Finding, Hunting, and Eradicating It

crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/

Jai Minton December 22, 2020

In this blog, we take a look at a recent incident that involved a persistent browser hijacking rootkit dubbed "Spicy Hot Pot." The name comes from Huorong (Tinder) Security, which first publicly reported on its discovery of this rootkit. Spicy Hot Pot is a browser hijacking rootkit that changes a user's homepage to point to a page controlled by the malware operator, in addition to uploading memory dumps from a machine to a predefined server and incorporating a local update feature to ensure it can remain updated. Usually a browser hijacker would do this through malicious executables or registry keys that change the user's homepage; however, Spicy Hot Pot takes this one step further by using two kernel-mode drivers that are dropped to disk and installed during the infection process to remain stealthy.

These kernel drivers have a number of functions, such as hindering security software by intercepting their callback functions, collecting any memory dumps created on the system from a specific directory, and giving the malware operator the ability to update the malware as they see fit. In addition, one of the kernel drivers acts as a minifilter, which gives it the ability to intercept and modify any user input or output requests. One of the functions of this driver is to intercept any attempts by a user to display the malicious files, effectively making them invisible.

This particular piece of malware is primarily focused on Chinese users. This is inferred based on 1) it was found dropped from a number of keygen/activation tools used to "crack" or illegitimately activate Microsoft products that are developed with Chinese language packs, and 2) this malware is specifically targeting

common antivirus software used in China. Although more can be said about this piece of malware, this blog post aims to give a quick overview of Spicy Hot Pot, its capabilities and how it can be manually removed from a host without the need for third-party software.

The Initial Detection

In June 2020, the CrowdStrike Falcon Complete™ team received a machine learning (ML) alert that a suspicious binary called “baofeng15.0” attempted to run in a customer’s environment. This had the below SHA256 hash:

```
498ed725195b5ee52e406de237afa9ef268cabc4ef604c363aee2e78b3b13193
```

After analyzing this binary, the determination was made that it is bundled with a browser hijacking rootkit. This rootkit is known to date back as early as December 2019 and remains prevalent with new variants being discovered to date.

Starting with dynamic analysis of the binary in question, it was revealed that it dropped nine items of interest (seven executables and two filter drivers) before disabling hibernation mode on the machine. A recreation of this activity after disabling preventions can be seen below using CrowdStrike Falcon’s process execution tree.

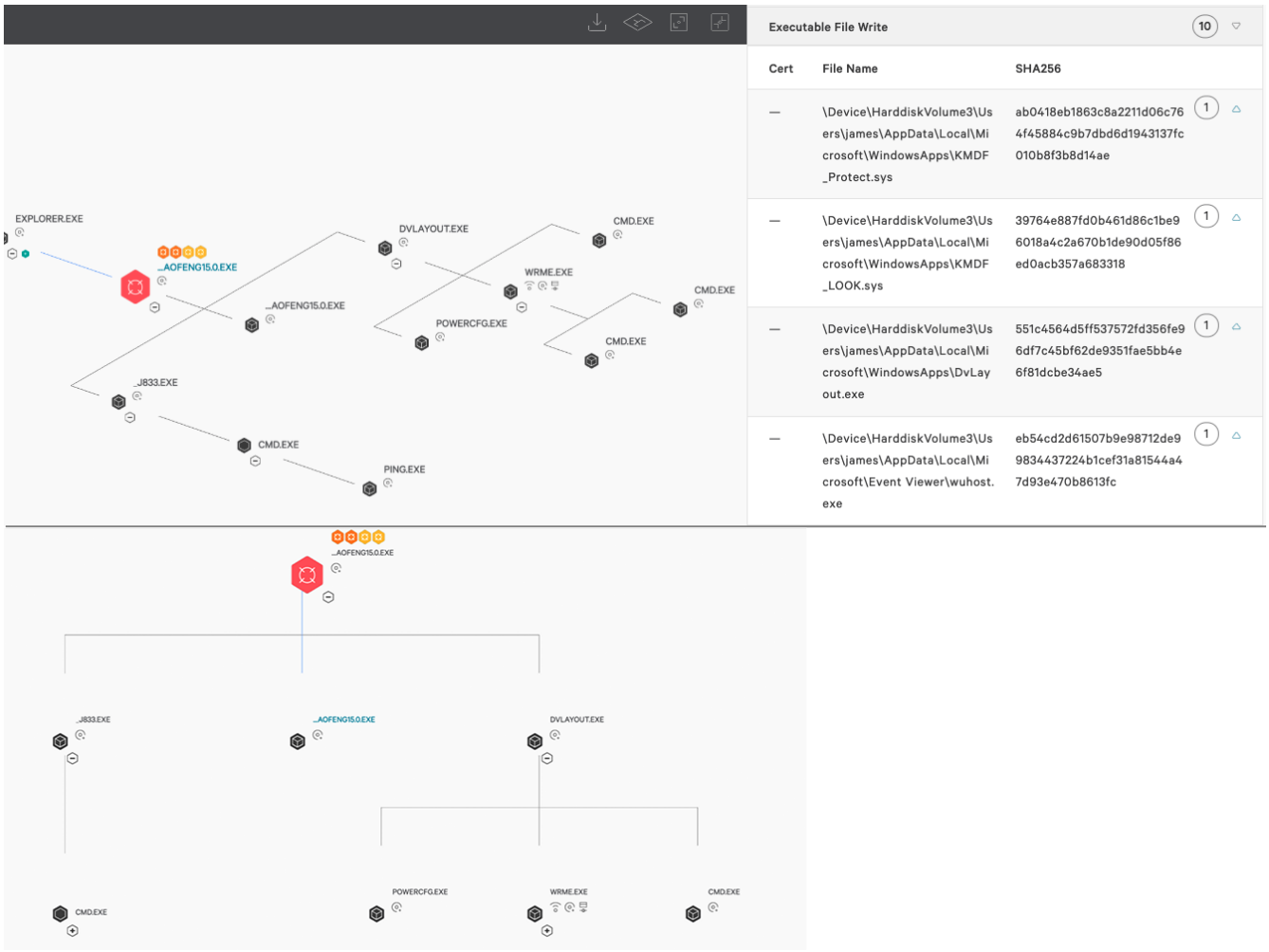

Figure 1. Spicy Hot Pot as seen in the CrowdStrike Falcon process execution tree (click image to enlarge)

This detection raises a number of questions due to the context and location of dropped binaries when run on a Windows 10 machine.

- `%localappdata%\Microsoft\Event Viewer\wccenter.exe`
- `%localappdata%\Microsoft\Event Viewer\wdlogin.exe`
- `%localappdata%\Microsoft\Event Viewer\wrme.exe`
- `%localappdata%\Microsoft\Event Viewer\wuhost.exe`
- `%localappdata%\Microsoft\WindowsApps\DvLayout.exe`
- `%localappdata%\Temp\_J861.exe`
- `%localappdata%\Temp\baofeng15.0.exe`
- `%localappdata%\Microsoft\WindowsApps\KMDF_LOOK.sys`
- `%localappdata%\Microsoft\WindowsApps\KMDF_Protect.sys`

On Windows 7, the drivers fall into “Media Player” instead of “WindowsApps.” In addition, this made a number of registry modifications to the local machine’s software hive:

- `Software\Microsoft\Helicarrier\st\stemp`
- `Software\Microsoft\Helicarrier\Channel`
- `Software\Microsoft\DirectX\DvVersion`
- `Software\Microsoft\DirectX\PvVersion`
- `Software\Microsoft\DirectX\RvVersion`
- `Software\Microsoft\Helicarrier\dp`
- `Software\Microsoft\Helicarrier\ca`
- `Software\Microsoft\Helicarrier\dr`
- `Software\Microsoft\Helicarrier\eu`
- `Software\Microsoft\Helicarrier\fd`
- `Software\Microsoft\Helicarrier\ap`

One important item to note is the presence of a new baofeng15.0.exe binary with a different hash. This was far more widespread than the binary that was just run and had a creation timestamp dating back four years:

```
2016-01-13 13:19:34
```

Based on this, it’s likely that an older cracking tool has been repackaged with this malware and distributed online by the malware operator. The other eight files dropped are signed by a few different signing certificates issued to “Beijing JoinHope Image Technology Ltd.” Unique samples found have different validity timeframes for their signing certificates, showing validity issued anywhere from 1 minute to 10 years ago. At the time of writing, all had expired; however, they were still able to be successfully installed due to exceptions to driver signing enforcement.

