d57c75273f820653440536)
modload	Loaded c:\windows\system32**vss_ps.dll** **Signed** (4d4e2a2fe9c824733c7a53f2e5454aff)
modload	Loaded c:\windows\system32\rsaenh.dll **Signed** (d79b45dd9e6048850c2939caa17fd6c9)
modload	Loaded c:\windows\system32\cryptsp.dll **Signed** (ffcdd2a0432ecefa1b9b275fac21833f)
modload	Loaded c:\windows\system32\msxml3.dll **Signed** (19685788d83fd7d3e7449f8b416675a6)

- 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:\"

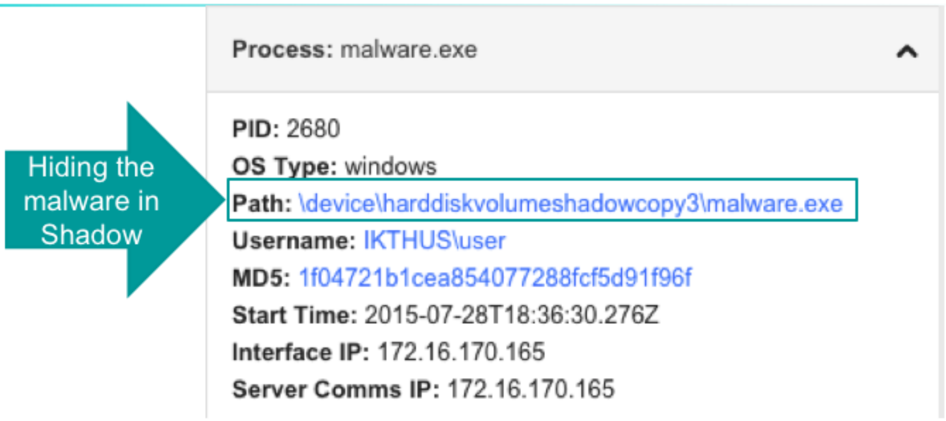
CARBON BLACK ARM YOUR ENDPOINTS

If we look a little closer at the vshadow.exe process we can see it loads a few modules that don't normally get loaded. One in particular that we are looking for is vss_ps.dll, which is a necessary component of the Volume Shadow Storage feature. I figured this out by googling vshadow.exe and the MSDN site listed it as a dependency.

In a 3,000-host environment, that query came back with only one process that matches the criteria. The process is the Windows process werfault.exe. So we can refine the query to ignore this process.

One caveat I found while researching this is the command "mklink" is a function of cmd.exe. Because of this, it is going to be hard for some IR tools to detect. luckily the tool I was using can see the command line and can detect this as written in the fourth query
<next slide>

