Recent Posts

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

HP Sure Click Enterprise 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 TVRAT (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.

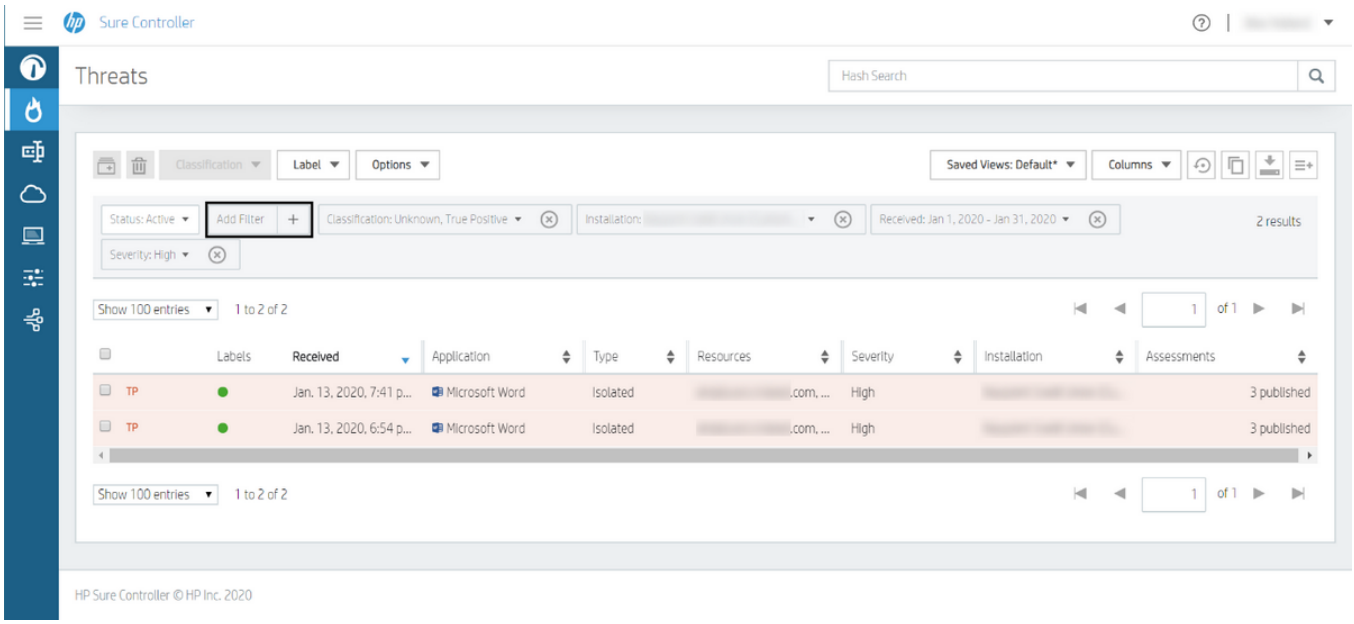

Figure 1 – The threat table view of alerts in HP Sure Controller.

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
- MITRE ATT&CK 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.