File Name	Signing Certificate
`DvLayout.exe`	Valid From 12:00 AM 05/16/2014 Valid To 11:59 PM 05/16/2015
`wccenter.exe`	Valid From 12:00 AM 05/16/2014 Valid To 11:59 PM 05/16/2015
`wrme.exe`	Valid From 12:00 AM 02/08/2010 Valid To 11:59 PM 02/07/2020
`wuhost.exe`	Valid From 12:00 AM 02/08/2010 Valid To 11:59 PM 02/07/2020
`wdlogin.exe`	Valid From 04:23 AM 08/22/2020 Valid To 04:23 AM 08/22/2020

`_J861.exe`	Valid From 12:00 AM 02/08/2010 Valid To 11:59 PM 02/07/2020
`baofeng15.0.exe`	Not Signed
`KMDF_LOOK.sys`	Valid From 02:21 AM 06/13/2020 Valid To 02:21 AM 06/13/2020
`KMDF_Protect.sys`	Valid From 12:00 AM 05/16/2014 Valid To 11:59 PM 05/16/2015

Table 1. Validity timeframes for the files dropped by Spicy Hot Pot

Comparing this signing certificate to a public repository of malware samples reveals hundreds of unique malware samples, indicating that the creator of this malware (or someone with access to these signing certificates) is in no rush to stop using certificates issued to this entity. Many pieces of malware signed by this entity contained similar debugging (pdb) locations in their debug strings.

Binary	PDB
`KMDF_LOOK.sys`	`G:\SVN\源码\驱动\LookFile\KMDF_LOOK\Release\KMDF_LOOK_64.pdb`
`KMDF_Protect.sys`	`G:\SVN\源码\驱动\protect\KMDF_Protect\Release\KMDF_Protect_64.pdb`
`wdlogin.exe`	`D:\Work\Install_Driver\Driver_helper\Release\wdlogin.pdb`
`wrme.exe`	`D:\Work\Install_Driver\Driver_helper\Release\wrme.pdb`
`wccenter.exe`	`D:\Work\Install_Driver\Driver_helper\Release\wccenter.pdb`
`_J861.exe`	`E:\work\Icon_Report\Release\_service.pdb`
`wuhost.exe`	`D:\Work\Install_Driver\Driver_helper\Release\wuhost.pdb`

Table 2. Debugging locations found in Spicy Hot Pot malware

To a normal user, the kernel drivers dropped to disk are completely invisible. This is because not only are they renamed and installed on infection, but through their installation they begin to act as a rootkit — and one of the drivers hides the malware files from being shown on disk. This extends to making the executables dropped to disk invisible. We can see the different filtering capabilities of this driver from analyzing pseudo-code of the file `KMDF_Protect.sys.`

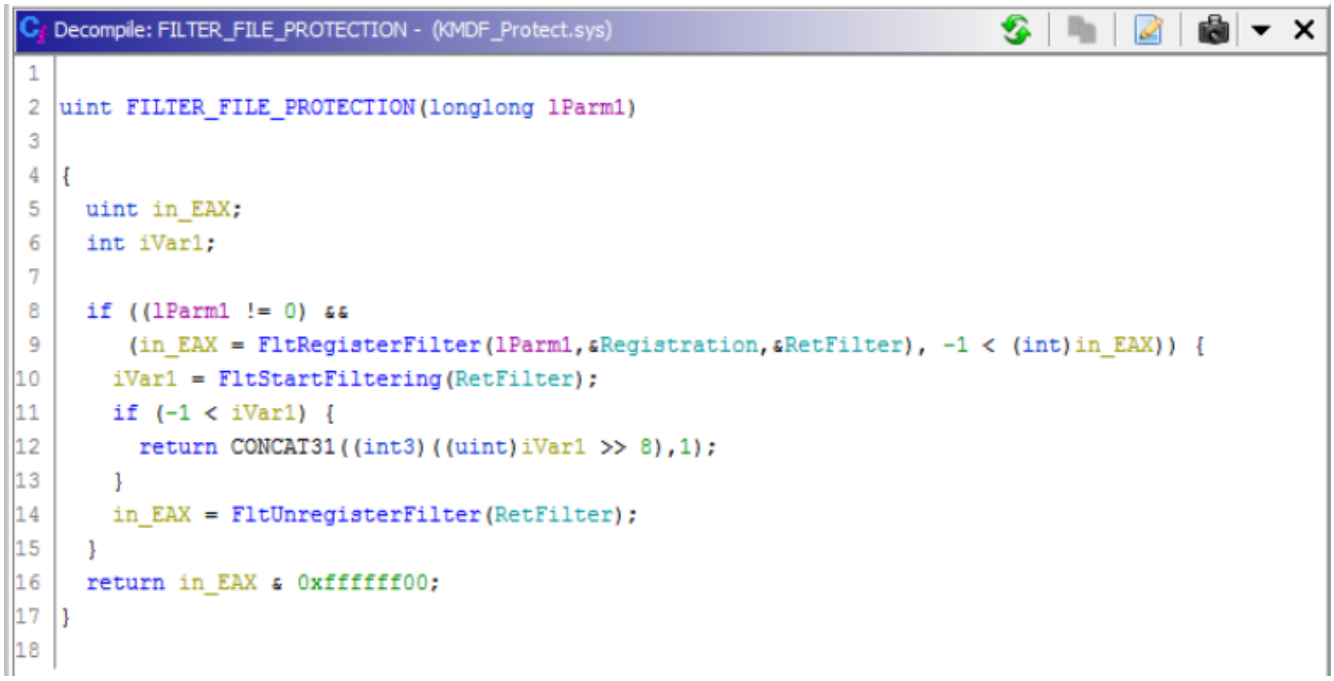

Figure 2. Minifilter being registered

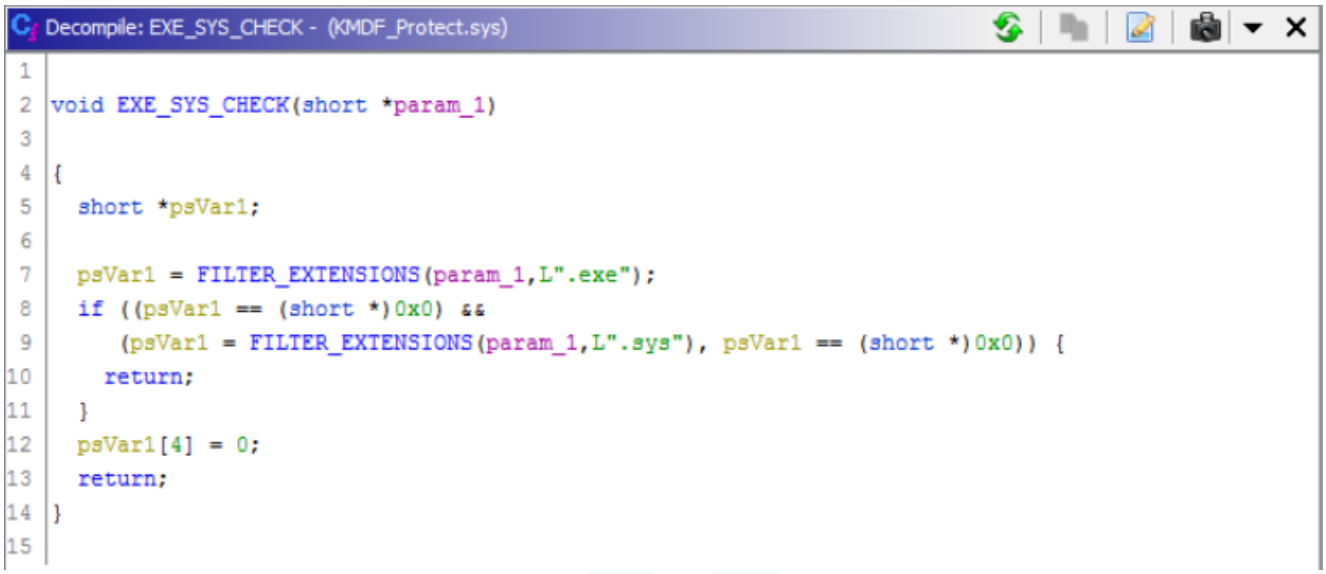

Figure 3. Searching for `.sys` and `.exe` files to filter on

In addition to this, `KMDF_Protect.sys` checks for any executables running with known binary names from Qihoo 360 software.

