

Huntsman Security Advisory: Detecting WannaCry Infected Hosts

OVERVIEW

Huntsman Security is releasing this security advisory due to the extreme and prolific nature of a new type of ransomware that is propagating around the globe. The following advice will assist customers in detecting infected devices and perform rapid containment.

WannaCry is self-propagating ransomware, that exploits an SMB vulnerability within Microsoft Windows to execute commands with system privileges. Multiple initial infection vectors are available, such as a link within an email or PDF, or a password encrypted ZIP file containing a PDF. After infecting a machine WannaCry will begin to encrypt files on local disk drives, network shares and removable storage devices. 2048-bit RSA encryption is used and only specific file types are targeted. Once all files are encrypted the user is presented with a ransom demand.

At this time three variants of the ransomware have been detected, with others expected to be released over time.

MALWARE ANALYSIS

After initial infection some variants of WannaCry first check for the existence of a web site at a hard coded domain. This domain is different in different variants, and in one variant this check is not performed at all. A successful response to this HTTP query causes the ransomware to shutdown, and effectively acts as a kill switch.

Note - It is important that domain queries for, and HTTP requests to, these kill switch domains should be permitted on all outbound firewalls and proxies since an active response will stop the malware executing.

If **no** response is received the malware attempts to move laterally within the network by scanning for other machines on TCP port 445. Any discovered devices are tested for the exploit detailed in MS17-010, which leverages an SMB vulnerability. If vulnerable, an exploit payload is sent to the remote system and executed with System Privileges. See <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx> for further details.

Whilst scanning the network for other potential victims, the malware also encrypts specific file types on local disks, network shares and removable media, generating a random key for the encryption of each file. It also attempts to delete any shadow copies on the machine to make data recovery more difficult. This is achieved using two main commands:

```
vssadmin delete shadows /all /quiet  
wmic shadowcopy delete
```

Once encryption is complete a ransom note is displayed detailing how payment can be made.

DETECTION

A number of indicators of compromise exist for this malware, which can be detected directly by Huntsman® - see Appendix for specific details. Additionally various third party security technologies now detect this malware and raise events and alerts which can be collected by Huntsman® and used as part of a broad detection and remediation strategy.

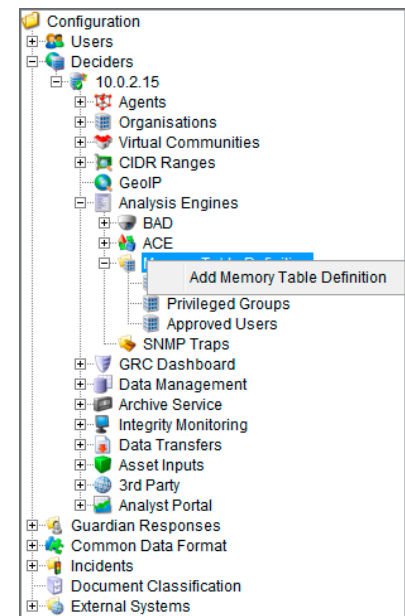
The following sections detail how to integrate this information into Huntsman® and use it within Autonomous Correlation Engine (ACE) rules.

Create an Indicators of Compromise file

Copy the IP address and domain information in the Appendix to a file and save this on the Huntsman® Decider server.

Create a Memory Table

Within the Huntsman® Configuration window expand the **Analysis Engines** section and right click on the **Memory Table Definition** branch.



Memory Table Name:

Data Source Type:

Memory Table Description:

Refresh Interval: Days: Hours: Minutes:

(If set to 0, data will only be loaded once.)

< Back Next > Reset Cancel

Provide a unique name for the memory table, e.g. WannaCry IoCs.

Configure the data source type as 'File' and set the refresh interval to 1 hour.

Click the **Next** button.

