# **Recent Posts**

months threatresearch.ext.hp.com/investigating-threats-in-hp-sure-controller-4-2/

June 21, 2020

#### HP Threat Research Blog • Investigating Threats in HP Sure Controller 4.2: TVRAT



# Investigating Threats in HP Sure Controller 4.2: TVRAT

<u>HP Sure Click Enterprise</u> captures a wealth of information about threats at the time of execution. HP Sure Controller is a management interface that is designed to help security analysts to quickly understand the nature of threats isolated by HP Sure Click Enterprise. In this blog post, we describe a typical investigation workflow, highlighting some of the useful features and views built into HP Sure Controller that enable security teams to investigate threats efficiently.

#### Background

The attack was an attempted intrusion against a financial organisation in January 2020 that was stopped by HP Sure Click Enterprise. The delivery method of the downloader, a malicious Microsoft Word document, was notable because the attacker disguised it as a resume and then uploaded it to a legitimate job portal website. It was subsequently downloaded and opened by a member of the target organisation's human resources department, bypassing email gateway and web proxy security controls. Ultimately, the downloader delivered <u>TVRAT</u> (also known as Spy-Agent), a remote access Trojan that is capable of remotely controlling an infected PC, transferring files and accessing the victim's microphone and webcam.

#### Threat Table

The threat table view lists alerts generated by HP Sure Click Enterprise. To prioritise which activity to investigate, you can apply filters to the table by clicking on the 'Add Filter' button. You can also create and apply labels to alerts to organise them. Figure 1 shows a filter applied for alerts containing high severity events that HP Sure Click Enterprise has classified as malicious (true positive) or unknown. Two alerts for malicious Microsoft Word documents match this filter criteria.

| =          | Sure Cont        | troller            |                       |                       |         |             |             |             |              |                   |      |       | (2)         |         |       |
|------------|------------------|--------------------|-----------------------|-----------------------|---------|-------------|-------------|-------------|--------------|-------------------|------|-------|-------------|---------|-------|
| 0          | Threats          |                    |                       |                       |         |             |             | Hash Search |              |                   |      |       |             |         | Q     |
| Q          |                  |                    |                       |                       |         |             |             |             |              |                   |      |       |             |         |       |
| œ₽         | = <u></u>        | Classification 💌   | Label 🔻 Options       | •                     |         |             |             |             | Save         | d Views: Default* | •    | Colur | mns 🔻 🕣 🗊   | +       | ≡+    |
| $\bigcirc$ |                  |                    |                       |                       |         |             |             | 0           |              |                   |      |       |             |         |       |
|            | Status: Act      | Add Filter         | + Classification: Unk | nown, True Positive 🔻 | ×) Inst | itallation: | Ŧ           | (×) Receive | d: Jan 1, 20 | 20 - Jan 31, 2020 | • (× | 9     |             | 2 resi  | ults  |
|            | Severity: H      | ligh ▼ (X)         |                       |                       |         |             |             |             |              |                   |      |       |             |         |       |
| ∜          | Show 100 e       | entries 🔹 1 to 2 d | of 2                  |                       |         |             |             |             |              |                   | M    | ۹     | 1 of 1      | ►       |       |
|            |                  | Labels             | Received 🗸            | Application           | T)      | lype 🜲      | Resources 🜲 | Severity    | \$           | Installation      |      | \$    | Assessments |         | \$    |
|            | П                | •                  | Jan. 13, 2020, 7:41 p | Microsoft Word        | ls      | solated     | .com,       | High        |              |                   |      |       |             | 3 publi | ished |
|            | 🔲 ТР             | •                  | Jan. 13, 2020, 6:54 p | Microsoft Word        | Is      | solated     | .com,       | High        |              |                   |      |       |             | 3 publ  | ished |
|            | 4                |                    |                       |                       |         |             |             |             |              |                   |      |       |             |         | ŀ     |
|            | Show 100 e       | entries 🔻 1 to 2 d | of 2                  |                       |         |             |             |             |              |                   |      | -     | 1 of 1      | ►       |       |
|            |                  |                    |                       |                       |         |             |             |             |              |                   |      |       |             |         |       |
|            |                  |                    |                       |                       |         |             |             |             |              |                   |      |       |             |         |       |
|            | HP Sure Controll | er © HP Inc. 2020  |                       |                       |         |             |             |             |              |                   |      |       |             |         |       |

Figure 1 – The threat table view of alerts in HP Sure Controller.