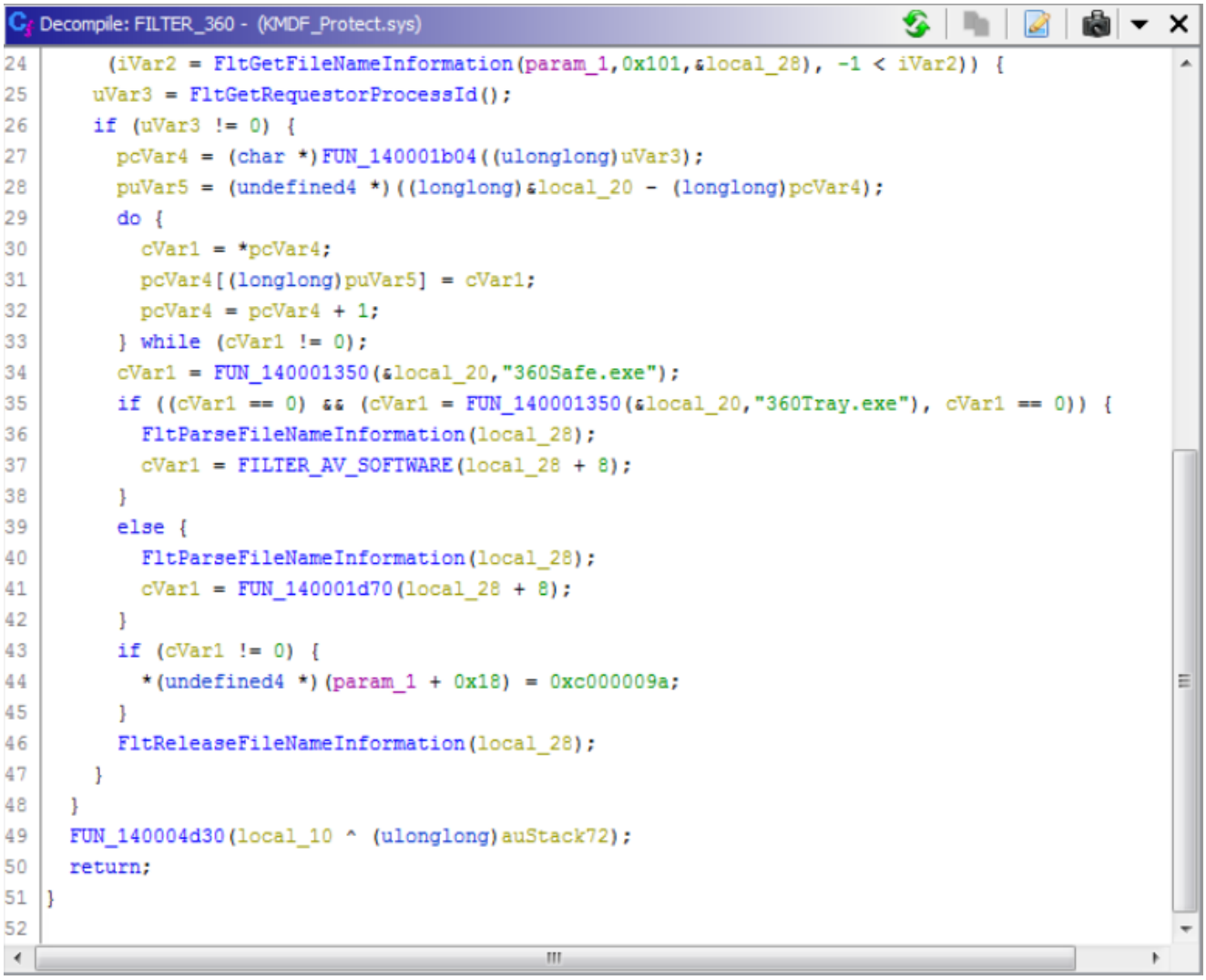

Figure 4. Checking for antivirus software attempting to run

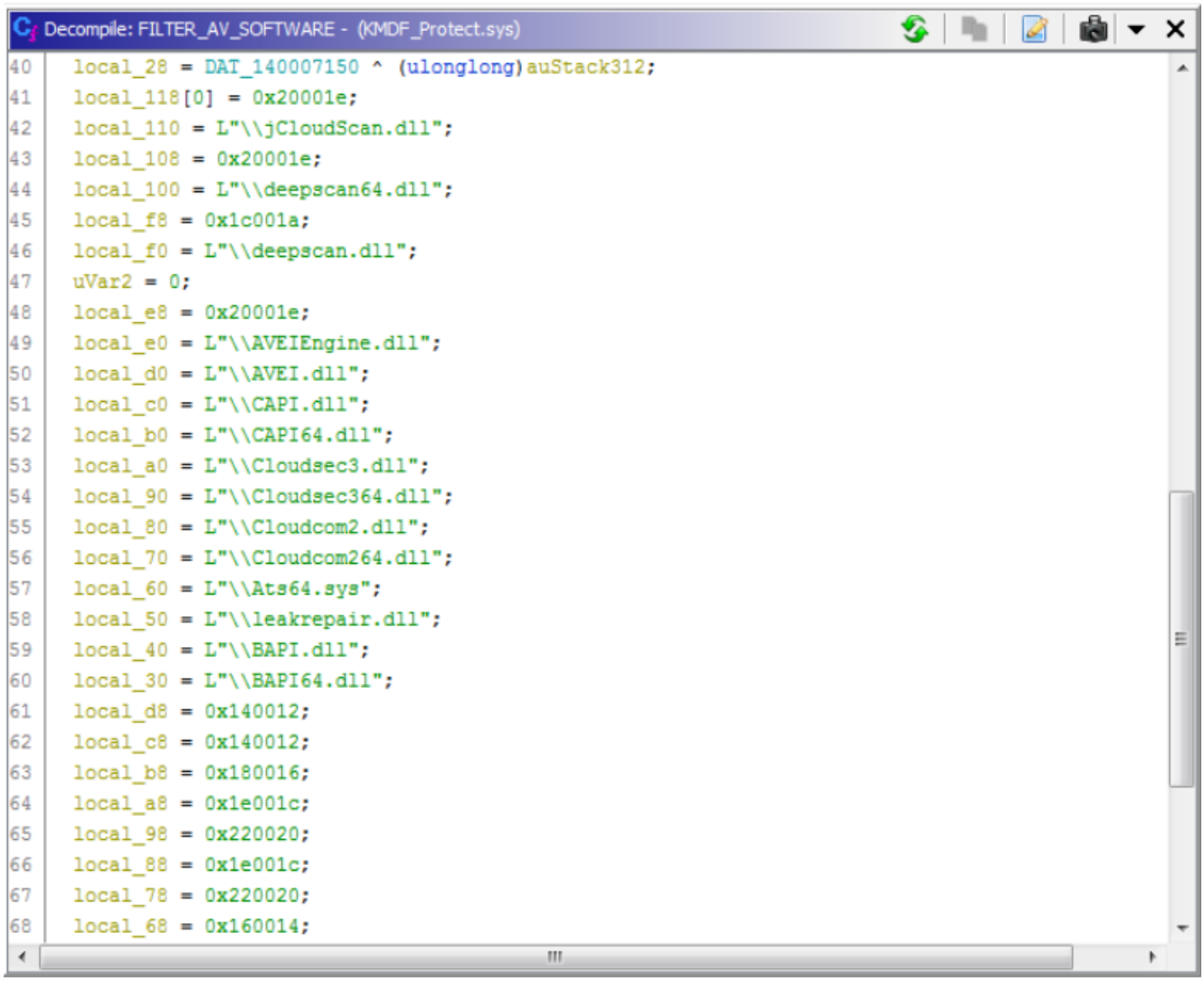

Figure 5. Strings used in preventing antivirus software from loading scanning modules

This also adds a shutdown callback for persistence. At shutdown, the driver attempts to write back the location of `wccenter.exe` to the system's "RunOnce" key so that it runs again on boot. As this is performed by the kernel-mode driver, this modification isn't shown by common registry monitoring tools.