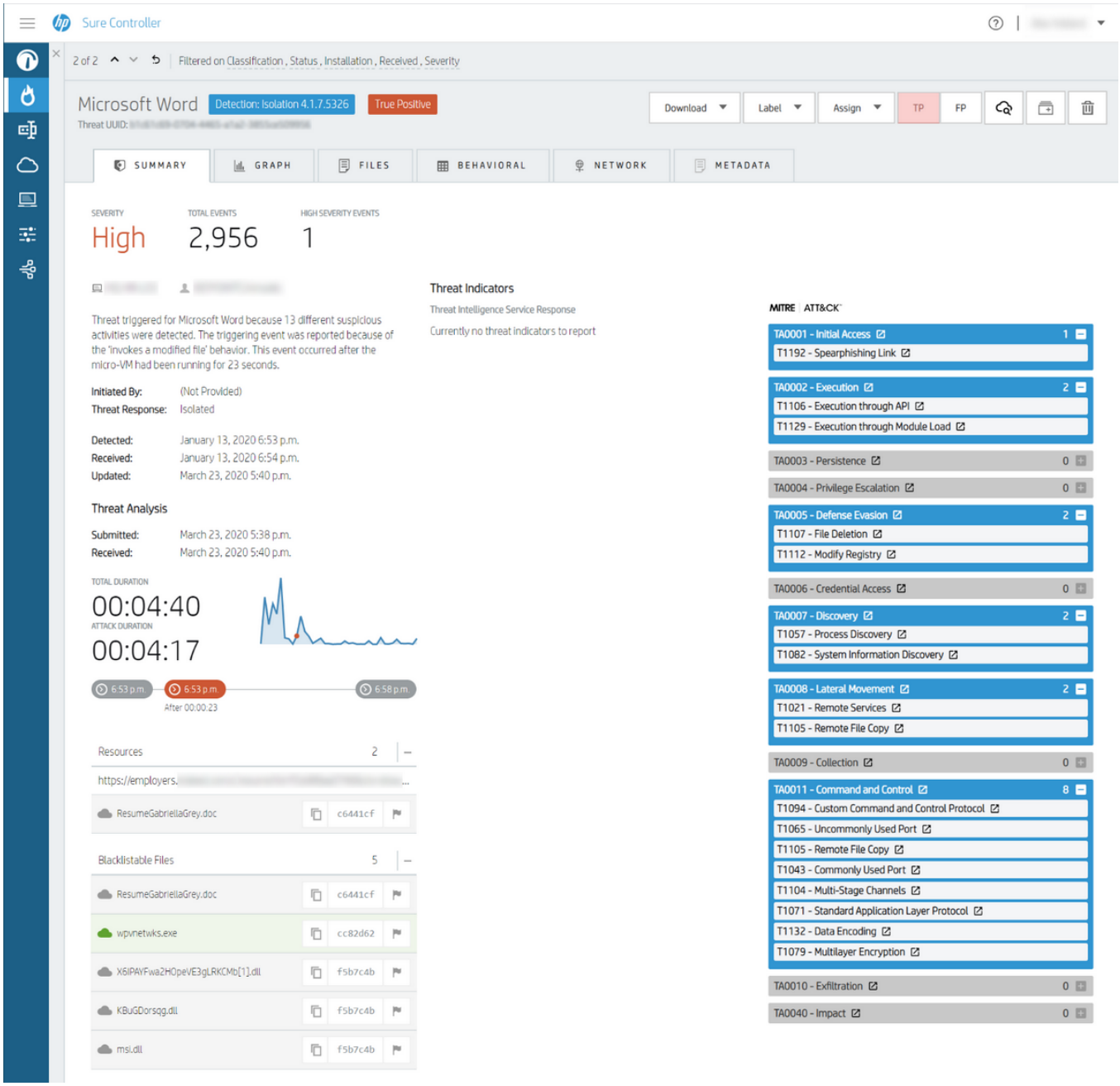

Figure 2 – The threat view of an alert in HP Sure Controller.

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 VirusTotal reveals that the file is a legitimate digitally-signed executable 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.