#### Threat View – Summary Tab

Clicking on one of the alerts opens the threat view 'Summary' tab, which gives an overview of information about the alert to enable an investigator to understand the threat quickly. The information about the alert shown on the 'Summary' tab includes:

- · the hostname of the endpoint
- · the user of the endpoint at the time of the activity
- the names and hash values of resources that triggered the alert, e.g. filenames and URLs
- the classification given by HP Sure Click Enterprise, i.e. True Positive, False Positive, Unknown
- the time and duration of the activity, including if the alert was uploaded to Threat Cloud for additional analysis
- <u>MITRE ATT&CK</u> techniques observed during the lifetime of the trace
- · files written to the filesystem during the lifetime of the micro-VM
- · DNS events
- · a process interaction graph showing parent-child relationships between processes
- · geolocation and a summary of network activity
- · a log of recent activity that allows HP Sure Controller users to comment on the threat

The Summary tab also allows users to download the files that triggered the alert (.VMM file) and the micro-VM trace (.XEVTS and .DEVTS files) at the time of the activity, in case there is a need to analyse the threat using other tools.

| Sure Controller   |  |   |   | 0                      |
|---|--|---|---|------------------------|
| 2 of 2 ^ Y 5 Filtered on Classification ,   | Status , Installation , Received   | 1, Severity   |   |                        |
| Microsoft Word Detection: Isolativ<br>Threat UUID:  | on 4.1.7.5326 True Posit   | tive  | Download 🔻 Label 💌 Assign 💌 TP  | FP 🗘 🗐                 |
| 💽 SUMMARY 🔟 GRAPH   | FILES  | ⊞ BEHAVIORAL 🌻 NETWORK                                    | E METADATA  |                        |
| seventy total events<br>High 2,956  | HIGH SEVERITY EVENTS   |   |   |                        |
| n 1   |  | Threat Indicators<br>Threat Intelligence Service Response | MITRE ATT&CK'   |                        |
| Threat triggered for Microsoft Word because 1<br>activities were detected. The triggering event v<br>the 'invokes a modified file' behavior. This even<br>micro-VM had been running for 23 seconds. | 3 different suspicious<br>was reported because of<br>nt occurred after the | Currently no threat indicators to report                  | TA0001 - Initial Access 2<br>T1192 - Spearphishing Link 2                                       | 1                      |
| Initiated By: (Not Provided)<br>Threat Response: Isolated   |  |   | TA0002 - Execution [2]<br>T1106 - Execution through API [2]<br>T1129 - Execution through Module | 2  <br>Load 🖸          |
| Detected:         January 13, 2020 6:53 p.           Received:         January 13, 2020 6:54 p.           Updated:         March 23, 2020 5:40 p.m.   | m.<br>m.   |   | TA0003 - Persistence 2<br>TA0004 - Privilege Escalation 2                                       | 0                      |
| Threat Analysis Submitted: March 23, 2020 5:38 p.m. Perceived: March 23, 2020 5:40 p.m.   |  |   | TA0005 - Defense Evasion [2]<br>T1107 - File Deletion [2]                                       | 2                      |
|   | •  |   | TA0006 - Credential Access 🗹  | 0                      |
| 00:04:17  | Ann  | ,   | TA0007 - Discovery 🖄<br>T1057 - Process Discovery 🚺<br>T1082 - System Information Discov        | 2  <br>ery [2]         |
|   | <b>⊘</b> 6.58 p.m.   |   | TACOOB - Lateral Movement [2]<br>T1021 - Remote Services [2]<br>T1105 - Remote File Conv. (2)   | 2                      |
| Resources   | 2 –  |   | TA0009 - Collection   | 0                      |
| https://employers.  |  |   | TA0011 - Command and Control [2]<br>T1094 - Custom Command and Con                              | 8 I<br>trol Protocol 🖸 |
| Blacklistable Files   | 5 –  |   | T1105 - Remote File Copy Z  |                        |
| ResumeGabriellaGrey.doc   | 🖺 c6441cf 🏴  |   | T1104 - Multi-Stage Channels 🖸<br>T1071 - Standard Application Laver                            | Protocol 🖸             |
| wpvnetwks.exe   | n cc82d62  |   | T1132 - Data Encoding 🖾<br>T1079 - Multilayer Encryption 🖄                                      |                        |
| X6IPAYFwa2HOpeVE3gLRKCMb[1].dll   | f5b7c4b 🏲  |   | TA0010 - Exfiltration 🖸   | 0                      |
| KBuGDorsqg.dll  | f5b7c4b 🏲  |   | TA0040 - Impact 🗹   | 0                      |
| 🌰 msi.dll   | 🖬 f5b7c4b 🏲  |   |   |                        |

Figure 2 – The threat view of an alert in HP Sure Controller.

