Threat Graphs examples: Malware detections

KB-000036359 Feb 27, 2023 0 people found this article helpful

English

Overview

This article provides examples of Sophos Threat Graphs (previously called Threat Cases) that have been automatically created due to a malware detection. The purpose of a threat graph is to help admins understand what happened on the affected computer before the detection occurred. Using this information can help you understand ongoing infections, as well as how to further improve your security against similar attacks in the future.

Please note this article only applies to customers licensed to use Sophos Central Intercept X (CIX) or Sophos Endpoint Detection and Response (XDR).

This article is part of a series of example Threat Graphs. The start of each article includes a detailed description of all the different sections in a Threat Graphs, if you are already familiar with this information, we suggest you skip to the Example Threat Graphs walkthroughs at the bottom. For more information, see the Related information section.

The following sections are covered:

- What is a Threat Graph?
  - Simplified events chain
  - Summary
  - Suggested next steps
  - Analyze
  - Artifacts
  - Create forensic snapshot
  - Export to CSV
  - Threat Intelligence
    - Intercept X without XDR
    - Intercept X with XDR
  - Clean and block
  - Case record
- Example Threat Graphs walkthroughs
  - Deep learning detection: ML/PE-A
    - Security improvement options
- Related information

Product and Environment

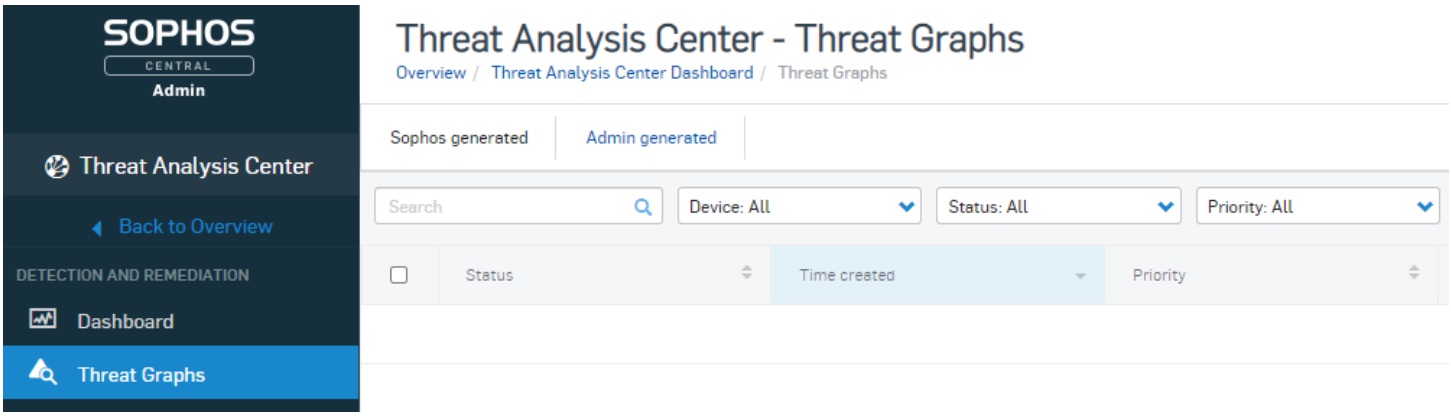
- Sophos Intercept X
- Sophos Endpoint Detection and Response
- Sophos Central Admin

What is a Threat Graph?

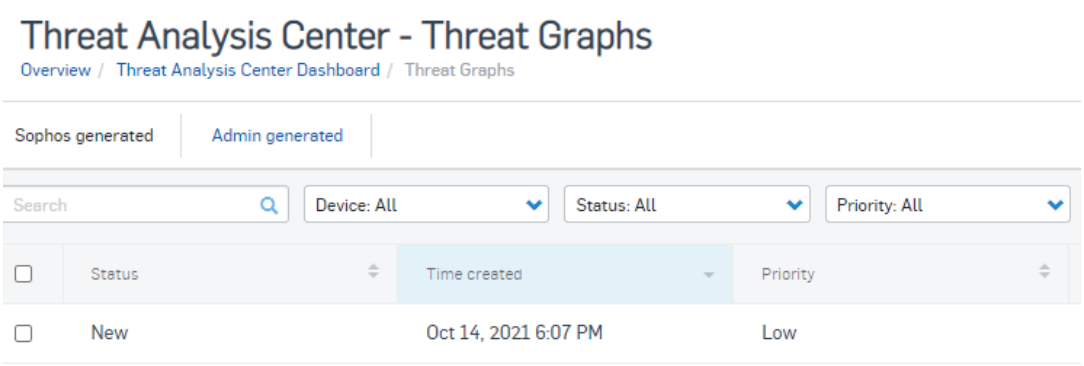
Threat Graphs are automatically created after a malicious detection occurs. The purpose of these is to help an admin understand what happened before the detection occurred. For example, a detection on a Microsoft Word file could have generated a Threat Graph that shows this file was written to the computer by `Outlook.exe`, indicating that the user received and opened a malicious attachment on an email. With this information, you may be able to identify gaps in your security that could be improved.