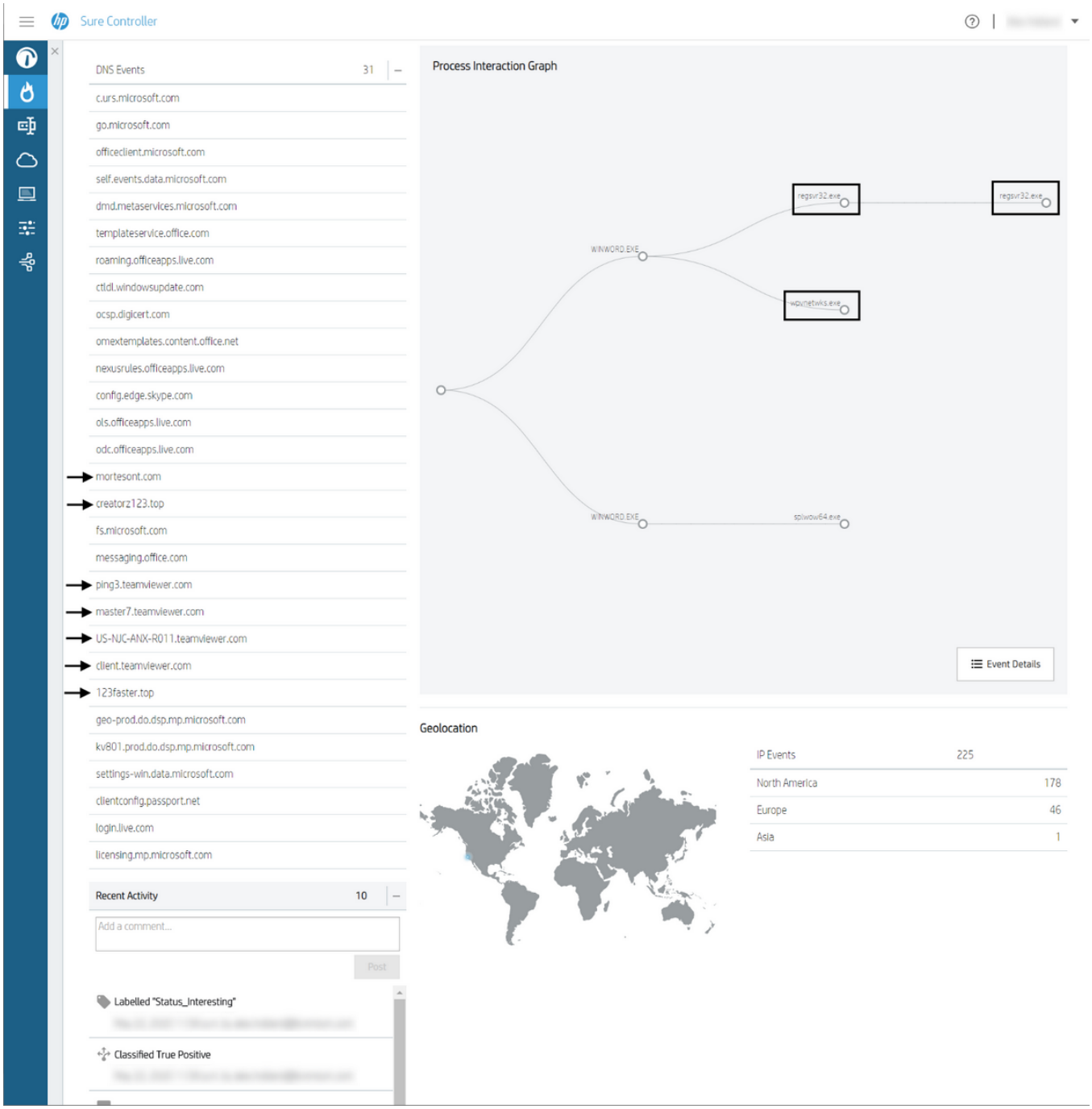

Figure 3 – Continued threat view of an alert in HP Sure Controller.