The severity of this alert is 'High' which indicates that suspicious behaviour commonly associated with malware occurred during the lifetime of the micro-VM.

In the 'Resources' section (Figure 2) a URL and a file called ResumeGabriellaGrey.doc are listed. The URL indicates that the user visited the website then downloaded and opened the file. To the left of the filename is a grey-coloured cloud icon which indicates that the file's hash value is not currently recognised by Threat Cloud. However, a file called wpvnetwks.exe listed in the 'Blacklistable Files' section (Figure 2) is known by Threat Cloud. It was marked as clean, as indicated by the green cloud icon. An unknown dynamic link library (DLL) was also written to the filesystem three times during the trace:

- msi.dll
- KBuGDorsqg.dll
- X6IPAYFwa2HOpeVE3gLRKCMb[1].dll

Looking up the hash value of wpvnetwks.exe in a malware repository such as <u>VirusTotal</u> reveals that the file is a <u>legitimate digitally-signed</u> <u>executable</u> used by TeamViewer, a remote access tool. In the 'DNS Events' section (Figure 3) you can see that seven suspicious DNS queries were made, including to domains associated with TeamViewer infrastructure.



#### Figure 3 – Continued threat view of an alert in HP Sure Controller.

The process interaction graph shows the parent-child relationships between processes created in the micro-VM and is designed to enable investigators to identify suspicious process relationships visually. You can see that a Microsoft Word process, winword.exe, created two child processes, wpvnetwks.exe and regsvr32.exe. Given our suspicion that wpvnetwks.exe is a file related to TeamViewer, it is unlikely that Microsoft Word would run this program legitimately. The other process created by Microsoft Word is also highly suspicious because regsvr32.exe is a tool that can be used to run malicious DLLs (T1117). At this stage, it seems a reasonable hypothesis that regsvr32.exe was used to run the DLL listed in the 'Blacklistable Files' section.

Despite TeamViewer being a legitimate tool, the summary of the activity in this alert suggests that it was likely used for a malicious purpose. We can inspect the micro-VM's activity in granular detail using the other tab views to confirm this assessment.

#### Threat View – Graph Tab

The Graph tab displays a timeline view of the events that occurred in the micro-VM, which enables investigators to trace through activity event by event to understand it in more detail. Clicking on an event in the left-hand column highlights it on the timeline. High severity events are indicated by their pink-coloured background. The Graph view is often useful to understand the context of events, for example, by

| $\equiv$      | Sure Controller   |  |  | ?   ▼              |
|---------------|---|--|--|--------------------|
| 0             | × 2 of 2 ^ v 5  | Filtered on Classification , Status , Installation , R   | celved , Severity  |                    |
| <b>∂</b><br>₽ | Microsoft W   | Ord Detection: Isolation 4.1.7.5326 Tru  | Download V Label V Assign V FP FP  | Q                  |
| $\bigcirc$    | SUMM/   | ARY 🔟 GRAPH 🗐 FILES  | I BEHAVIORAL 👳 NETWORK 🗏 METADATA  |                    |
| \$P #i □      | Behavioral Events<br>Total events: 2943   | 2901 events hidden by filters  | THREAT   | +                  |
|               | WINWORD.EXE PID: 5 TYPE ACTION THREAT INTEL SOURCE PATH TARGET PATH FILE SIZE SHA-256 WINWORD.EXE PID: 5 TYPE ACTION THREAT INTEL SOURCE PATH TARGET PATH TARGET PATH TARGET PATH TARGET PATH | 008 (-00:00:00:235)         Image: Comparison of Compa | WINWORLEXE         0 | -<br>+:<br>(;<br>i |
|               | WINWORD,EXE PID: 5<br>TYPE<br>ACTION<br>DESCRIPTION<br>API<br>PID<br>Wpvnetwks.exe PID: 1<br>TYPE<br>ACTION<br>THREAT INTEL<br>SOURCE PATH<br>TARGET PATH<br>FILE SIZE<br>SHA-255             | 008 (+00:00:00.031)<br>User Hook<br>API Call<br>Suspended Process Created<br>CreateProcess<br>2160<br>1160 (+00:00:00.031)<br>Process<br>Load User Space<br>Unknown<br>VUsers(bruser1729(AppData)Roaming(Windows<br>Media Player(msi.dll<br>Users(bruser1729(AppData)Roaming(Windows<br>Media Player(msi.dll<br>296192<br>15b7c4303039021567e5bdb768c9ca3407a05<br>005d0da5c1dfaa88a93939436bb   | wpmetwks.exe<br>WINWORD.EXE<br>splwow64.exe  |                    |