Note:
Threat Graphs are only created for malicious detections; this does not include detections for PUAs, Application Control, Device Control, Web Control. Additionally, if Sophos Central cannot automatically confirm a root cause, a Threat Graph may not be generated.

Threat Graphs can be found by signing in to the Sophos Central Admin console and clicking the **Threat Analysis Center**:



The most recent Threat Graphs are displayed at the top of the **Dashboard** page:



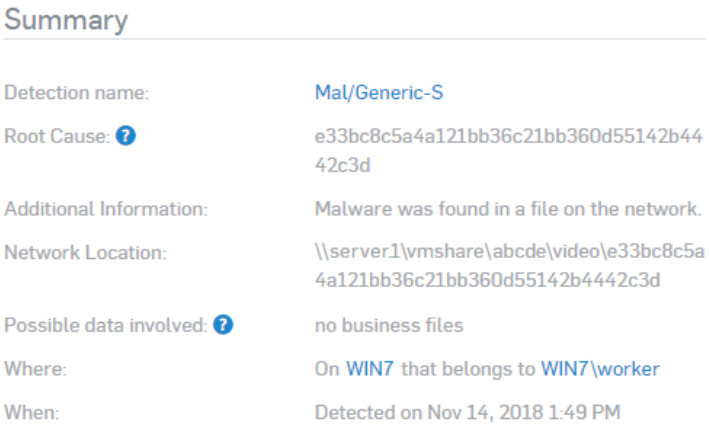
To view a Threat Graph click on the detection **Name**.

Simplified events chain

At the top of every Sophos Central-generated threat graph (excludes Admin generated), you will see the simplified events chain. This gives you the very basic details of what happened.

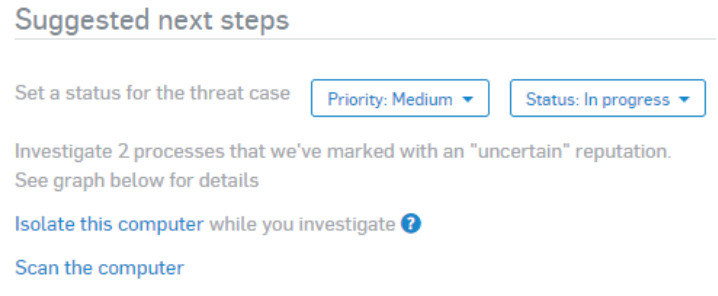
Summary

Every Threat Graph will have a Summary section that displays the basic information. This includes the detection name, root cause, possible data involved, the user and device name, and when the detection happened. Depending on the detection, there may be additional information shown.