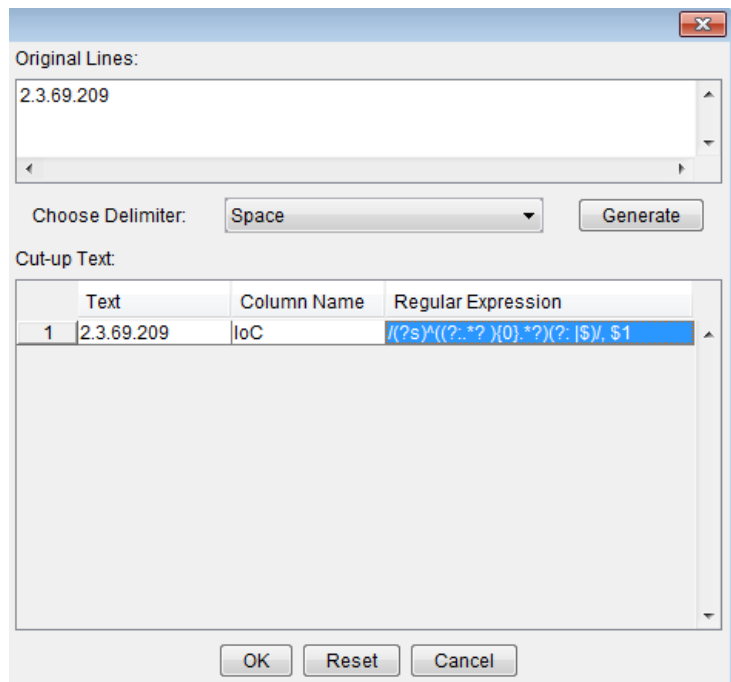
Select the option to make the memory table available to both the Decider and Alerter and browse to the previously created file containing the indicators of compromise.



The screenshot shows a configuration window with three radio button options: 'Decider Only', 'Alerter Only', and 'Decider & Alerter'. The 'Decider & Alerter' option is selected and highlighted with a red box. Below the 'Decider & Alerter' option, the text 'Decider and Alerter are on the same server' is displayed. A 'File' input field contains the path 'C:\Demo\MemoryTables\WannaCry-IoCs.txt' and a 'Browse...' button is visible to its right.

Click **Next** to move to the next part of the configuration. Click the **Auto-Generate** button to open the field definition window and click the **Generate** button.

In the row displayed in the 'Cut-up Text' window define a column name of '**IoC**' - the regular expression for the field will be automatically generated after inputting the column name.



The 'Cut-up Text' window displays a table with the following data:

	Text	Column Name	Regular Expression
1	2.3.69.209	IoC	/(?s)((?:.*?){0}.*?)(?: \$)/, \$1

The 'Generate' button is visible above the table, and 'OK', 'Reset', and 'Cancel' buttons are at the bottom.

Click **OK** to close the window.

Click the **Format Data** button to test that all data is correctly read by the regular expressions – data that will not be added to the memory table will be shown on the Failed Records tab.

File Sample:

```
2.3.69.209
38.229.72.16
46.101.166.19
50.7.161.218
79.172.193.32
81.30.158.223
89.45.235.21
91.121.65.179
128.31.0.39
144.217.254.3
```

Data Formatting Rules:

Column Name	Regular Expression
IoC	/((?s)^((?:.*?)(?:.*?)(?:.*?))?\$), \$1

Successful Records
Failed Records

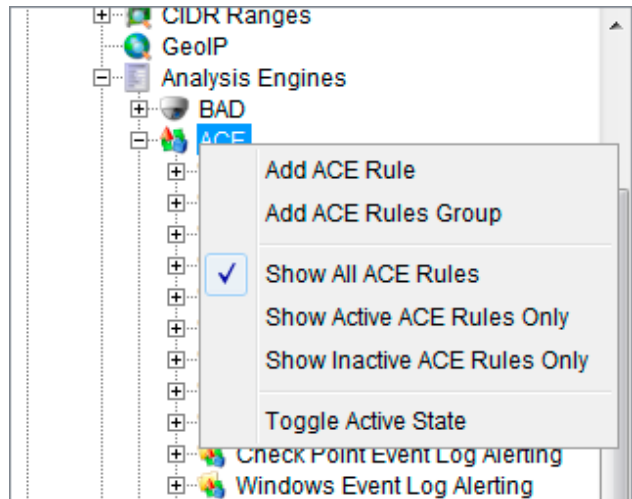
	IoC
20	zu uqensoupsnjapusu ngosunjaew wergwea.com
21	Rphjmrpwmfv6v2e.onion
22	Gx7ekbenv2riuclf.onion
23	57g7spgrzlojinas.onion
24	xxvbrloxvry2c5.onion
25	76jdd2lr2embyv47.onion
26	cwwnhwhlz52maqm7.onion

Click **Finish** to create the Memory Table.

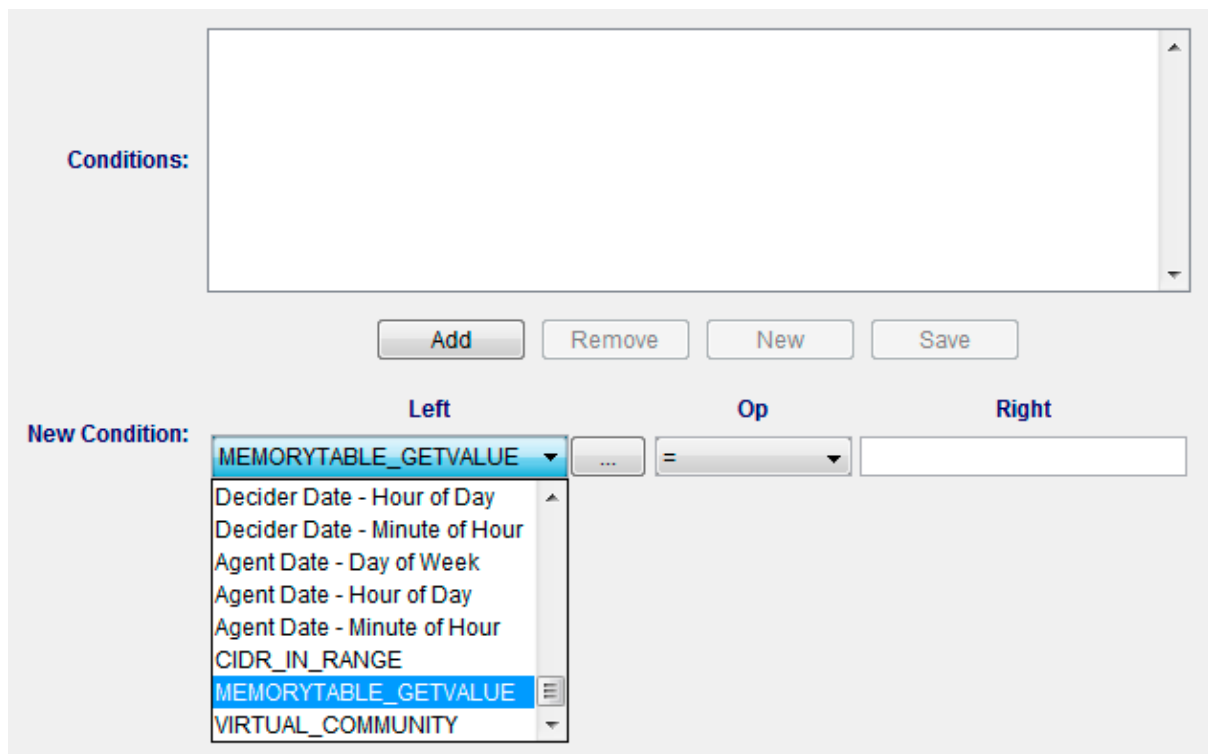
Add memory table queries to ACE rules


Note – The following instructions show the use of the created memory table on the Trigger Definition tab to detect indicators of compromise in event data. In addition to this memory tables can also be used in a similar manner on the Alerting tab to include specific data about the matched IoC in the alert message raised by Huntsman®.