Finding Vshadow Being Used



Hiding the malware in Shadow

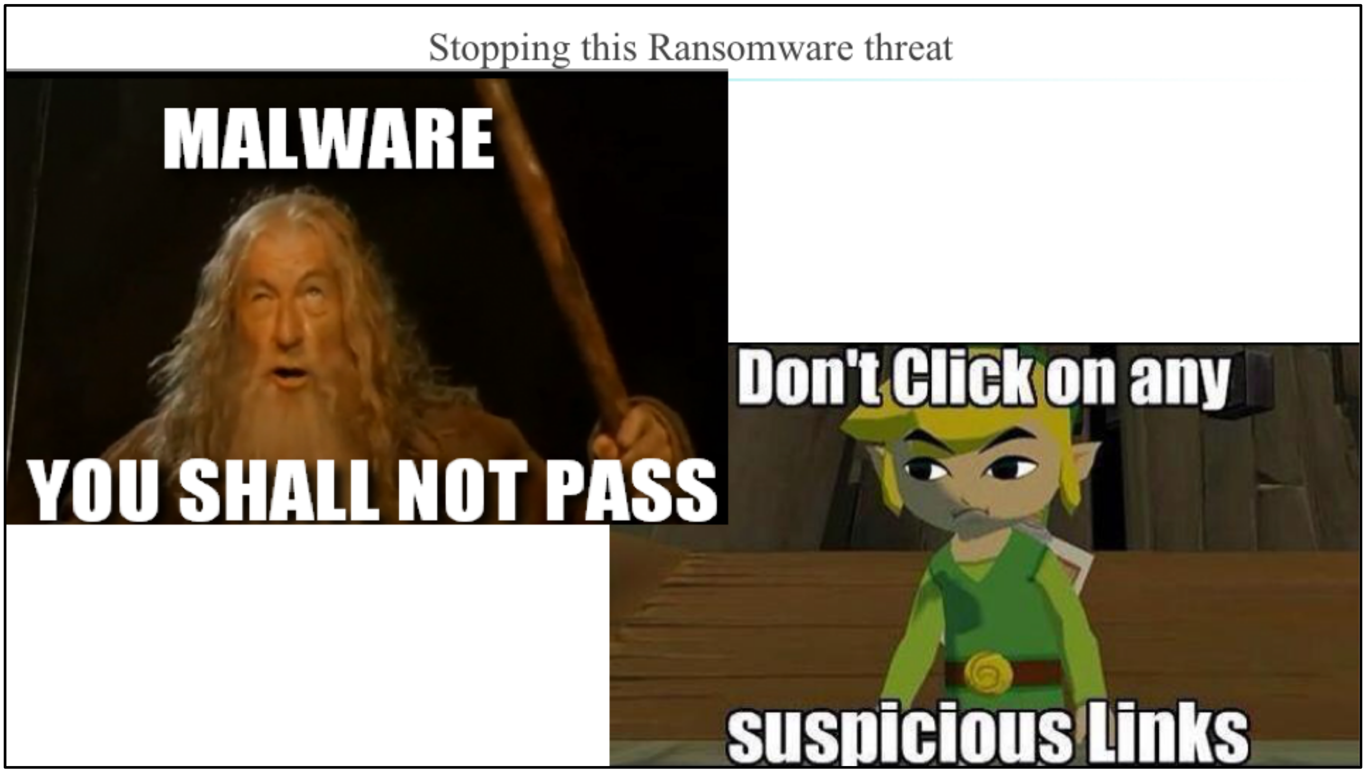
Process: malware.exe

PID: 2680
OS Type: windows
Path: \device\harddiskvolumeshadowcopy3\malware.exe
Username: IKTHUS\user
MD5: 1f04721b1cea854077288fcf5d91f96f
Start Time: 2015-07-28T18:36:30.276Z
Interface IP: 172.16.170.165
Server Comms IP: 172.16.170.165

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

When taking a closer look at the malware.exe process we can see that the true file system path is \Device\harddiskvolumeshadowcopy3\malware.exe

This means we can flag this malware being executed from the volume shadow, along with other processes being run from locations that have “device/harddiskvolume” in the path.
<next slide>