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

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

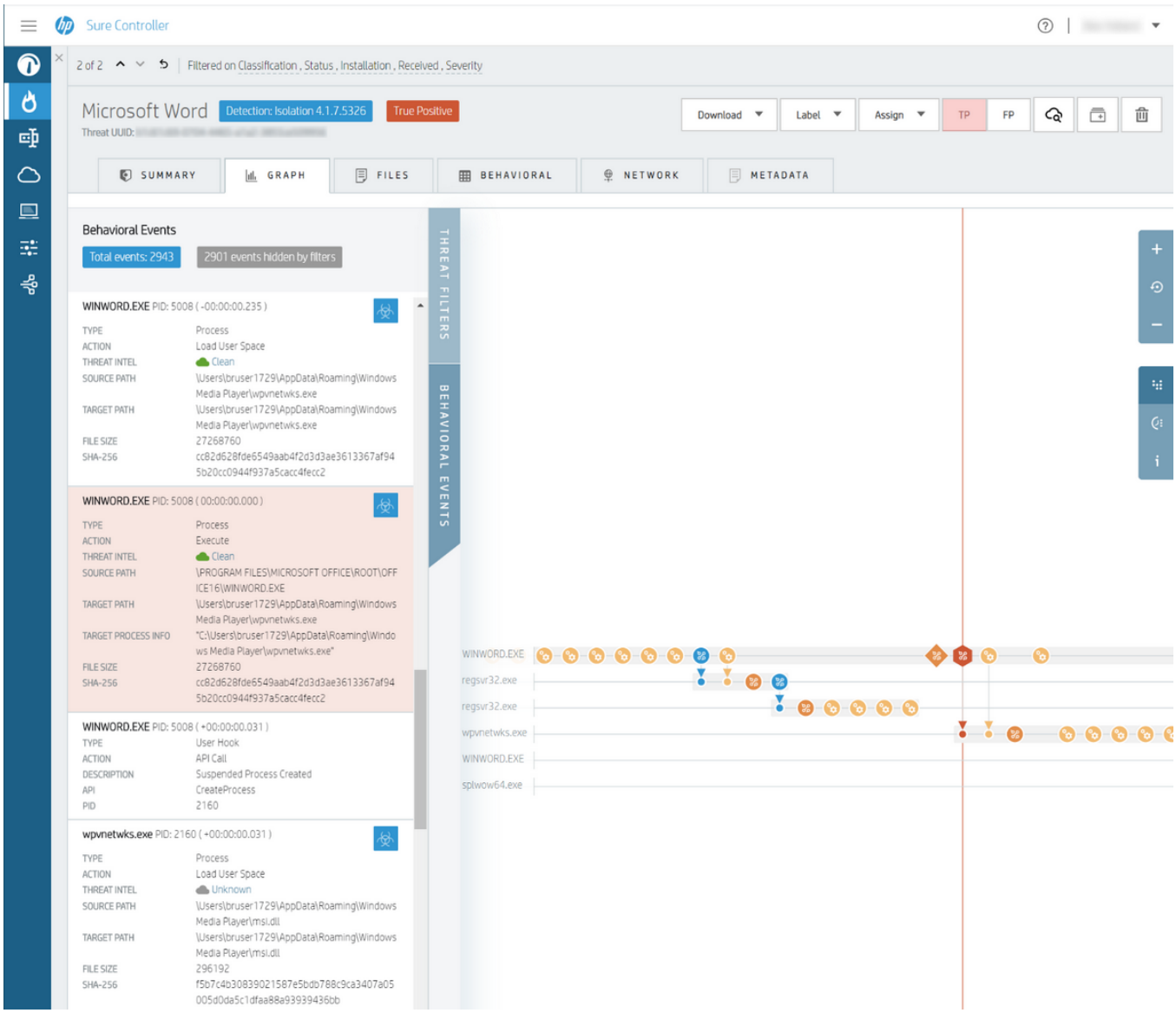

Figure 4 – Graph view of an alert in HP Sure Controller.

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 DLL side-loading (T1073). 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.