Create a new ACE rule (or edit an existing rule).



On the Trigger Definition tab create a new condition using the MEMORYTABLE_GETVALUE for the left hand side.



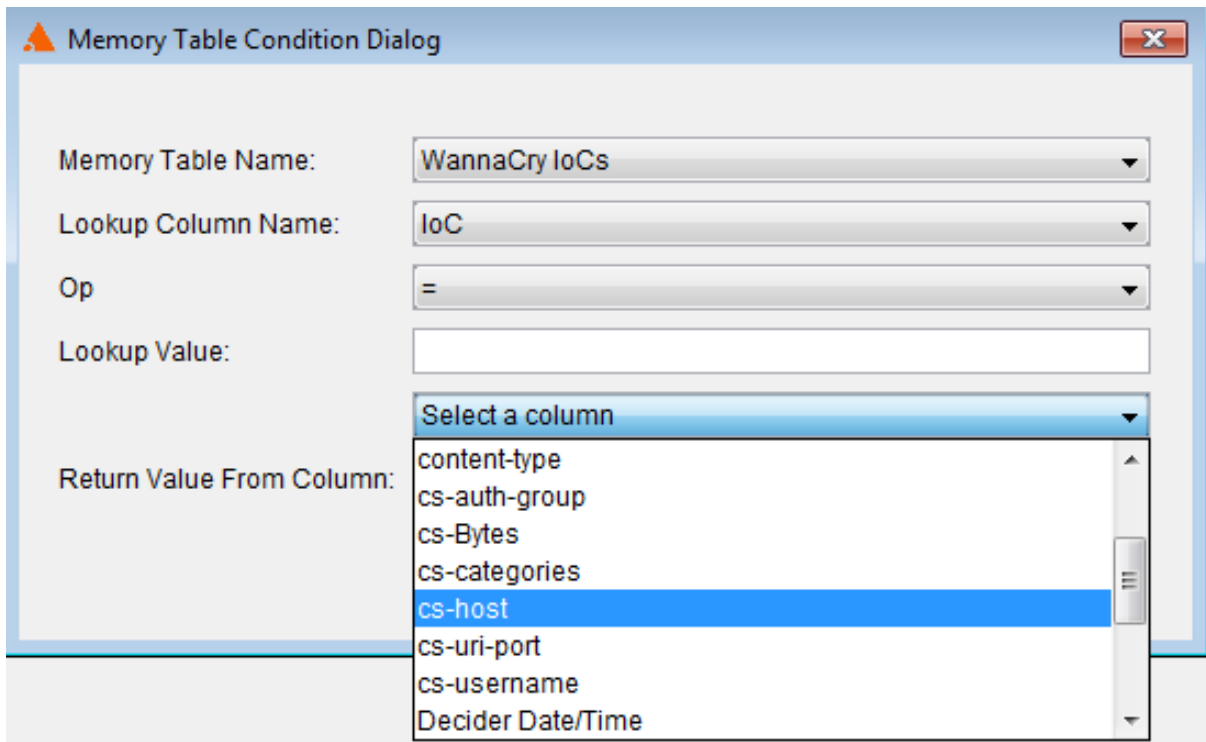
Click the button with the ellipsis () to open the memory table condition dialog and edit the condition for matching event data to memory table values. Define the following:

- Memory Table Name: **WannaCry IoCs**
- Lookup Column Name: **IoC**
- Op: '='
- Return Value From Column: **IoC**

Finally select the appropriate lookup value from the event source the ACE rule is based upon to match against the IoC data in the memory table. The correct column can be selected using the drop down list and will be different for various types of event data, e.g. an IP address in a firewall or a domain name in a web proxy event type. The following sections show the final configuration for different possibilities.