#### examining the activity that occurred immediately before and after a high severity event.

Figure 4 – Graph view of an alert in HP Sure Controller.

In Figure 4, you can see that a high-severity event was generated when winword.exe executed wpvnetwks.exe from C:\Users\bruser1729\AppData\Roaming\Windows Media Player\. Looking at the previous events reveals that winword.exe also launched regsvr32.exe, which in turn ran one of the copies of the unknown DLL, KBuGDorsqg.dll. One of the libraries that wpvnetwks.exe loads at runtime is msi.dll, a legitimate Microsoft DLL located in the System32 directory. However, the events after wpvnetwks.exe was executed shows evidence of <u>DLL side-loading (T1073)</u>. Another copy of the unknown DLL, msi.dll, was loaded into the process of wpvnetwks.exe instead of the legitimate msi.dll.

#### Threat View – Behavioural Tab

The Behavioural tab displays micro-VM events in a chronological table and allows investigators to filter on events based on properties such as type, action, severity and name. For example, Figure 5 shows the Behavioural view that has been filtered to only show process execution and network events. You can see that approximately seven seconds before the high severity event, HP Sure Click Enterprise saw an HTTPS connection to morteson[.]com (194.67.90[.]67). Afterwards, KBuGDorsqg.dll was written to the filesystem in two locations, which suggests that the file was downloaded from morteson[.]com. The downloaded file was then run using regsvr32.exe and was shortly followed by a DNS query to creatorz123[.]top (176.121.14[.]139), indicative of command and control (C2) check-in activity. Tracing through the events also shows network activity relating to teamviewer[.]com, which corroborates the hypothesis that wpvnetwks.exe is a TeamViewer binary.