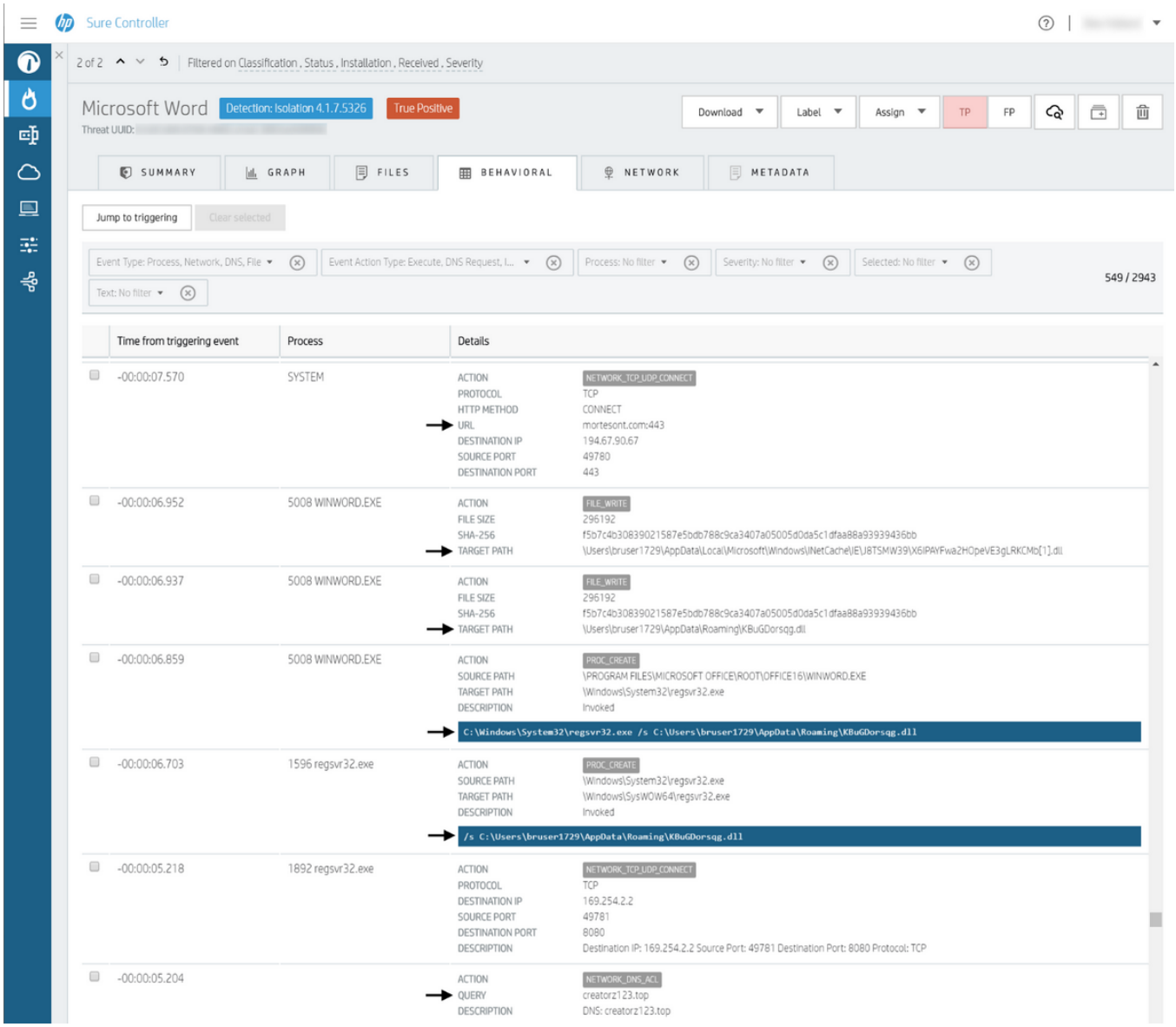

Figure 5 – Behavioural view in HP Sure Controller.

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.

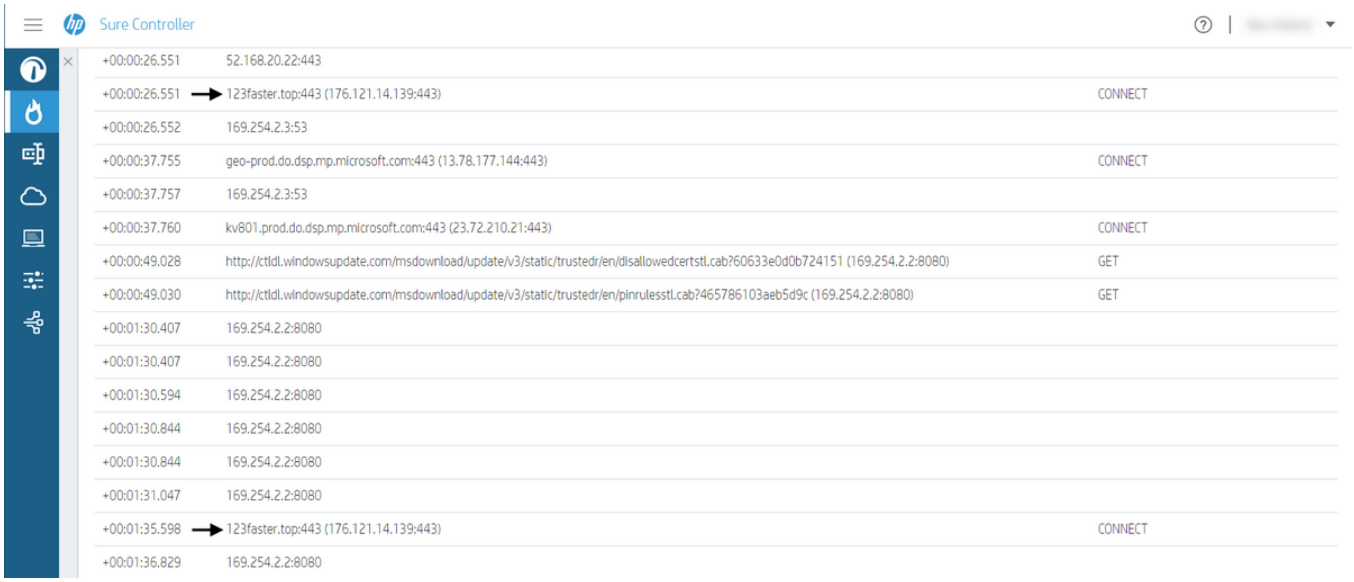

Figure 6 – Network view in HP Sure Controller.