Domain matching

Select the column containing the URL data within the event source, e.g. **cs-host** is the hostname within a client request in Blue Coat event logs.



Memory Table Condition Dialog

Memory Table Name:

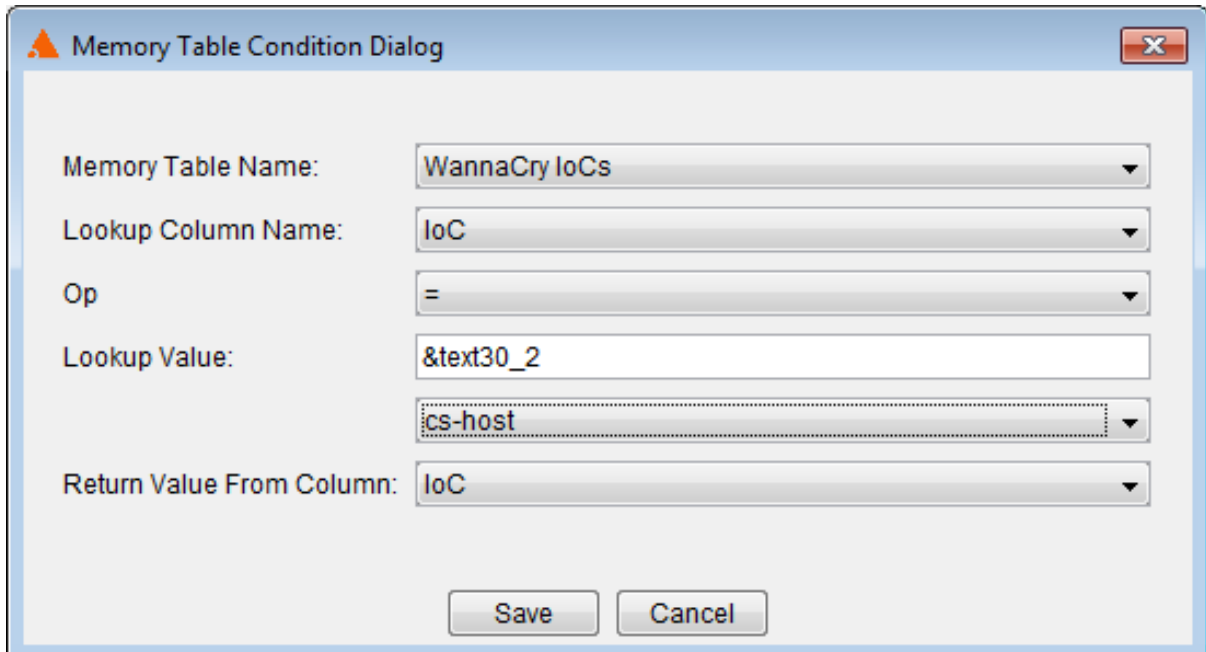
Lookup Column Name:

Op:

Lookup Value:

Return Value From Column:

- content-type
- cs-auth-group
- cs-Bytes
- cs-categories
- cs-host**
- cs-uri-port
- cs-username
- Decider Date/Time



The dialog box is titled "Memory Table Condition Dialog" and contains the following fields:

- Memory Table Name: WannaCry IoCs
- Lookup Column Name: IoC
- Op: =
- Lookup Value: &text30_2
- cs-host
- Return Value From Column: IoC

Buttons: Save, Cancel

Click Save to close the memory table condition dialog and then set the operator in the condition to **'is not null'**.



The dialog box shows a list of conditions and a "New Condition" section.