| $\equiv$       | (hp) | Sure          | 2 Controller   |  |   |  |  |                                       |  |           |           | 0        |   | Ŧ |
|----------------|------|---------------|--|--|---|--|--|---------------------------------------|--|-----------|-----------|----------|---|---|
| 0              | × 2  | of 2          | ∧ ∨ 5   Filtered on Classifica                               | ation , Status , Installation , Received , | Severity  |  |  |                                       |  |           |           |          |   |   |
| <b>ර්</b><br>⊡ |      | Mic<br>Threat | rosoft Word Detection: H                                     | solation 4.1.7.5326 True Positiv           | 2   |  | Download 👻                               | Label                                 | Assign 🔻                               | ТР        | FP        | ବ        | Ē | ⑪ |
| $\bigcirc$     |      |               | SUMMARY  | RAPH 🗐 FILES                               | ⊞ BEHAVIORAL  | ⊕ NETWORK  | 🗐 ма                                     | TADATA                                |  |           |           |          |   |   |
|                |      | Jur           | np to triggering Clear selected                              |  |   |  |  |                                       |  |           |           |          |   |   |
| 아<br>아         |      | Eve           | ent Type: Process, Network, DNS, File 🔹<br>dt: No filter 🔹 🛞 | Event Action Type: Execute, I              | IS Request, I • 🛞 Process: No filter • 🛞 Severity: No filter • 🛞 Selected: No filter • 🛞      |  |  |                                       |  |           | 549/3     | 2943     |   |   |
|                |      |               | Time from triggering event                                   | Process                                    | Details   |  |  |                                       |  |           |           |          |   |   |
|                |      |               | -00:00:07.570  | SYSTEM                                     | ACTION<br>PROTOCOL<br>HTTP METHOD<br>URL<br>DESTINATION IP<br>SOURCE PORT<br>DESTINATION PORT | NETWORK_TCP_UDP_CONNE<br>TCP<br>CONNECT<br>mortesont.com:443<br>194.67.90.67<br>49780<br>443 | 9  |                                       |  |           |           |          |   | • |
|                |      |               | -00:00:06.952  | 5008 WINWORD.EXE                           | ACTION<br>FILE SIZE<br>SHA-256<br>TARGET PATH   | FILE_WRITE<br>296192<br>f5b7c4b30839021587e<br>\Users\bruser1729\AppD                        | 5bdb788c9ca3407a<br>)ata\Local\Microsoft | 05005d0da5c1dfa<br>\\Windows\INetCacl | a88a93939436bb<br>ne\IE\J8TSMW39\X6IPA | /Fwa2HOpe | VE3gLRKCM | b(1).dll |   |   |
|                |      |               | -00:00:06.937  | 5008 WINWORD.EXE                           | ACTION<br>FILE SIZE<br>SHA-256<br>TARGET PATH   | HLE_WRITE<br>296192<br>f5b7c4b30839021587e<br>\Users\bruser1729\AppD                         | 5bdb788c9ca3407a<br>Jata\Roaming\KBuG    | 05005d0da5c1dfa<br>Dorsqg.dll         | a88a93939436bb                         |           |           |          |   |   |
|                |      |               | -00:00:06.859  | 5008 WINWORD.EXE                           | ACTION<br>SOURCE PATH<br>TARGET PATH<br>DESCRIPTION   | PROC_CREATE<br>\PROGRAM FILES\MICROS<br>\Windows\System32\reg<br>Invoked                     | 50FT OFFICE\ROOT\<br>svr32.exe           | OFFICE16\WINWOF                       | RD.EXE                                 |           |           |          |   |   |
|                |      |               |  |  | C:\Windows\System32\regsvr32.exe /s C:\Users\bruser1729\AppOata\Roaming\KBuGOorsqg.dll        |  |  |                                       |  |           |           |          |   |   |
|                |      |               | -00:00:06.703  | 1596 regsvr32.exe                          | ACTION<br>SOURCE PATH<br>TARGET PATH<br>DESCRIPTION   | PROCLCREATE<br>\Windows\System32\reg<br>\Windows\SysWOW64\re<br>Invoked                      | svr32.exe<br>gsvr32.exe                  |                                       |  |           |           |          |   |   |
|                |      |               |  | -  | /s C:\Users\bruser172   | 29\AppData\Roaming\KBu   | GDorsqg.dll                              |                                       |  |           |           |          |   |   |
|                |      |               | -00:00:05.218  | 1892 regsvr32.exe                          | ACTION<br>PROTOCOL<br>DESTINATION IP<br>SOURCE PORT<br>DESTINATION PORT<br>DESCRIPTION        | NETWORK_TCP_UDP_CONNE<br>TCP<br>169.254.2.2<br>49781<br>8080<br>Destination IP: 169.254.2    | CT<br>2.2 Source Port: 497               | 81 Destination Por                    | t: 8080 Protocol: TCP                  |           |           |          |   |   |
|                |      |               | -00:00:05.204  | -  | ACTION<br>QUERY<br>DESCRIPTION  | NETWORK_DNS_ACL<br>creatorz123.top<br>DNS: creatorz123.top                                   |  |                                       |  |           |           |          |   |   |

Figure 5 – Behavioural view in HP Sure Controller.

## Threat View – Network Tab

The Network view is a table that lists all network communications that the micro-VM made during its lifetime. Figure 6 shows that approximately 26 seconds after the triggering high severity event an HTTPS session was established to 123faster[.]top (176.121.14[.]139) over TCP port 443. The network activity shows that roughly every minute a CONNECT method request occurred to that domain, indicating that this session is likely the C2 connection used by the threat actor.