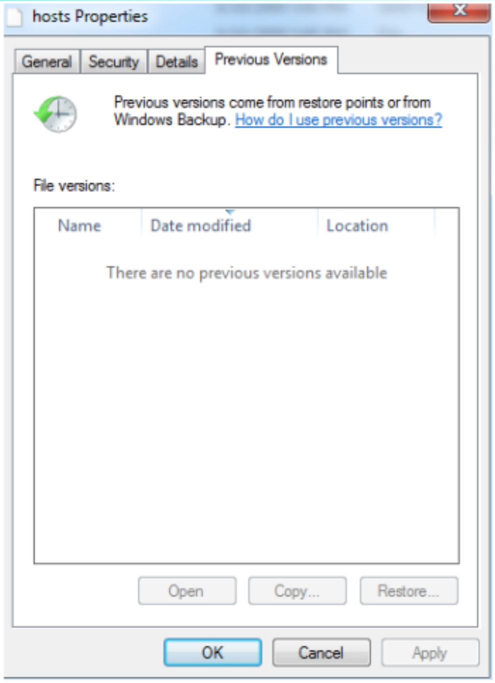


Stopping this Ransomware threat

Let’s talk about how to defend against this type of Ransomware
<click>

<next slide>

How to restore files encrypted using Shadow Volume Copies



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

There are no previous versions available

CARBON BLACK ARM YOUR ENDPOINTS

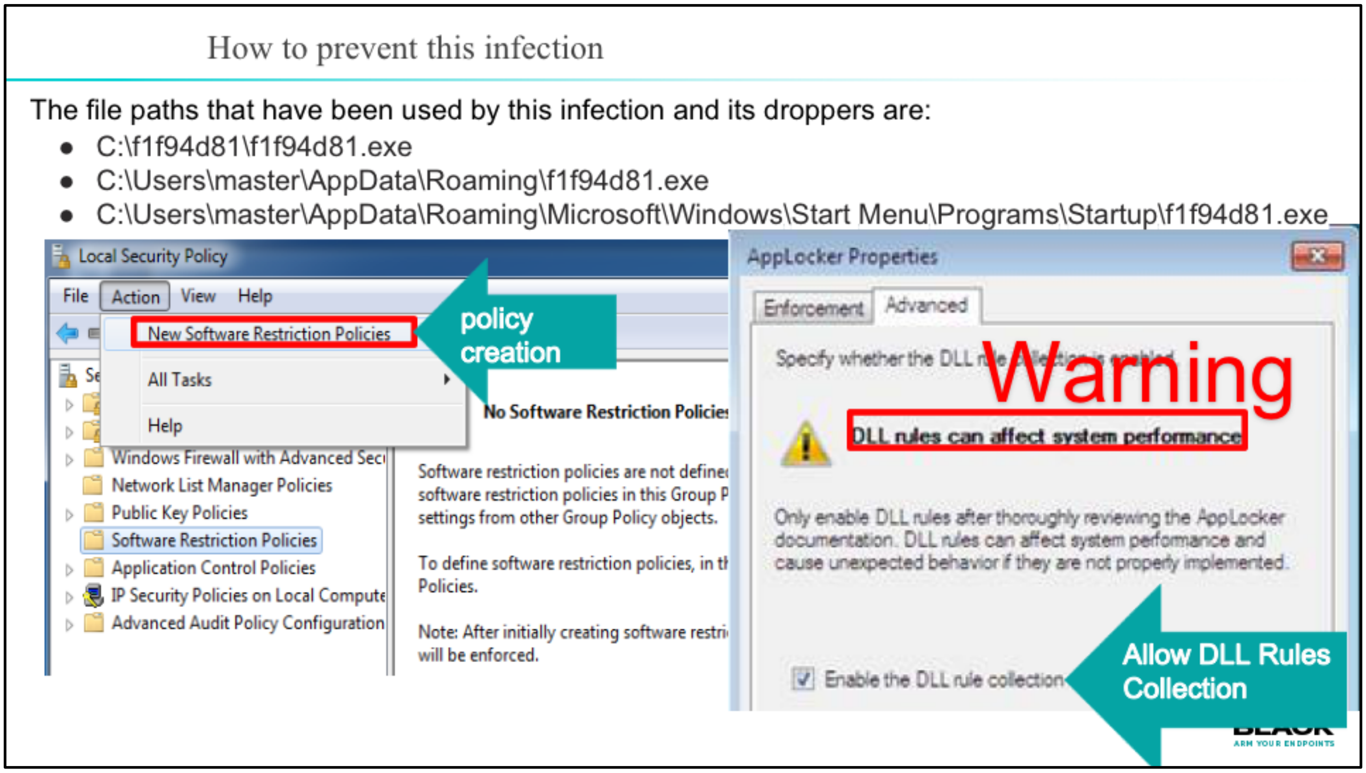
If you have “System Restore” enabled, your system will create shadow copies that hold copies of your files from that moment back.

These copies “may,” and I use the term “may” dripping with hope, allow you to restore your files from before they were encrypted.

Using shadow copies is not foolproof and the version of the files in the shadow copy may not be the latest version and could be useless to you.

The method I normally use is the native Windows option because it has the most probability of being available to me on a supported Windows system.

If possible, use whitelisting on any system you can. This will prevent the execution of any unknown binary.
<next slide>



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

Local Security Policy
File
Action
View
Help
New Software Restriction Policies
All Tasks
Help
Se
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
policy creation
No Software Restriction Policies
AppLocker Properties
Enforcement
Advanced
Warning
Allow DLL Rules Collection
ARM YOUR ENDPOINTS

Software restriction policies are not define software restriction policies in this Group P settings from other Group Policy objects.

To define software restriction policies, in th Policies.

Note: After initially creating software restri will be enforced.

Specify whether the DLL rule collection is enabled.