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.

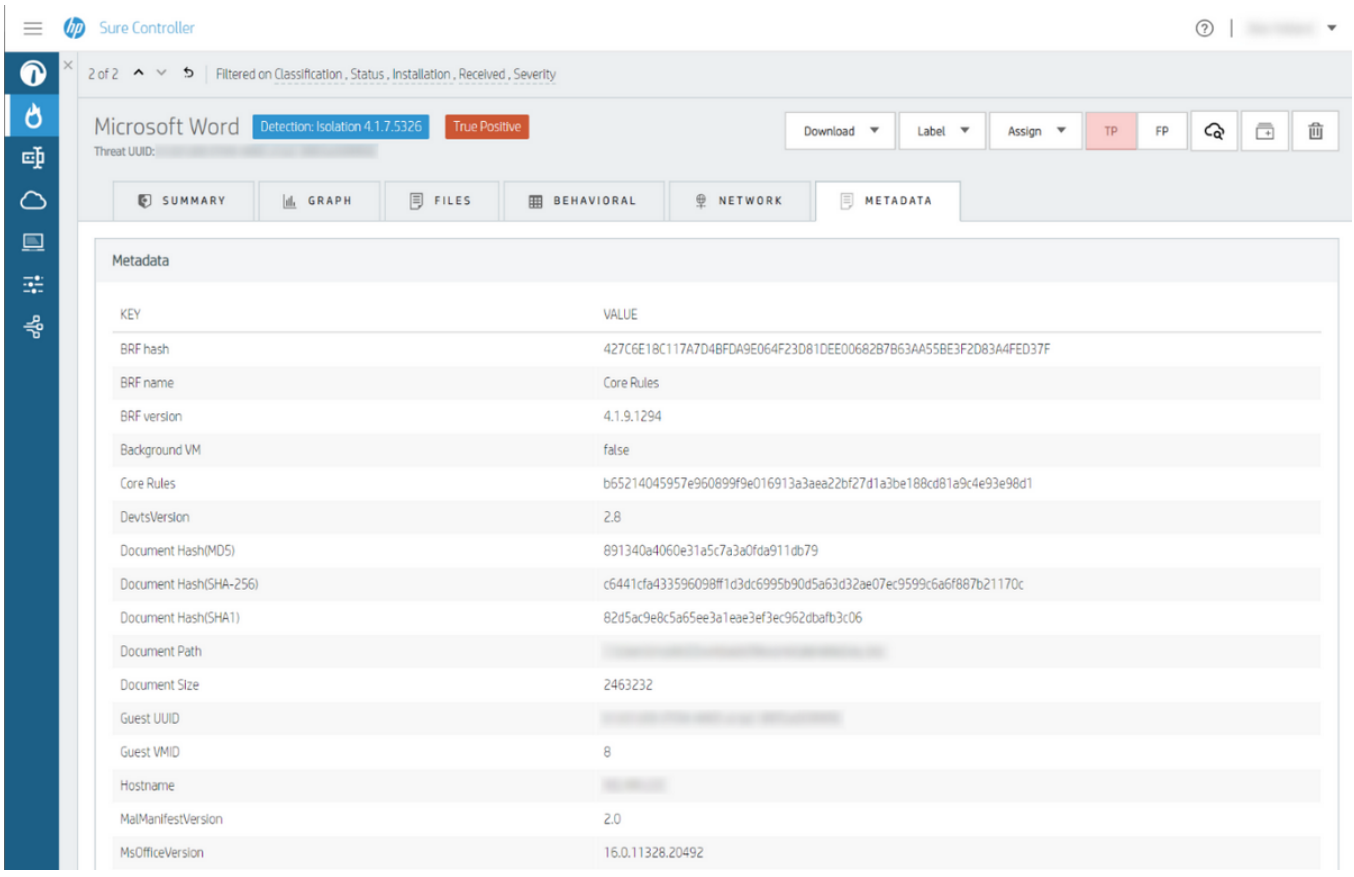

Figure 7 – Metadata view in HP Sure Controller.