| ≡          | Ø | Sure Controller |  |         | ⑦   ▼ |
|------------|---|-----------------|--|---------|-------|
|            | × | +00:00:26.551   | 52.168.20.22:443   |         |       |
| 4          |   | +00:00:26.551 - | ► 123faster.top:443 (176.121.14.139:443)   | CONNECT |       |
| 0          |   | +00:00:26.552   | 169,254.2.3:53   |         |       |
| e          |   | +00:00:37.755   | geo-prod.do.dsp.mp.microsoft.com:443 (13.78.177.144:443)   | CONNECT |       |
| $\bigcirc$ |   | +00:00:37.757   | 169.254.2.3:53   |         |       |
|            |   | +00:00:37.760   | kv801.prod.do.dsp.mp.mlcrosoft.com:443 (23.72.210.21:443)  | CONNECT |       |
|            |   | +00:00:49.028   | http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?60633e0d0b724151 (169.254.2.2:8080) | GET     |       |
|            |   | +00:00:49.030   | http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?465786103aeb5d9c (169.254.2.2:8080)       | GET     |       |
| *          |   | +00:01:30.407   | 169.254.2.2:8080   |         |       |
|            |   | +00:01:30.407   | 169.254.2.2:8080   |         |       |
|            |   | +00:01:30.594   | 169.254.2.2:8080   |         |       |
|            |   | +00:01:30.844   | 169.254.2.2:8080   |         |       |
|            |   | +00:01:30.844   | 169.254.2.2:8080   |         |       |
|            |   | +00:01:31.047   | 169.254.2.2:8080   |         |       |
|            |   | +00:01:35.598 - | ▶ 123faster.top:443 (176.121.14.139:443)   | CONNECT |       |
|            |   | +00:01:36.829   | 169.254.2.2:8080   |         |       |

Figure 6 – Network view in HP Sure Controller.

## Threat View – Metadata Tab

The Metadata view gives information about the host that triggered the alert, such as its HP Sure Click Enterprise configuration policy and the versions of software running on the host. This information may be relevant to identify whether an exploit affects only certain versions of software installed within micro-VMs.

| $\equiv$         | (bp | Sure Controller   |                        |  |                | ⊘   • |  |  |  |  |
|------------------|-----|---|------------------------|--|----------------|-------|--|--|--|--|
| 0                | ×   | 2 of 2 A Y 5   Filtered on Classification, Status, Installation, Received, Severity |                        |  |                |       |  |  |  |  |
| <b>८</b><br>⊈    |     | Microsoft Word Detection: Isolation 4<br>Threat UUID:                               | 1.7.5326 True Positive |  | ም <b>ፍ</b> 🗈 🛍 |       |  |  |  |  |
| $\bigcirc$       |     | 🕼 SUMMARY 🔟 GRAPH   | FILES EBEHAT           | VIORAL 🌐 NETWORK   | E METADATA     |       |  |  |  |  |
| <b>.</b>         |     | Metadata  |                        |  |                |       |  |  |  |  |
| - <del>-</del> - |     | KEY   |                        | VALUE  |                |       |  |  |  |  |
| 76               |     | BRF hash  |                        | 427C6E18C117A7D4BFDA9E064F23D81DEE00682B7B63AA55BE3F2D83A4FED37F |                |       |  |  |  |  |
|                  |     | BRF name  |                        | Core Rules   |                |       |  |  |  |  |
|                  |     | BRF version   |                        | 4.1.9.1294   |                |       |  |  |  |  |
|                  |     | Background VM   |                        | false  |                |       |  |  |  |  |
|                  |     | Core Rules  |                        | b65214045957e960899f9e016913a3aea22bf27d1a3be188cd81a9c4e93e98d1 |                |       |  |  |  |  |
|                  |     | DevtsVersion  |                        | 2.8  |                |       |  |  |  |  |
|                  |     | Document Hash(MD5)  |                        | 891340a4060e31a5c7a3a0fda911db79                                 |                |       |  |  |  |  |
|                  |     | Document Hash(SHA-256)  |                        | c6441cfa433596098ff1d3dc6995b90d5a63d32ae07ec9599c6a6f887b21170c |                |       |  |  |  |  |
|                  |     | Document Hash(SHA1)   |                        | 82d5ac9e8c5a65ee3a1eae3ef3ec962dbafb3c06                         |                |       |  |  |  |  |
|                  |     | Document Path   |                        |  |                |       |  |  |  |  |
|                  |     | Document Size   |                        | 2463232  |                |       |  |  |  |  |
|                  |     | Guest UUID  |                        |  |                |       |  |  |  |  |
|                  |     | Guest VMID  |                        | 8  |                |       |  |  |  |  |
|                  |     | Hostname  |                        |  |                |       |  |  |  |  |
|                  |     | MatManifestVersion  |                        | 2.0  |                |       |  |  |  |  |
|                  |     | MsOfficeVersion   |                        | 16.0.11328.20492   |                |       |  |  |  |  |



Threat View – Files Tab

The Files view is a table that lists all files that were created or modified during the lifetime of the micro-VM. If Threat Cloud is enabled, the reputation of the files based on their hash values is checked against a database of known-good and known-bad files. Figure 8 shows that several known-good files related to TeamViewer were written to the user's AppData directory in a subfolder named 'Windows Media Player'.