DLL rules can affect system performance

Only enable DLL rules after thoroughly reviewing the AppLocker documentation. DLL rules can affect system performance and cause unexpected behavior if they are not properly implemented.

☑ Enable the DLL rule collection

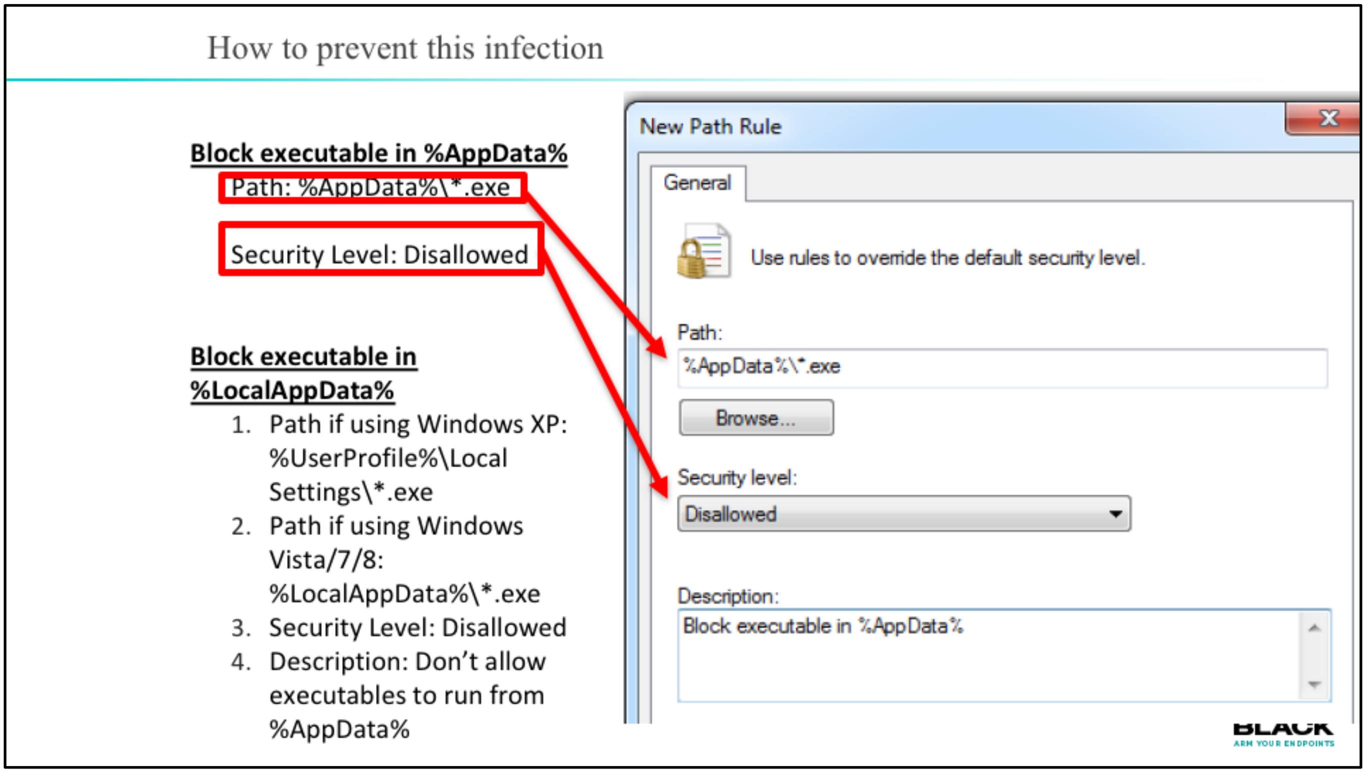
You can create a software restriction policy for a single computer using the Local Security Policy Editor or for an entire domain use the Group Policy Editor

Fun Fact: you can use applocker to enforce DLL's as well as binaries.
Second Fun Fact: stick to just binaries if you can because this will degrade system performance and that makes users very sad pandas.

The DLL Rules Collection

The DLL rules collection is used to block applications that call specific DLL files.
This is an advanced rule collection and should not be used unless you are certain you know what you are doing.
This type of rule can also severely impact system performance as it requires AppLocker to check every DLL an application uses when it initializes.
The DLL rules collection is not enabled by default due to the reasons mentioned above. If you want to create a DLL rule you can do so be going to the main AppLocker configuration screen, choosing Configure Rule Enforcement, selecting the Advanced tab, and placing a check mark next to the Enable the DLL rule collection option. After doing this you will see the DLL rule collection in the left pane alone with the three other rule collections.