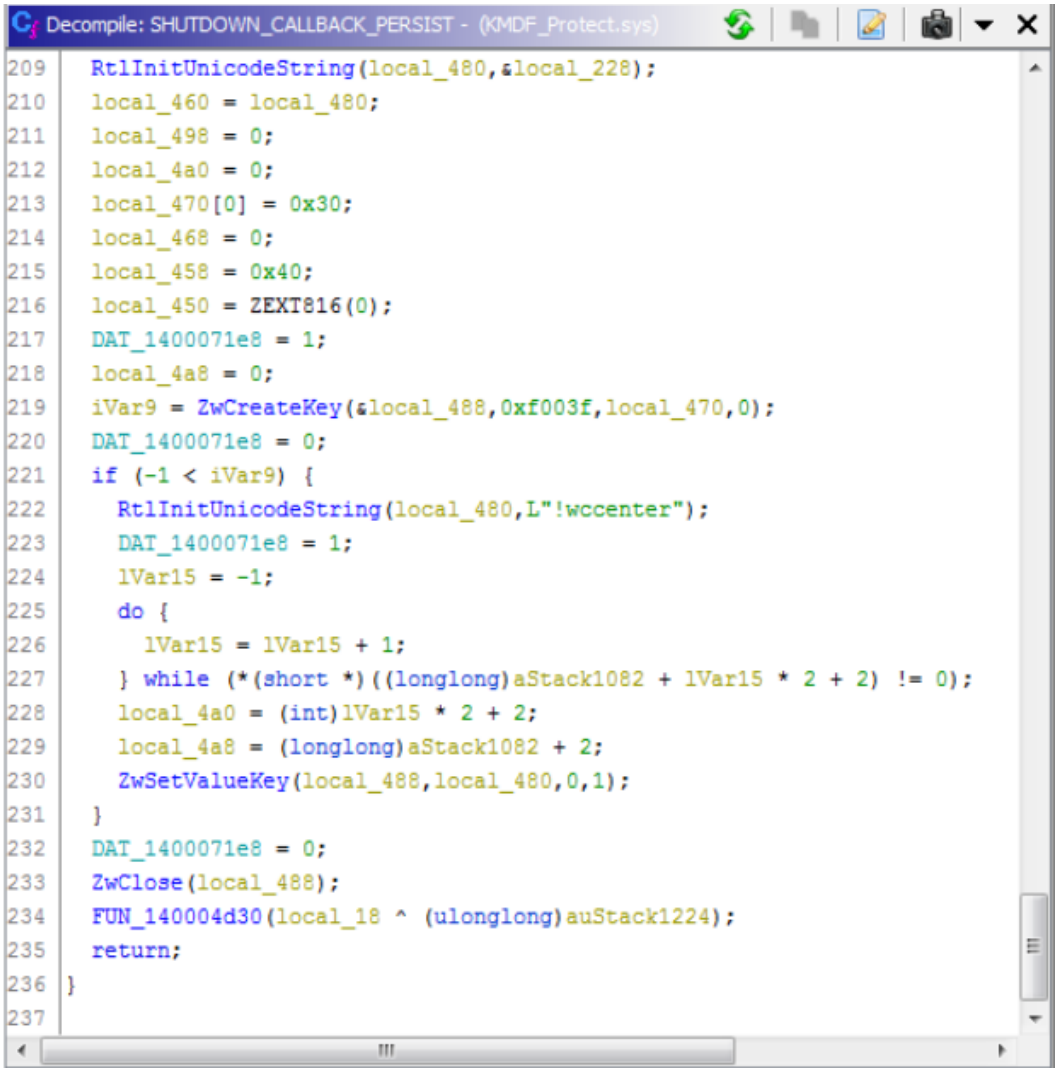

Figure 6. Persistence through a shutdown function callback

If we compare this to `KMDF_LOOK.sys`, we can see that its primary function is to hijack the user's homepage and delete process callbacks to security software.

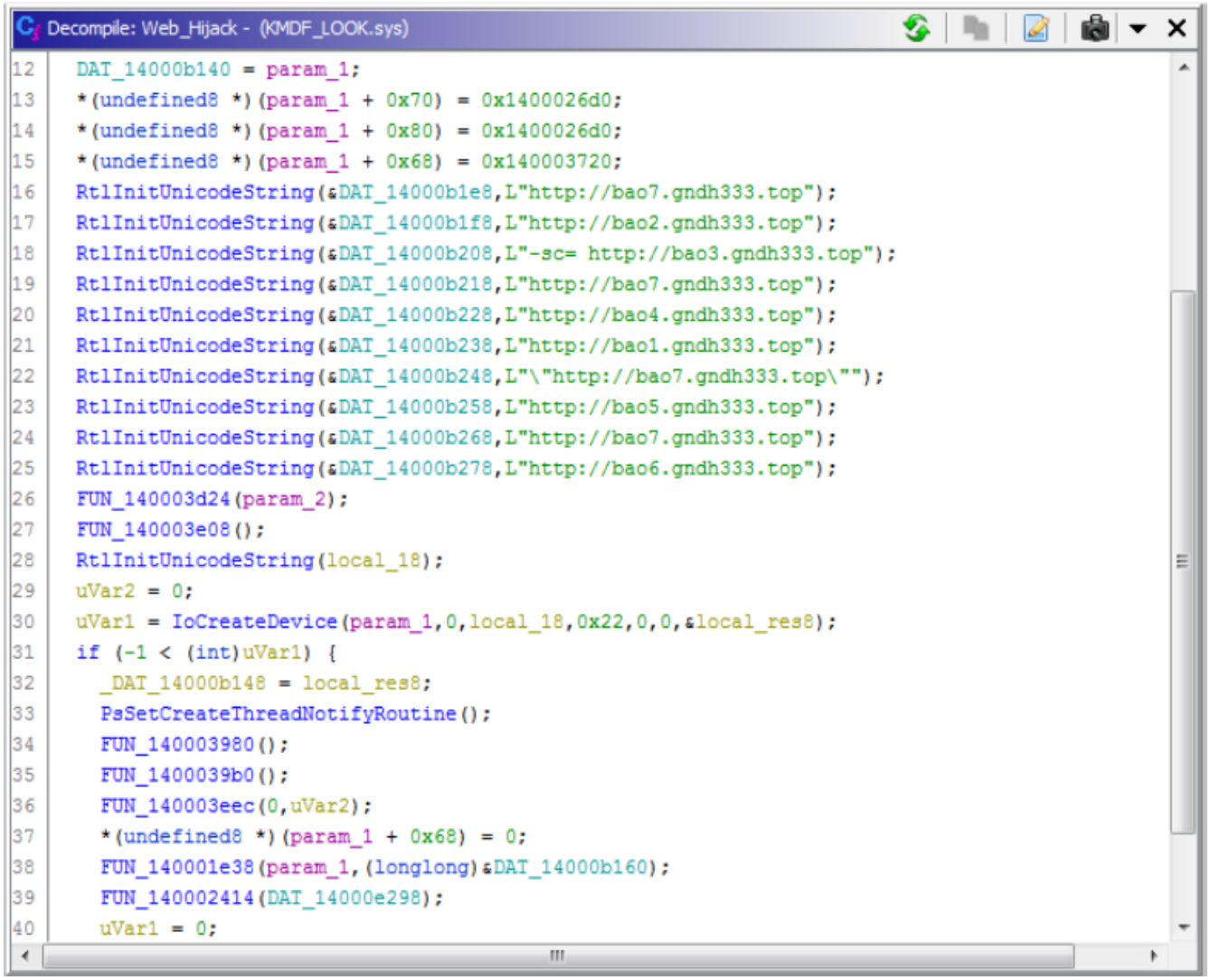

Figure 7. Hardcoded URLs for the browser hijacking component

It should be noted that both drivers masquerade as legitimate service names to remain stealthy:

Driver	Malicious Service Name	Masqueraded Legitimate Service Name
`KMDF_Protect.sys`	iaLPSS1z	iaLPSSi*: Intel Serial IO Driver
`KMDF_LOOK.sys`	LSI_SAS2I	LSI_SAS2: LSI SAS GEN 2 Driver (StorPort)

Briefing over other components of this malware:

- `DVLayout.exe` is used to install the rootkit. This creates the Mutex “DVLayout.”
- **`_J861.exe` is used to gather system information of the infected client, including serial number, and has a number of networking functions that support the operation of this malware. This temporarily creates a service called “R.”**
- `wccenter.exe` communicates with `KMDF_Protect.sys` using a named device created called `\\Device\\iaLPSS1z` and is used to run `wdlogin.exe`, `wuhost.exe` and `wrme.exe`.