You can optionally blacklist a file for a device, device group or all for devices by clicking on the grey-coloured flag icon to the right of the hash value.

| =          | (hp | Sure Controller   |                             | ⊘           |
|------------|-----|---|-----------------------------|-------------|
| 0          | ×   | 2 of 2 A Y 5   Filtered on Classification, Status, Installation, Received, Severity   |                             |             |
| <b>♂</b>   |     | Microsoft Word Detection: Isolation 4.1.7.5326 True Positive Threat UUID:   | iownload 🔻 Label 💌 Assign 💌 | тр FP ᡇ 🖬   |
| $\bigcirc$ |     | 🕼 SUMMARY   | E METADATA                  |             |
| <u>■</u>   |     | Path: Windows Media Player • (*)     Hash: No filter • (*)     Threat Name: No filter • (*)     Cloud Result: No filter • (*) |                             | 6 / 275     |
| +<br>%     |     | Path  | Hash                        | Threat Name |
|            |     | \Users\bruser1729\AppData\Roaming\Windows Media Player\wpwnetwks.exe  | ☐ cc82d62                   |             |
|            |     | \Users\bruser1729\AppData\Roaming\Windows Media Player\TeamViewer.Ini   | 🛅 26d13ec 🏲                 |             |
|            |     | \Users\bruser1729\AppData\Roaming\Windows Media Player\TeamViewer_Desktop.exe   | 🛅 f2c4a28 🏲                 |             |
|            |     | \Users\bruser1729\AppData\Roaming\Windows Media Player\TeamViewer_Resource_en.dll   | 🖺 8cee930 🏲                 |             |
|            |     | \Users\bruser1729\AppData\Roaming\Windows Media Player\TeamViewer_StaticRes.dll   | 🖻 ea27f86 🏴                 |             |
|            |     | \Users\bruser1729\AppData\Roaming\Windows Media Player\msl.dll  | <table-cell></table-cell>   |             |
|            |     |   |                             |             |

Figure 8 – Files view in HP Sure Controller.

## **Closing Thoughts**

The different views in HP Sure Controller make it possible to characterise each stage of the attempted infection and obtain indicators of compromise (IOCs) such as the domains and IP addresses of the malware's C2 channel. Based on the information captured by HP Sure Click Enterprise we can identify the malware as a variant of TVRAT. As you have seen from this example, the information presented in HP Sure Controller enables security teams to efficiently investigate threats without having to re-run samples in sandboxes or resort to manual analysis, saving time and effort.

### Indicators of Compromise

| Indicator   | SHA-256 Hash   | Purpose   |
|---|--|---|
| ResumeGabriellaGrey.doc   | c6441cfa433596098ff1d3dc6995b90d5a63d32ae07ec9599c6a6f887b21170c | Downloader  |
| C:\Users\<br>[USER]\AppData\Roaming\Windows Media<br>Player\wpvnetwks.exe | cc82d628fde6549aab4f2d3d3ae3613367af945b20cc0944f937a5cacc4fecc2 | Legitimate<br>TeamViewer<br>executable            |
| C:\Users\<br>[USER]\AppData\Roaming\Windows Media<br>Player\msi.dll       | f5b7c4b30839021587e5bdb788c9ca3407a05005d0da5c1dfaa88a93939436bb | TVRAT DLL<br>side-loaded<br>into<br>wpvnetwks.exe |
| C:\Users\<br>[USER]\AppData\Roaming\KBuGDorsqg.dll                        | f5b7c4b30839021587e5bdb788c9ca3407a05005d0da5c1dfaa88a93939436bb | TVRAT DLL<br>run using<br>regsvr32.exe            |
| morteson[.]com (194.67.90[.]67:443)                                       |  | Web server<br>hosting TVRAT<br>DLL                |
| creatorz123[.]top (176.121.14[.]139:443)                                  |  | TVRAT C2<br>server                                |
| 123faster[.]top (176.121.14[.]139:443)                                    |  | TVRAT C2<br>server                                |