<next slide>



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%

New Path Rule

Use rules to override the default security level.

Path: %AppData%*.exe

Security level: Disallowed

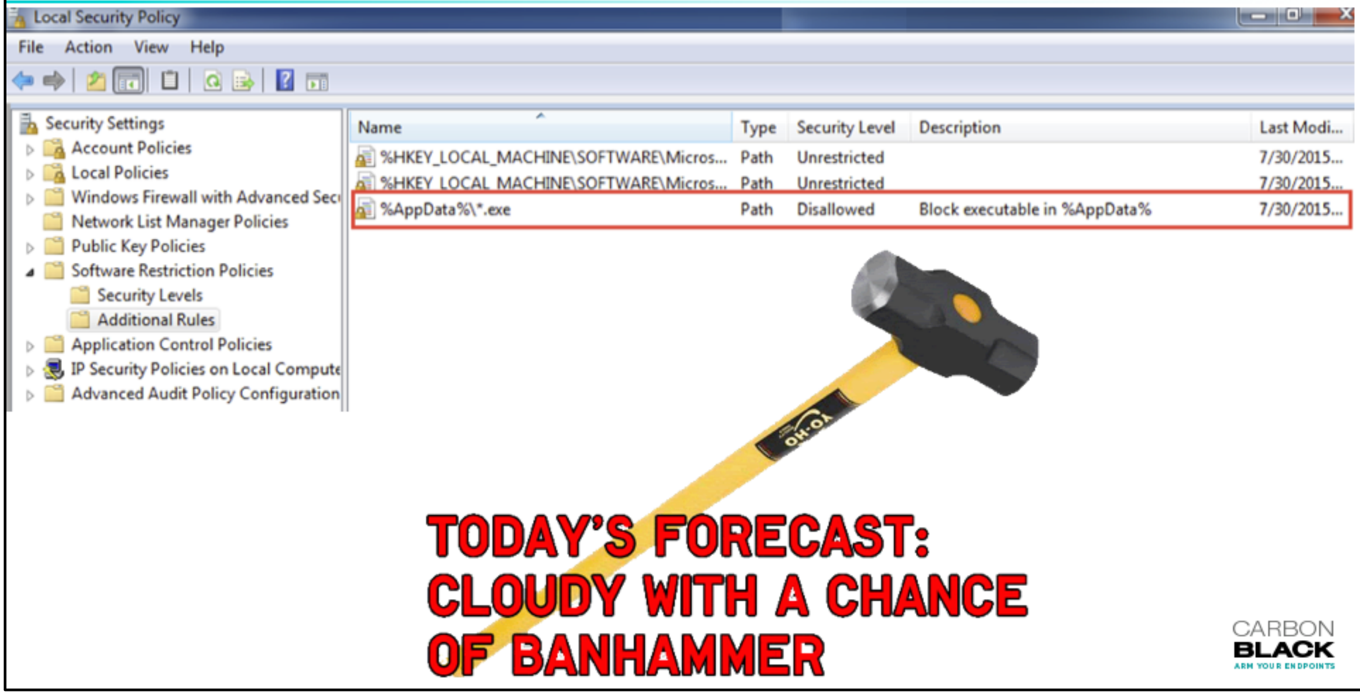
Description: Block executable in %AppData%

The software restriction policies can cause issues when trying to run legitimate applications from weird locations. For them, you will need to add exception rules.

There is some trial and error here since this enforcement technique is the equivalent of trying to open a jar of pickles with a sledgehammer.