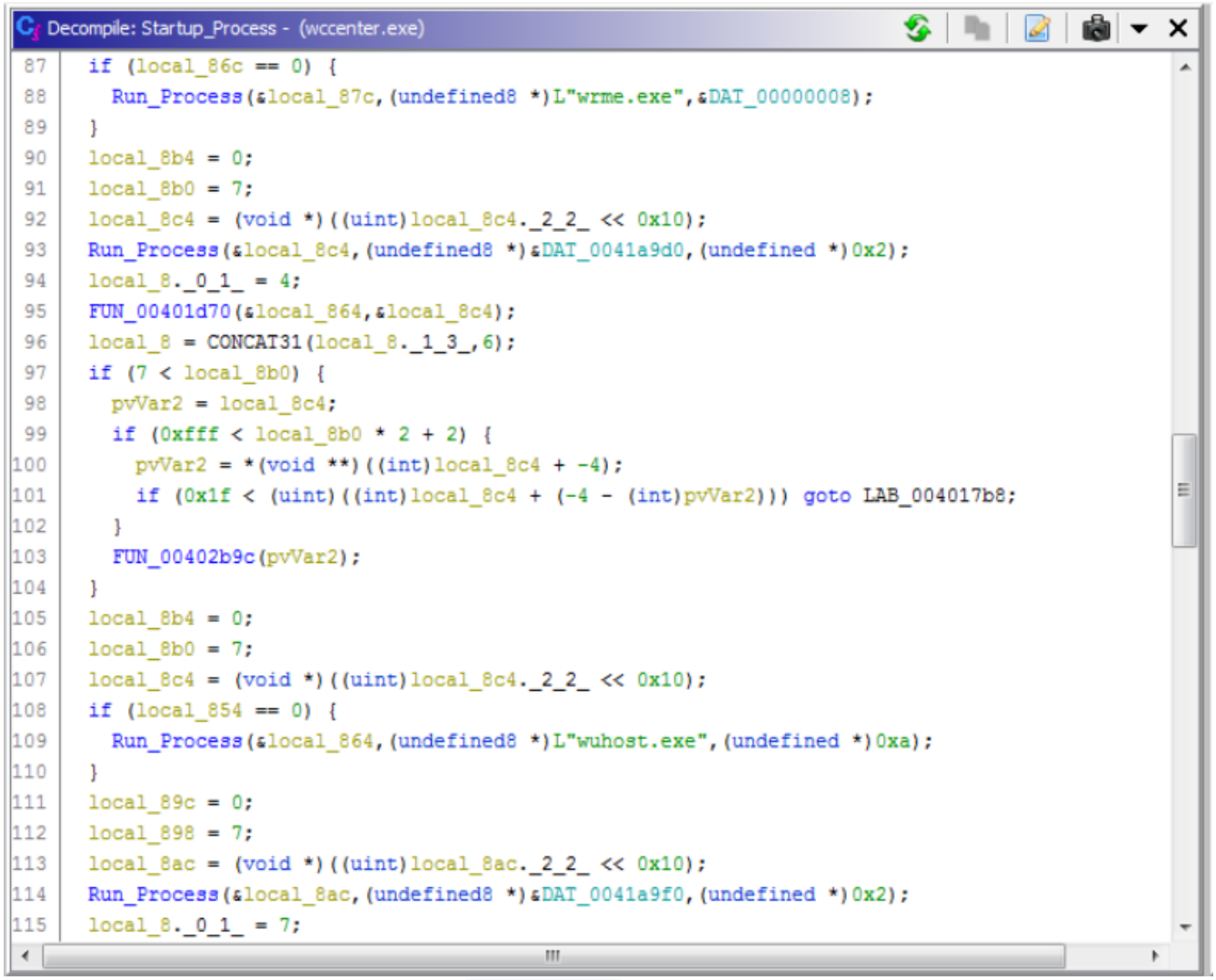

Figure 8. `wccenter.exe` startup execution

`wuhost.exe` is used to update the rootkit drivers and modules as required. It creates the Mutex “Update” and contacts one of the following domains to fetch this update:

- https[:]//du[.]testjj[.]com
- https[:]//da[.]testiu[.]com
- https[:]//db[.]testyk[.]com

`wrme.exe` is used to download and start or install modules such as wuhost.exe and wdlogin.exe in addition to gathering information about the operating system. It creates the Mutex “DLreport.”

`wdlogin.exe` is used to find any dump file ending with dmp in the %SystemRoot%\minidump directory, compress it, and upload it to one of the above servers at the endpoint /api/v1/post_dump. This is likely for troubleshooting any blue screen errors that may be caused by the rootkit. It creates the Mutex “dumping.”

Investigation with Endpoint Detection and Response Data

Using CrowdStrike Falcon’s telemetry via our Endpoint Activity Monitoring (EAM) application, we’re able to see the infection actions taking place when protections are disabled. This includes file writes of `_J861.exe, KMDF_Protect.sys, KMDF_LOOK.sys`, and their associated driver loads.

PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp_J861.exe
FileCreateInfo	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp\nsbFB4B.tmp\System.dll
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp\J861.exe
PackedExecutableWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp\baofeng15.0.exe
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\KMDF_LOOK.sys
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wdlogin.exe
FileCreateInfo	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wrme.exe
NewExecutableWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wccenter.exe
FileCreateInfo	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\DvLayout.exe
NewExecutableWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\Event Viewer\wuhost.exe
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\KMDF_Protect.sys
NewExecutableRenamed	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys
NewExecutableRenamed	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys
PeFileWritten	\Device\HarddiskVolume3\Users\james\AppData\Local\Temp\~J861.exe

Figure 9. File events as seen in CrowdStrike Falcon's EAM Application (click image to enlarge)

2020-10-11 21:37:49.157	DriverLoad	\Device\HarddiskVolume3\Windows\System32\drivers\vmmemctl.sys
2020-10-11 21:09:37.532	DriverLoad	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys
2020-10-11 21:09:36.172	DriverLoad	\Device\HarddiskVolume3\Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys
2020-10-11 21:08:30.538	DriverLoad	\Device\HarddiskVolume3\Windows\System32\drivers\bthenum.sys

Figure 10. DriverLoad events as seen in the CrowdStrike Falcon EAM application (click image to enlarge)

By checking the registry and filter drivers on this host through CrowdStrike Falcon's Real Time Response (RTR) capability, we can locate the kernel drivers running and the dropped binaries to prove they reside on disk, given that we know their name and location. This works even though Spicy Hot Pot filters user input and output requests to make the files invisible to a normal user of Windows.

```
C:\> ls 'Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys'
Directory listing for C:\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys

Name                                    Type            Size (bytes)       Size (MB)
----                                    ----            ------------       ---------
SUCHETTC.sys                            .sys                  280064           0.267

C:\> ls 'Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys'
Directory listing for C:\Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys

Name                                    Type            Size (bytes)       Size (MB)
----                                    ----            ------------       ---------
VCTXRYDQ.sys                            .sys                  280064           0.267
```