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.

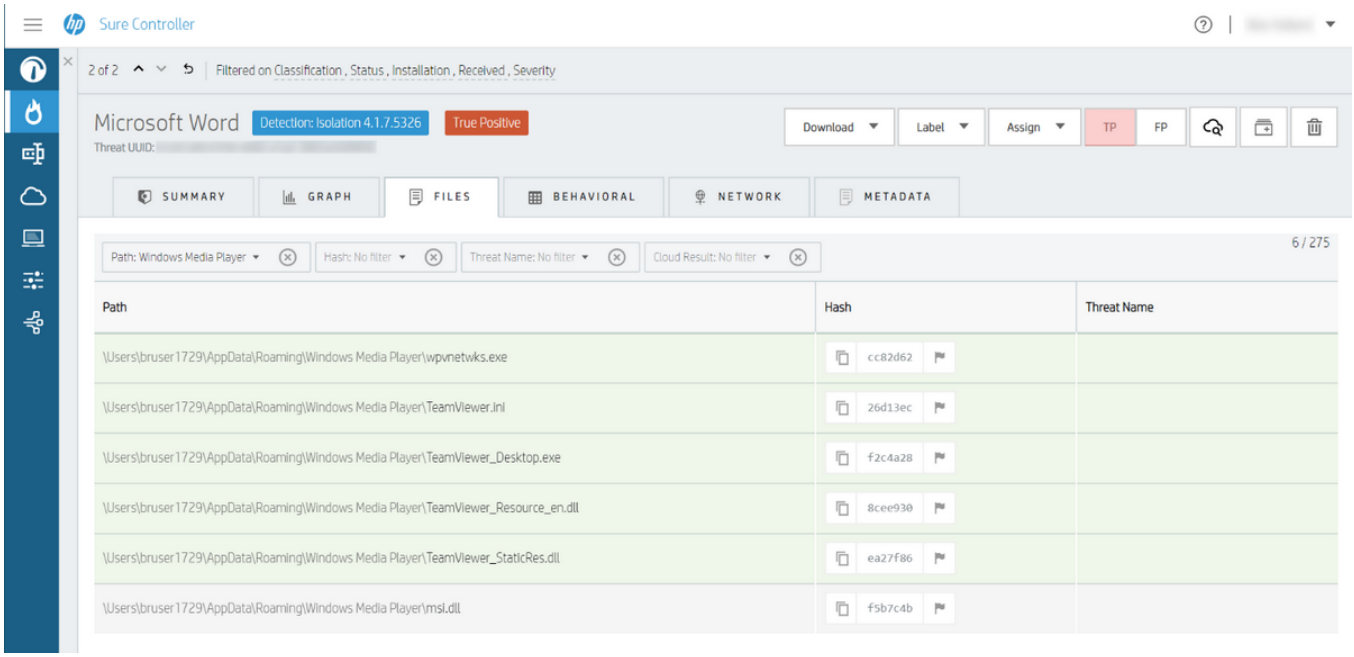

Figure 8 – Files view in HP Sure Controller.

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\[USER]\AppData\Roaming\Windows Media Player\wpvnetwks.exe	cc82d628fde6549aab4f2d3d3ae3613367af945b20cc0944f937a5cacc4fecc2	Legitimate TeamViewer executable
C:\Users\[USER]\AppData\Roaming\Windows Media Player\msi.dll	f5b7c4b30839021587e5bdb788c9ca3407a05005d0da5c1dfaa88a93939436bb	TVRAT DLL side-loaded into wpvnetwks.exe
C:\Users\[USER]\AppData\Roaming\KBuGDorsqg.dll	f5b7c4b30839021587e5bdb788c9ca3407a05005d0da5c1dfaa88a93939436bb	TVRAT DLL run using regsvr32.exe
morteson[.]com (194.67.90[.]67:443)		Web server hosting TVRAT DLL
creatorz123[.]top (176.121.14[.]139:443)		TVRAT C2 server
123faster[.]top (176.121.14[.]139:443)		TVRAT C2 server

Tags