Conditions:

Add Remove New Save

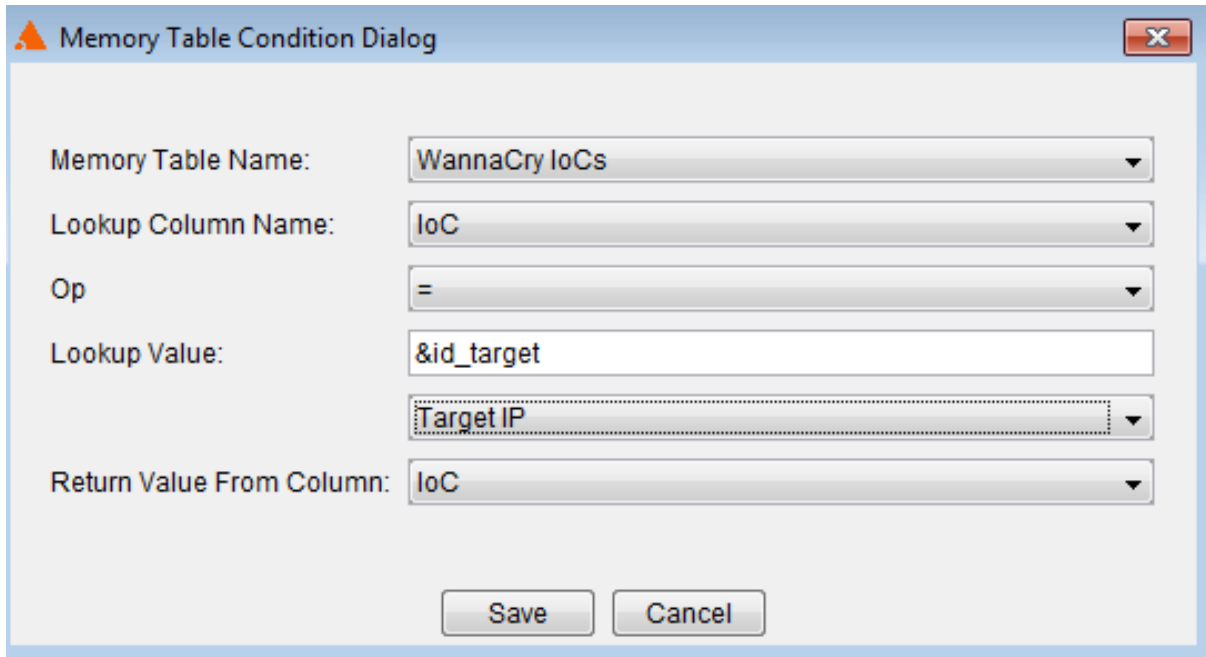
New Condition:

Left	Op	Right
MEMORYTABLE_GETVALUE	is not null	

If a domain in the event source is found to match one listed in the memory table list of IoCs the response from the memory table query will not be null which will cause a positive match with the right-hand side of the condition statement. If a match is not found then the query will return a 'null' and no match will be made.

IP address matching

Select the column containing the IP address data within the event source, e.g. Target IP is the destination IP address of a connection within many event types.



The dialog box is titled "Memory Table Condition Dialog" and contains the following fields:

- Memory Table Name: WannaCry IoCs
- Lookup Column Name: IoC
- Op: =
- Lookup Value: &id_target
- Target IP (selected in a dropdown menu)
- Return Value From Column: IoC

Buttons: Save, Cancel

Click **Save** to close the memory table condition dialog and then set the operator in the condition to **'is not null'**.



The dialog shows a list of conditions (currently empty) and a "New Condition" section with the following configuration:

Left	Op	Right
MEMORYTABLE_GETVALUE	...	is not null

If a destination IP address in the event source is found to match one listed in the memory table list of IoC's the response from the memory table query will not be null which will cause a positive match with the right-hand side of the condition statement. If a match is not found then the query will return a 'null' and no match will be made.

Updates

As new variants of WannaCry are released updates to the WannaCry indicators of compromise file will be required. This new information should simply be added to the file as required and Huntsman[®] will automatically update the Memory Table data when it next reads the file.