Figure 11. Rootkit drivers as seen through Real Time Response (RTR)

```
C:\> reg query HKLM\SYSTEM\CurrentControlSet\Services\LSI_SAS2l
Subkeys of HKLM\SYSTEM\CurrentControlSet\Services\LSI_SAS2l :

SubKeyName SubKeyCount ValueCount
---------- ----------- ----------
Instances            1          1



Properties of (HKLM\SYSTEM\CurrentControlSet\Services\LSI_SAS2l) :

Property               Type Value
--------               ---- -----
Type                  DWord 2
Start                 DWord 1
ErrorControl          DWord 0
ImagePath        ExpandString \??\C:\Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys
DisplayName           String LSI_SAS2l
Group                 String System Reserved
DependOnService       String FltMgr
```

Figure 12. Rootkit service as seen through Real Time Response (RTR)

```
C:\> reg query HKLM\SYSTEM\CurrentControlSet\Services\iaLPSS1z
Subkeys of HKLM\SYSTEM\CurrentControlSet\Services\iaLPSS1z :

SubKeyName SubKeyCount ValueCount
---------- ----------- ----------
Instances            1          1



Properties of (HKLM\SYSTEM\CurrentControlSet\Services\iaLPSS1z) :

Property               Type Value
--------               ---- -----
Type                  DWord 2
Start                 DWord 1
ErrorControl          DWord 0
ImagePath        ExpandString \??\C:\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys
DisplayName           String iaLPSS1z
Group                 String System Reserved
DependOnService       String FltMgr
```

Figure 13. Rootkit service as seen through Real Time Response (RTR)

The Remediation

Spicy Hot Pot, like many other rootkits, utilizes kernel filter drivers that once started cannot be stopped by a user. These filter drivers prevent removal of registry keys, services or the kernel drivers themselves that are associated with the infection. Due to this, removing Spicy Hot Pot malware remotely can be quite challenging. Remediating a rootkit often requires doing so from a machine that is powered off or booted into safe mode; however, we can remove a rootkit such as Spicy Hot Pot without going to these extremes by making sure it cannot run at startup.

Spicy Hot Pot places the malicious filter drivers within the “WindowsApps” folder, which, in addition to the “Event Viewer” or “Media Player” folder, is what is being filtered on. If you rename the folder, the filter drivers immediately become visible.

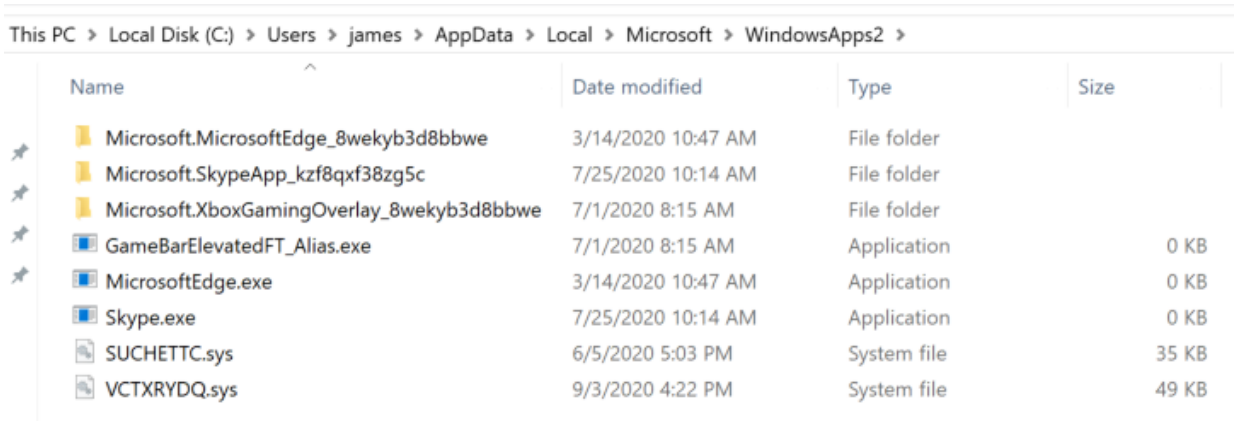

Figure 14. Rootkit drivers visible after renaming WindowsApps folder

This can be done even when the kernel filters are running, but the filter drivers cannot be removed by a user as they’re still running and protected.

```
C:\> rm C:\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys
Access to the path is denied.

C:\> rm C:\Users\james\AppData\Local\Microsoft\WindowsApps\VCTXRYDQ.sys
Access to the path is denied.
```

Figure 15. Protected in-use kernel drivers that cannot be removed

After renaming the folder, if you restart an infected system, the path that is referenced by the kernel filter driver services no longer exists, and the drivers will fail to load. At this point, the drivers and associated malicious executables can be removed, and the folder renamed to “WindowsApps” once more. The services and registry keys associated with the rootkit can also be removed now.

```
C:\> reg query HKLM\SYSTEM\CurrentControlSet\Services\iaLPSS1z
Subkeys of HKLM\SYSTEM\CurrentControlSet\Services\iaLPSS1z :

SubKeyName SubKeyCount ValueCount
---------- ---------- ----------
Instances            1          1



Properties of (HKLM\SYSTEM\CurrentControlSet\Services\iaLPSS1z) :

Property               Type Value
--------               ---- -----
Type                  DWord 2
Start                 DWord 1
ErrorControl          DWord 0
ImagePath        ExpandString \??\C:\Users\james\AppData\Local\Microsoft\WindowsApps\SUCHETTC.sys
DisplayName           String iaLPSS1z
Group                 String System Reserved
DependOnService       String FltMgr
```

Figure 16. Rootkit driver removal as seen through Real Time Response (RTR)

Conclusion

This post touched on a common browser hijacker being distributed with tools designed to illegitimately activate Microsoft products. It highlights some of the concerns associated with running “cracking” tools on a machine, and why it’s important to monitor and prevent not only unknown executables that are running, but also drivers that are loaded by an operating system and any minifilters present.

By fusing CrowdStrike Falcon’s detection and prevention capabilities, enriched endpoint telemetry, Real Time Response capability and the expertise of the CrowdStrike Falcon Complete team, you’re uniquely positioned with the capability to detect, investigate, understand and respond to unknown threats within your environment 24/7, 365 days of the year.

Indicators

Type	Name/Purpose	Indicator
SHA256	baofeng15.0	498ed725195b5ee52e406de237afa9ef268cabc4ef604c363aee2e78b3b13193
SHA256	DvLayout.exe	551c4564d5ff537572fd356fe96df7c45bf62de9351fae5bb4e6f81dcbe34ae5
SHA256	wccenter.exe	17095beda4afeabb7f41ff07cf866ddc42e49da1a4ed64b9c279072caab354f6
SHA256	wrme.exe	7e489f1f72cac9f1c88bdc6be554c78b5a14197d63d1bae7e41de638e903af21
SHA256	wuhost.exe	eb54cd2d61507b9e98712de99834437224b1cef31a81544a47d93e470b8613fc
SHA256	wdlogin.exe	7c0fdee3670cc53a22844d691307570a21ae3be3ce4b66e46bb6d9baad1774b8
SHA256	_J861.exe	c83e6b96ee3aa1a580157547eae88d112d2202d710218f2ed496f7fe3d861abc
SHA256	baofeng15.0.exe	c5802c7fbad5cdf257bcc0f71e8b1c8853e06da411133b5dc78bd6c891f27500
SHA256	KMDF_LOOK.sys	39764e887fd0b461d86c1be96018a4c2a670b1de90d05f86ed0acb357a683318
SHA256	KMDF_Protect.sys	ab0418eb1863c8a2211d06c764f45884c9b7dbd6d1943137fc010b8f3b8d14ae
Domain	Update/C2	du[.]testjj[.]com
Domain	Update/C2	da[.]testiu[.]com
Domain	Update/C2	db[.]testyk[.]com
Domain	Hijacking Domain	gndh333[.]top
Mutex	wrme.exe	DLreport
Mutex	wdlogin	dumping
Mutex	wuhost	Update
Mutex	DVLayout	DVLayout