Applications like Chrome and Spotify are known to use AppData or a child directory of appdata for update binaries. So beware of collateral damage.
<next slide>

How to prevent this infection

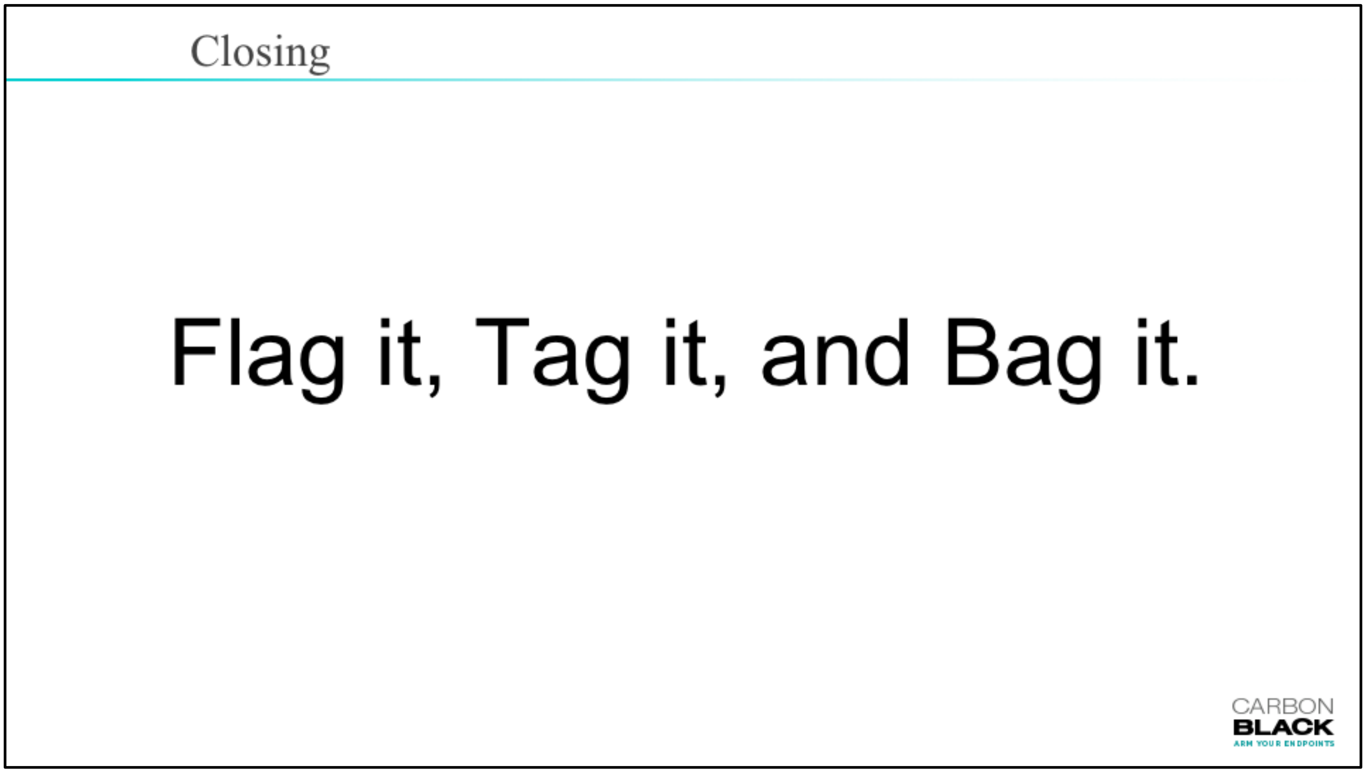


- Security Settings
  - Account Policies
  - Local Policies
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
    - Security Levels
    - Additional Rules
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Name	Type	Security Level	Description	Last Modi...
%HKEY_LOCAL_MACHINE\SOFTWARE\Micros...	Path	Unrestricted		7/30/2015...
%HKEY_LOCAL_MACHINE\SOFTWARE\Micros...	Path	Unrestricted		7/30/2015...
%AppData%*.exe	Path	Disallowed	Block executable in %AppData%	7/30/2015...

CARBON BLACK
ARM YOUR ENDPOINTS

Save the rule and drop that ban hammer
<next slide>



Closing

Flag it, Tag it, and Bag it.

CARBON
BLACK
ARM YOUR ENDPOINTS

In closing, Ransomware is annoyingly effective.

The recent additions of features such as removing shadow copies makes it even more dangerous.

Regardless of what security products you use, your best defense to any attack is user training and backups.

Anything preventative you can implement proactively, whether it’s automated tools or a manual implementation is going to help protect you and your company.

Thank you fall for your time today and until next time, remember my motto: “Flag it, Tag it and Bag it.”
<next slide>