Your documents, photos, databases and other important files have been encrypted!

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

1. http://cerberhhyed5frqa.xmfr0.win/30EF-3C4E-A460-005E-93C9
3. http://cerberhhyed5frqa.3051ot.win/30EF-3C4E-A460-005E-93C9
Your documents, photos, databases and other important files have been encrypted!

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

3. http://cerberhhyed5frqa.3051ot.win/30EF-3C4E-A460-005E-93C9

Uh oh.
Ransomware Lab

Hi! I’m an endpoint!

we8106desk

webbackupsvr1 WE9041SRV

wenessus1 192.168.2.50

LAN

suricata-ids

Fortigate NG Firewall 192.168.250.1

Internet

OD-FM-CONF-NA (AWS)

splunk-02

webackupsvr1 WE9041SRV

wenessus1 192.168.2.50

LAN

suricata-ids

Fortigate NG Firewall 192.168.250.1

Internet

OD-FM-CONF-NA (AWS)

Hi! I’m an endpoint!

we8106desk

webbackupsvr1 WE9041SRV

wenessus1 192.168.2.50
USB Drive with Malicious Word Macro Doc

- we8106desk
- WE9041SRV 192.168.250.1
- wenessus1
- suricata-ids
- Fortigate NG Firewall 192.168.250.1
- Internet
- OD-FM-CONF-NA (AWS)
- splunk

- LAN
- WESIFTSVR1
- WESTOQSVR1

- Infected.dotm (via USB drive)
SELECT "Command", "ParentCommandLine", STRLEN(Command) AS longtell FROM events WHERE "EventID"=''1' AND "host2"='we8105desk' AND longtell>500
Related: Finding (very) long command lines
Event Chaining - Identifying Parent/Child Processes

• What is the parent process ID of 121214.tmp?
  • 3968
Identifying Removable Media

• What is the name of the USB key inserted by Bob Smith?
I Know Nothing About USB Keys!!!

Where Do I Start?

- Start by googling “finding windows registry usb name site:microsoft.com”


- I see something called FriendlyName
  - Continue researching?
  - Move Forward with that hypothesis
Use index and windows registry sourcetype as our boundary
Refine that with the term friendlyname we found on the msdn site
Let’s see what we get
  • Maybe we refine (too large of a result set returned), maybe not
Question asked about Bob Smith, so looking at specific hosts that he has touched would be a good thing to target our search a bit more