MITRE ATT&CK® Mapping

Tactic	Technique	Sub-Technique	ID
Reconnaissance	Search Open Websites/Domains	Search Engines	T1593.002
Resource Development	Acquire Infrastructure	Domains	T1583.001
Resource Development	Obtain Capabilities	Digital Certificates	T1588.004
Initial Access	Supply Chain Compromise	Compromise Software Supply Chain	T1195.002
Persistence	Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder	T1547.001
Persistence	Create or Modify System Process	Windows Service	T1543.003
Defense Evasion	Rootkit	–	T1014
Defense Evasion	Impair Defenses	Disable or Modify Tools	T1562.001
Defense Evasion	Masquerading	Invalid Code Signature	T1036.001
Defense Evasion	Masquerading	Masquerade Task or Service	T1036.004
Defense Evasion	Masquerading	Match Legitimate Name or Location	T1036.005
Collection	Automated Collection	–	T1119
Command and Control	Encrypted Channel	Asymmetric Cryptography	T1573.002
Exfiltration	Automated Exfiltration	–	T1020
Exfiltration	Exfiltration Over C2 Channel	–	T1041
Impact	Defacement	Internal Defacement	T1491.001
Impact	Service Stop	–	T1489

Yara Rules

/*
YARA Rule Set
Author: jai-minton
Date: 2020-11-01
Identifier: SpicyHotPot
Reference: https://www.crowdstrike.com/blog/author/jai-minton/
copyright = “(c) 2020 CrowdStrike Inc.”
// Rule Set ———————————————————————— */

```
rule SpicyHotPot_wdlogin {
meta:
description = "SpicyHotPot - wdlogin.exe: Used to identify memory dump uploading
component"
author = "jai-minton"
reference = "https://www.crowdstrike.com/blog/author/jai-minton/"
copyright = "(c) 2020 CrowdStrike Inc."
```

```
 date = "2020-11-01"
 hash1 = "7c0fdee3670cc53a22844d691307570a21ae3be3ce4b66e46bb6d9baad1774b8"
 strings:
 $x1 = "D:\\Work\\Install_Driver\\Driver_helper\\Release\\wdlogin.pdb" fullword ascii
 $x2 = "kmdf_protect.sys" fullword ascii
 $x3 = "kmdf_look.sys" fullword ascii
 $x4 = "/api/v1/post_dump" fullword ascii
 $s1 = "Negotiate: noauthpersist -> %d, header part: %s" fullword ascii
 $s2 = "https://db.testyk.com" fullword ascii
 $s3 = "https://da.testiu.com" fullword ascii
 $s4 = "https://du.testij.com" fullword ascii
 $s5 = "schannel: CertGetNameString() failed to match connection hostname (%s) against
server certificate names" fullword ascii
 $s6 = "No more connections allowed to host %s: %zu" fullword ascii
 $s7 = "RESOLVE %s:%d is - old addresses discarded!" fullword ascii
 $s8 = "Content-Disposition: %s%s%s%s%s%s%s" fullword ascii
 $s9 = "dumping" fullword wide
 condition:
 uint16(0) == 0x5a4d and filesize < 2000KB and
 1 of ($x*) and 3 of ($s*)
 }

 rule SpicyHotPot__J861 {
 meta:
 description = "SpicyHotPot - _J861.exe: Used to identify system fingerprinting,
enumeration and networking component"
 author = "jai-minton"
 reference = "https://www.crowdstrike.com/blog/author/jai-minton/"
 copyright = "(c) 2020 CrowdStrike Inc."
 date = "2020-11-01"
 hash1 = "c83e6b96ee3aa1a580157547eae88d112d2202d710218f2ed496f7fe3d861abc"
 strings:
 $x1 = "E:\\work\\Icon_Report\\Release\\_service.pdb" fullword ascii
 $x2 = "RESOLVE %s:%d is - old addresses discarded!" fullword ascii
 $x3 = "https://du.testij.com/api/v1/id" fullword ascii
 $s1 = "SEC_E_ILLEGAL_MESSAGE (0x%08X)" ascii
 $s2 = "Failed reading the chunked-encoded stream" fullword ascii
 $s3 = "Negotiate: noauthpersist -> %d, header part: %s" fullword ascii
 $s4 = "AppPolicyGetProcessTerminationMethod" fullword ascii
 $s5 = "schannel: CertGetNameString() failed to match connection hostname (%s) against
server certificate names" fullword ascii
 $s6 = "failed to load WS2_32.DLL (%u)" fullword ascii
 $s7 = "/c ping -n 3 127.1 >nul & del /q %s" fullword ascii
 $s8 = "No more connections allowed to host %s: %zu" fullword ascii
 $s9 = "%d ReadPhysicalDriveInNTUsingSmart ERROR DeviceIoControl(%d, SMART_GET_VERSION)
returned 0, error is %d" fullword ascii
 $s10 = "%d ReadPhysicalDriveInNTWithAdminRights ERROR DeviceIoControl() %d,
DFP_GET_VERSION) returned 0, error is %d" fullword ascii
 $s11 = "Content-Disposition: %s%s%s%s%s%s%s" fullword ascii
 $s12 = "Content-Type: %s%s%s" fullword ascii
 $s13 = "SOCKS4%s: connecting to HTTP proxy %s port %d" fullword ascii
 $s14 = "No valid port number in connect to host string (%s)" fullword ascii
 $s15 = "Excess found in a read: excess = %zu, size = %I64d, maxdownload = %I64d,
bytecount = %I64d" fullword ascii
 condition:
 uint16(0) == 0x5a4d and filesize < 3000KB and
 2 of ($x*) and 8 of ($s*)
 }

 rule SpicyHotPot_wuhost {
 meta:
 description = "SpicyHotPot - wuhost.exe: Used to identify rootkit and module updating
component"
 author = "jai-minton"
 reference = "https://www.crowdstrike.com/blog/author/jai-minton/"
 copyright = "(c) 2020 CrowdStrike Inc."
 date = "2020-11-01"
 hash1 = "eb54cd2d61507b9e98712de99834437224b1cef31a81544a47d93e470b8613fc"
 strings:
```

```
 $x1 = "wdlogin.exe" fullword ascii
 $x2 = "UpdateTemp.exe" fullword ascii
 $x3 = "UpdateSelf.exe" fullword ascii
 $x4 = "wrme.exe" fullword ascii
 $x5 = "wccenter.exe" fullword ascii
 $x6 = "D:\\Work\\Install_Driver\\Driver_helper\\Release\\wuhost.pdb" fullword ascii
 $x7 = "wuhost.exe" fullword ascii
 $s1 = "SEC_E_ILLEGAL_MESSAGE (0x%08X) - This error usually occurs when a fatal SSL/TLS
alert is received (e.g. handshake failed). More " ascii
 $s2 = "Failed reading the chunked-encoded stream" fullword ascii
 $s3 = "Negotiate: noauthpersist -> %d, header part: %s" fullword ascii
 $s4 = "https://db.testyk.com" fullword ascii
 $s5 = "https://da.testiu.com" fullword ascii
 $s6 = "https://du.testij.com" fullword ascii
 $s7 = "dump_temp" fullword ascii
 $s8 = "AppPolicyGetProcessTerminationMethod" fullword ascii
 $s9 = "schannel: CertGetNameString() failed to match connection hostname (%s) against
server certificate names" fullword ascii
 $s10 = "failed to load WS2_32.DLL (%u)" fullword ascii
 $s11 = "No more connections allowed to host %s: %zu" fullword ascii
 $s12 = "RESOLVE %s:%d is - old addresses discarded!" fullword ascii
 condition:
 uint16(0) == 0x5a4d and filesize < 2000KB and
 2 of ($x*) and 4 of them
 }

 rule SpicyHotPot_wrme {
 meta:
 description = "SpicyHotPot - wrme.exe: Used to identify module starting and reporting
component"
 author = "jai-minton"
 reference = "https://www.crowdstrike.com/blog/author/jai-minton/"
 copyright = "(c) 2020 CrowdStrike Inc."
 date = "2020-11-01"
 hash1 = "7e489f1f72cac9f1c88bdc6be554c78b5a14197d63d1bae7e41de638e903af21"