SUMMARY

Huntsman[®]'s Memory Table functionality allows customers to detect WannaCry indicators of compromise within existing event data. Detection can be performed either by extending existing alerting rules, or by creating dedicated rules focused on this threat.

For further information on WannaCry please see:

[Http://Blog.Talosintelligence.Com/2017/05/Wannacry.Html](http://Blog.Talosintelligence.Com/2017/05/Wannacry.Html)

<https://blog.comae.io/wannacry-the-largest-ransom-ware-infection-in-history-f37da8e30a58>

<https://blog.comae.io/wannacry-new-variants-detected-b8908fefa7e>

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/?utm_source=t.co&utm_medium=referral

REVISION HISTORY

Date	Detail
14 May 2017	Initial document release
15 May 2017	Additional IoC IP addresses added Additional kill switch domain added Check Point IPS corrections and additions

APPENDIX – INDICATORS OF COMPROMISE

The following indicators of compromise can be used by Huntsman[®] to detect the presence of WannaCry on an infected system.

IP Addresses

2.3.69.209	5.9.158.75
38.229.72.16	50.7.151.47
46.101.166.19	51.254.115.225
50.7.161.218	62.138.7.231
79.172.193.32	83.162.202.182
81.30.158.223	84.80.80.69
89.45.235.21	91.134.139.207
91.121.65.179	94.23.173.93
128.31.0.39	94.23.204.175
144.217.254.3	104.238.167.111
146.0.32.144	136.243.176.148
149.202.160.69	138.201.132.17
188.138.33.220	144.76.42.239
188.166.23.127	163.172.35.247
193.23.244.244	163.172.153.12
197.231.221.221	163.172.185.132
212.47.232.237	171.25.193.9
213.61.66.116	178.62.173.203
217.79.179.177	185.97.32.18
	188.42.216.83
	198.199.90.205
	217.172.190.251

Kill Switch Domains

luqerfsodp9ifjaposdfjhgosurijfaewrwegwea.com
lfferfsodp9ifjaposdfjhgosurijfaewrwegwea.com
ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com

Tor Domains

rphjmrpwmfv6v2e.onion
gx7ekbenv2riucmf.onion
57g7spgrzlojinas.onion
xxlvbrloxvriy2c5.onion
76jdd2ir2embyv47.onion
cwwnhwhlz52maq7.onion

APPENDIX – THIRD PARTY IPS DETECTIONS

Snort Rules

- 41978
- 42329-42332
- 42340

Check Point IPS Protections

- Microsoft Windows EternalBlue SMB Remote Code Execution – CPAI-2017-0332
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0143) – CPAI-2017-0177
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0144) – CPAI-2017-0198
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0145) – CPAI-2017-0200
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0146) – CPAI-2017-0203
- Microsoft Windows SMB Information Disclosure (MS17-010: CVE-2017-0147) – CPAI-2017-0205
- Microsoft Windows NT Null CIFS Sessions
- Non-Compliant CIFS

Trend Micro TippingPoint Filters

- 5614, 27433, 27711, 27935, 27928
- ThreatDV Filter 30623
- Policy Filter 11403

McAfee NPS Signatures

- 0x43c0b800 - NETBIOS-SS: Windows SMBv1 identical MID and FID type confusion vulnerability (CVE-2017-0143)
- 0x43c0b400 - NETBIOS-SS: Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144)
- 0x43c0b500 - NETBIOS-SS: Windows SMB Remote Code Execution Vulnerability (CVE-2017-0145)
- 0x43c0b300 - NETBIOS-SS: Microsoft Windows SMB Out of bound Write Vulnerability (CVE-2017-0146)
- 0x43c0b900 - NETBIOS-SS: Windows SMBv1 information disclosure vulnerability (CVE-2017-0147)
- A dedicated UDS is also available from KB55447 for supported customers