New Search

index=main  sourcetype="winregistry"  friendlyname

2 events (8/24/16 12:00:00.000 AM to 8/25/16 12:00:00.000 AM)  No Event Sampling
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>we8105desk</td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>WinRegistry</td>
<td></td>
</tr>
<tr>
<td>sourcetype</td>
<td>WinRegistry</td>
<td></td>
</tr>
<tr>
<td>action</td>
<td>modified</td>
<td></td>
</tr>
<tr>
<td>data</td>
<td>MIRANDA_PRI</td>
<td></td>
</tr>
<tr>
<td>data_type</td>
<td>REG_SZ</td>
<td></td>
</tr>
<tr>
<td>dest</td>
<td>we8105desk</td>
<td></td>
</tr>
<tr>
<td>event_status</td>
<td>(0): The operation completed successfully.</td>
<td></td>
</tr>
<tr>
<td>eventtype</td>
<td>winregistry_windows (change endpoint or windows)</td>
<td></td>
</tr>
<tr>
<td>key_path</td>
<td>HKLM\system\controlset001\enum\wpdbusenumroot\umb&amp;37c186b&amp;8&amp;storage#volume#_??_usbstor#disk&amp;ven_generic&amp;prod_flash_disk&amp;rev_8.0?7?d96119680&amp;88#friendlyname</td>
<td></td>
</tr>
<tr>
<td>msg</td>
<td>The operation completed successfully.</td>
<td></td>
</tr>
<tr>
<td>object</td>
<td>friendlyname</td>
<td></td>
</tr>
<tr>
<td>object_category</td>
<td>registry</td>
<td></td>
</tr>
<tr>
<td>object_path</td>
<td>HKLM\system\controlset001\enum\wpdbusenumroot\umb&amp;37c186b&amp;8&amp;storage#volume#_??_usbstor#disk&amp;ven_generic&amp;prod_flash_disk&amp;rev_8.0?7?d96119680&amp;88#</td>
<td></td>
</tr>
<tr>
<td>pid</td>
<td>708</td>
<td></td>
</tr>
<tr>
<td>process_image</td>
<td>c:\Windows\System32\svchost.exe</td>
<td></td>
</tr>
<tr>
<td>registry_key_name</td>
<td>2&amp;37c186b&amp;8&amp;storage#volume#_??_usbstor#disk&amp;ven_generic&amp;prod_flash_disk&amp;rev_8.0?7?d96119680&amp;88#</td>
<td></td>
</tr>
<tr>
<td>registry_path</td>
<td>HKLM\system\controlset001\enum\wpdbusenumroot\umb&amp;37c186b&amp;8&amp;storage#volume#_??_usbstor#disk&amp;ven_generic&amp;prod_flash_disk&amp;rev_8.0?7?d96119680&amp;88#</td>
<td></td>
</tr>
<tr>
<td>registry_type</td>
<td>SetValue</td>
<td></td>
</tr>
<tr>
<td>registry_value_data</td>
<td>MIRANDA_PRI</td>
<td></td>
</tr>
<tr>
<td>registry_value_name</td>
<td>friendlyname</td>
<td></td>
</tr>
</tbody>
</table>
Identifying Removable Media

• What is the name of the USB key inserted by Bob Smith?
  • MIRANDA_PRI
Communication to Download Cryptor Code

we8106desk - webackupsvr1 - WE9041SRV - wenessus1 - 192.168.2.50

LAN

we8106desk

webackupsvr1

WE9041SRV

wenessus1 - 192.168.2.50

suricata-ids

Fortigate NG Firewall - 192.168.250.1

Internet

OD-FM-CONF-NA (AWS)

webackupsvr1

WE9041SRV

wenessus1 - 192.168.2.50

suricata-ids

Fortigate NG Firewall - 192.168.250.1

Internet

OD-FM-CONF-NA (AWS)
Identifying Cryptor Code Filename and Origin

• The malware downloads a file that contains the Cerber ransomware cryptor code. What is the name of that file?
<table>
<thead>
<tr>
<th>dest</th>
<th>count</th>
<th>values(url)</th>
</tr>
</thead>
<tbody>
<tr>
<td>104.107.45.91</td>
<td>3</td>
<td><a href="http://go.microsoft.com/fwlink/">http://go.microsoft.com/fwlink/</a></td>
</tr>
</tbody>
</table>
| 199.117.103.168| 10 | http://crl.microsoft.com/pki/crl/products/CodeSignPCA.crl  
                       |                                  | http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl  
                       |                                  | http://crl.microsoft.com/pki/crl/products/MicCodeSignPCA_08-31-2010.crl  
                       |                                  | http://crl.microsoft.com/pki/crl/products/WinPCA.crl  
                       |                                  | http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl  
| 199.117.103.176| 2   | http://crl.microsoft.com/pki/crl/products/CodeSignPCA.crl  
| 204.79.197.200| 3   | http://www.bing.com/favicon.ico                  |
| 23.2.143.41   | 5     | http://go.microsoft.com/fwlink/                  |
| 23.2.192.158  | 1     | http://www.microsoft.com/pki/CRL/products/Microsoft%20Windows%20Hardware%20Compatibility%20PCA(1).crl  
| 23.6.155.123  | 1     | http://go.microsoft.com/fwlink/                  |
| 23.63.188.67  | 1     | http://www.microsoft.com/pki/CRL/products/Microsoft%20Windows%20Hardware%20Compatibility%20PCA(1).crl  
| 37.187.37.150 | 1     | http://solidatedeportxmate.org/mhtr.jpg         |
| 54.148.194.58 | 1     | http://ipinfo.io/json                            |
| 67.132.183.25 | 5     | http://shell.windows.com/0409/fileassoc.css     
                       |                                  | http://shell.windows.com/HeaderSlice.jpg  
                       |                                  | http://shell.windows.com/fileassoc/fileassoc.asp  
| 92.222.104.182| 1     | http://92.222.104.182/mhtr.jpg                   |
SELECT "URL", "site", COUNT(*) as num_sites FROM events WHERE sourceip='192.168.250.100' and "Vendor"='Suricata' AND NOT (site ILIKE '%live%') AND NOT (site ILIKE '%bing%') AND NOT (site ILIKE '%sym%') AND NOT (site ILIKE '%digicert%') AND NOT (site ILIKE '%omniroot%') AND NOT (site ILIKE '%acronis%') AND NOT (site ILIKE '%windows%') AND NOT (site ILIKE '%microsoft%') AND NOT (site ILIKE '%msn%') AND site IS NOT NULL GROUP BY site,URL ORDER BY num_sites DESC
The command line then executes wscript [wscript.exe PID: 1432] with the dropped vbs file [28156.vbs], which in turn downloads the first Cerber Ransomware malicious file [Fig. 4] [272730.tmp] while accessing the following sites:

- Solidaritedeproximitel.]org/mhtr.jpg
- 92.222.104[.]182/mhtr.jpg
SELECT "Message" FROM events
WHERE sourceip='192.168.250.100' AND "Vendor"='Fortinet' AND severity>'8'
GROUP BY Message
Local File Encryption

- **we8106desk**
- **webbackupsvr1**
- **WE9041SRV**
- **wenessus1 192.168.2.50**
- **LAN**
- **STM**
- **splunk-02**
- **WESIFTSVR1**
- **WESTOQSVR1**
- **suri-cata-ids**
- **Fortigate NG Firewall 192.168.250.1**
- **Internet**
- **OD-FM-CONF-NA (AWS)**
Our Initial Search
Event ID 1: Process creation
- The process creation event provides extended information about a newly created process.
- The full command line provides context on the process execution.

Event ID 2: A process changed a file creation time
- The change file creation time event is registered when a file creation time is explicitly modified by a process.
- This event helps tracking the real creation time of a file.
<table>
<thead>
<tr>
<th>result.file_path.keyword: Descending</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Sysmon_Eula.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Sysmon\AuditPol_AFTER_WE8105DESK.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Sysmon\AuditPol_BEFORE_WE8105DESK.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Sysmon\Eula.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Office 2010 Pro\Key.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Project 2010\Key.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset_Help.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset_readme.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\Help.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\Lang\CHIPARA_license.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\Lang\CHIPARBL\license.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\Lang\CHIPARA\license.txt</td>
<td>1</td>
</tr>
<tr>
<td>C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\Lang\CHIPARBL\license.txt</td>
<td>1</td>
</tr>
</tbody>
</table>
Wildcard on a File Directory Structure

\texttt{\textit{windows\_xml.System.EventID:2 AND result.file\_path:"C:\Users\bob.smith.WAYNECORPINC\" AND *.txt}}
Damage Assessment - Identifying Encrypted Text Files

- The Cerber ransomware encrypts files located in Bob Smith's Windows profile. How many .txt files does it encrypt?
  - 406
Lateral Move to Fileshare

- **webackupsvr1**
- **WE9041SRV**
- **wenessus1 192.168.2.50**
- **splunk**
- **Fortigate NG Firewall 192.168.250.1**
- **suricata-ids**
- **OD-FM-CONF-NA (AWS)**
- **LAN**
- **Internet**
- **we8106desk**
- **STM**
- **splunk-02**
- **WESIFTSVR1 WESTOQSVR1**
Searching with the Correct Destination
Want this data?

https://goo.gl/14rmuU