 strings:
 $x1 = "DvUpdate.exe" fullword ascii
 $x2 = "D:\\Work\\Install_Driver\\Driver_helper\\Release\\wrme.pdb" fullword ascii
 $x3 = "No more connections allowed to host %s: %zu" fullword ascii
 $s1 = "SEC_E_ILLEGAL_MESSAGE (0x%08X) - This error usually occurs when a fatal SSL/TLS
alert is received (e.g. handshake failed). More " ascii
 $s2 = "Failed reading the chunked-encoded stream" fullword ascii
 $s3 = "Content-Type: %s%s%s" fullword ascii
 $s4 = "Excess found in a read: excess = %zu, size = %I64d, maxdownload = %I64d,
bytecount = %I64d" fullword ascii
 $s5 = "Negotiate: noauthpersist -> %d, header part: %s" fullword ascii
 $s6 = "https://db.testyk.com" fullword ascii
 $s7 = "https://da.testiu.com" fullword ascii
 $s8 = "https://du.testij.com" fullword ascii
 $s9 = "AppPolicyGetProcessTerminationMethod" fullword ascii
 $s10 = "schannel: CertGetNameString() failed to match connection hostname (%s) against
server certificate names" fullword ascii
 $s11 = "failed to load WS2_32.DLL (%u)" fullword ascii
 $s12 = "Content-Disposition: %s%s%s%s%s%s%s" fullword ascii
 $s13 = "RESOLVE %s:%d is - old addresses discarded!" fullword ascii
 condition:
 uint16(0) == 0x5a4d and filesize < 2000KB and
 2 of ($x*) and 7 of ($s*)
 }

 rule SpicyHotPot_DvLayout {
 meta:
 description = "SpicyHotPot - DvLayout.exe: Used to identify rootkit installation
component"
 author = "jai-minton"
 reference = "https://www.crowdstrike.com/blog/author/jai-minton/"
 copyright = "(c) 2020 CrowdStrike Inc."
 date = "2020-11-01"
 hash1 = "551c4564d5ff537572fd356fe96df7c45bf62de9351fae5bb4e6f81dcbe34ae5"
```

```
strings:
$x1 = "KMDF_LOOK.sys" fullword ascii
$x2 = "KMDF_Protect.sys" fullword ascii
$x3 = "StartService Error, errorode is : %d ." fullword ascii
$x4 = "Software\\Microsoft\\%s\\st" fullword wide
$s1 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s2 = "@api-ms-win-core-synch-l1-2-0.dll" fullword wide
$s3 = "Genealogy.ini" fullword wide
$s4 = "powercfg /h off" fullword ascii
$s5 = " Type Descriptor'" fullword ascii
$s6 = "find %s failed , errorcode : %d" fullword ascii
$s7 = "find %s failed , errorcode : %d" fullword ascii
$s8 = "Delete %s failed , errorcode : %d" fullword wide
$s9 = "Delete %s failed , errorcode : %d" fullword wide
$s10 = "OpenService failed , errorcode : %d" fullword wide
$s11 = "&Beijing JoinHope Image Technology Ltd.1/0-" fullword ascii
$s12 = "/c del /q %s" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 800KB and
1 of ($x*) and 5 of ($s*)
}

rule SpicyHotPot_wccenter {
meta:
description = "SpicyHotPot - wccenter.exe: Used to identify malware that communicates
with the rootkit component"
author = "jai-minton"
reference = "https://www.crowdstrike.com/blog/author/jai-minton/"
copyright = "(c) 2020 CrowdStrike Inc."
date = "2020-11-01"
hash1 = "17095beda4afeabb7f41ff07cf866ddc42e49da1a4ed64b9c279072caab354f6"
strings:
$x1 = "D:\\Work\\Install_Driver\\Driver_helper\\Release\\wccenter.pdb" fullword ascii
$x2 = "wdlogin.exe" fullword wide
$x3 = "wuhost.exe" fullword wide
$x4 = "wrme.exe" fullword wide
$s1 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s2 = " Type Descriptor'" fullword ascii
$s3 = "&Beijing JoinHope Image Technology Ltd.1/0-" fullword ascii
$s4 = "operator co_await" fullword ascii
$s5 = "&Beijing JoinHope Image Technology Ltd.0" fullword ascii
$s6 = "RvVersion" fullword wide
$s7 = " Class Hierarchy Descriptor'" fullword ascii
$s8 = "Base Class Descriptor" ascii
$s9 = "Beijing1" fullword ascii
$s10 = " Complete Object Locator'" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 400KB and
2 of ($x*) and 4 of ($s*)
}

rule SpicyHotPot_KMDF_LOOK {
meta:
description = "SpicyHotPot - KMDF_LOOK.sys: Used to identify browser hijacking
component"
author = "jai-minton"
reference = "https://www.crowdstrike.com/blog/author/jai-minton/"
copyright = "(c) 2020 CrowdStrike Inc."
date = "2020-11-01"
hash1 = "39764e887fd0b461d86c1be96018a4c2a670b1de90d05f86ed0acb357a683318"
strings:
$x1 = "G:\\SVN\\" ascii
$s1 = "TSWebDownLoadProtect.dll" fullword wide
$s2 = "ShellIco.dll" fullword wide
$s3 = "QMLogEx.dll" fullword wide
$s4 = "SSOCommon.dll" fullword wide
$s5 = "TsService.exe" fullword ascii
$s6 = "Hookport.sys" fullword wide
$s7 = "SafeWrapper32.dll" fullword wide
```

```
$s8 = "safemon.dll" fullword wide
$s9 = "iNetSafe.dll" fullword wide
$s10 = "ieplus.dll" fullword wide
$s11 = "wdui2.dll" fullword wide
$s12 = "ExtBhoIEToSe.dll" fullword wide
$s13 = "360NetBase.dll" fullword wide
$s14 = "urlproc.dll" fullword wide
$s15 = "360sdbho.dll" fullword wide
$s16 = "360base.dll" fullword wide
$s17 = "360UDiskGuard.dll" fullword wide
$s18 = "TSClinicWebFix.dll" fullword wide
$s19 = "QMEmKit.dll" fullword wide
$s20 = "WdHPFileSafe.dll" fullword wide
condition:
uint16(0) == 0x5a4d and filesize < 1000KB and
8 of them
}

rule SpicyHotPot_KMDF_Protect {
meta:
description = "SpicyHotPot - KMDF_Protect.sys: Used to identify driver protection and
filtering component"
author = "jai-minton"
reference = "https://www.crowdstrike.com/blog/author/jai-minton/"
copyright = "(c) 2020 CrowdStrike Inc."
date = "2020-11-01"
hash1 = "ab0418eb1863c8a2211d06c764f45884c9b7dbd6d1943137fc010b8f3b8d14ae"
strings:
$x1 = "wdlogin.exe" fullword wide
$x2 = "\\Windows\\System32\\cmd.exe" fullword wide
$x3 = "wuhost.exe" fullword wide
$x4 = "wrme.exe" fullword wide
$x5 = "UpdateSelf.exe" fullword ascii
$x6 = "wccenter.exe" fullword wide
$s1 = "jCloudScan.dll" fullword wide
$s2 = "DSFScan.dll" fullword wide
$s3 = "avescan.dll" fullword wide
$s4 = "\\Cloudcom2.dll" fullword wide
$s5 = "\\Cloudcom264.dll" fullword wide
$s6 = "AVEIEngine.dll" fullword wide
$s7 = "AVEI.dll" fullword wide
$s8 = "BAPI.dll" fullword wide
$s9 = "BAPI64.dll" fullword wide
$s10 = "360Tray.exe" fullword ascii
$s11 = "360Safe.exe" fullword ascii
$s12 = "\\jCloudScan.dll" fullword wide
$s13 = "\\deepscan64.dll" fullword wide
$s14 = "\\deepscan.dll" fullword wide
condition:
uint16(0) == 0x5a4d and filesize < 1000KB and
2 of ($x*) and 6 of ($s*)
}
```

Additional Resources

- *Learn more by visiting the Falcon Complete product webpage.*
- *Read a white paper: CrowdStrike Falcon Complete: Instant Cybersecurity Maturity for Organizations of All Sizes.*
- *Test CrowdStrike next-gen AV for yourself: Start your free trial of Falcon Prevent™.*