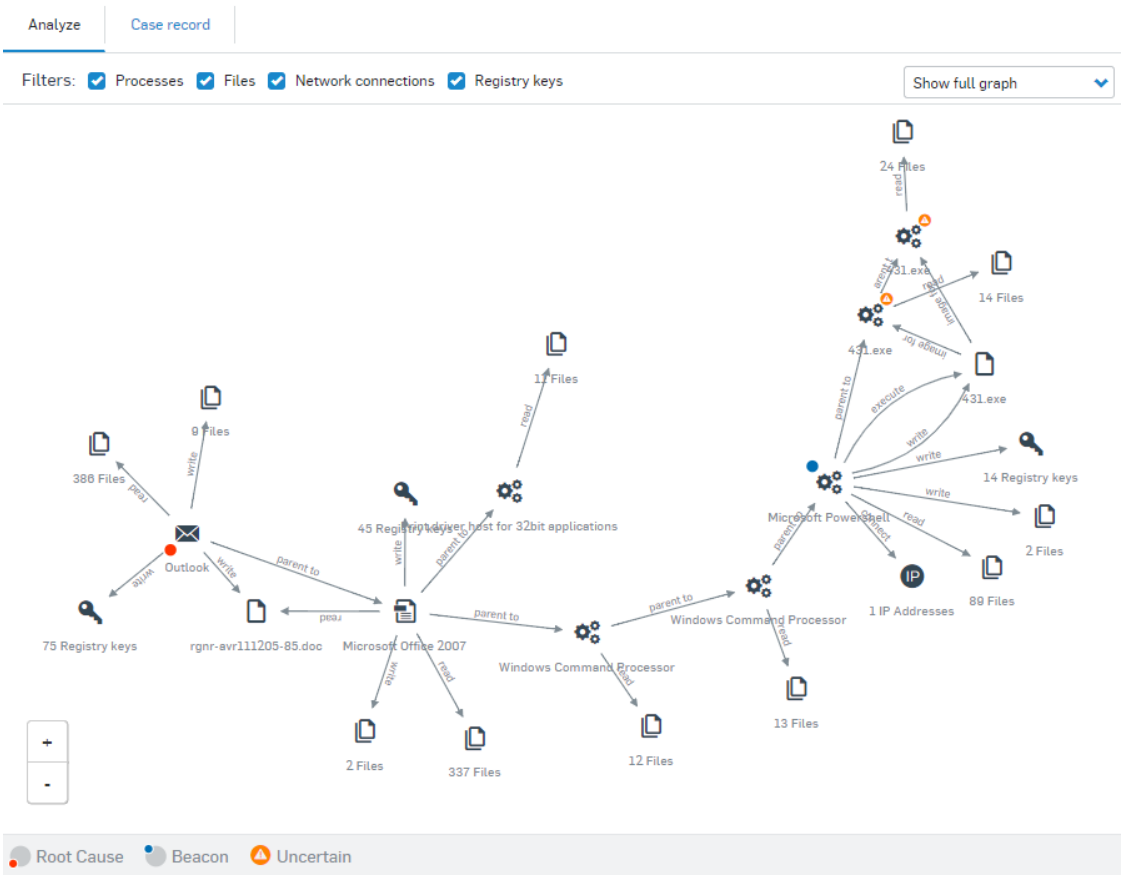
Suggested next steps

This section provides automated advice on the possible next actions you can take. The advice displayed is dependent on the type of detection and the information that was collected. It includes the ability to set the priority and status of the record for this Threat Graph, this is covered in more detail later. For Sophos XDR customers, you will have the additional option to isolate this computer. For more information on computer isolation please see Sophos Central - Computer Isolation Overview (KB-000038424)



Analyze

The Analyze tab contains the majority of the Threat Graph information. Here you will be presented with a graph of what Sophos has detected, which is referred to as the **Beacon**, and what we have determined was the **Root Cause**. The Beacon and Root Cause will be linked by a chain of events that is known as the attack chain. Below is an example attack chain:

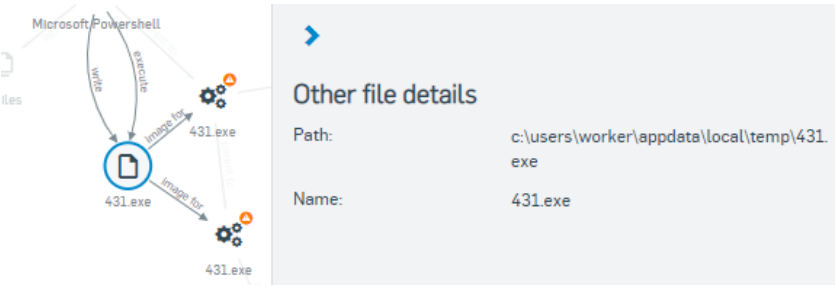


Attack chains include several different icons to help you quickly identify what happened and the most suspicious events to investigate.

Icon	Description
	Root cause
	Beacon
	Uncertain reputation
	Bad reputation

	Allowed application
	Network drive
	Peripheral
	A process
	A file(s)
	A registry key
	An IP address
	A URL
	A Domain
	An email client
	A document editor
	A browser

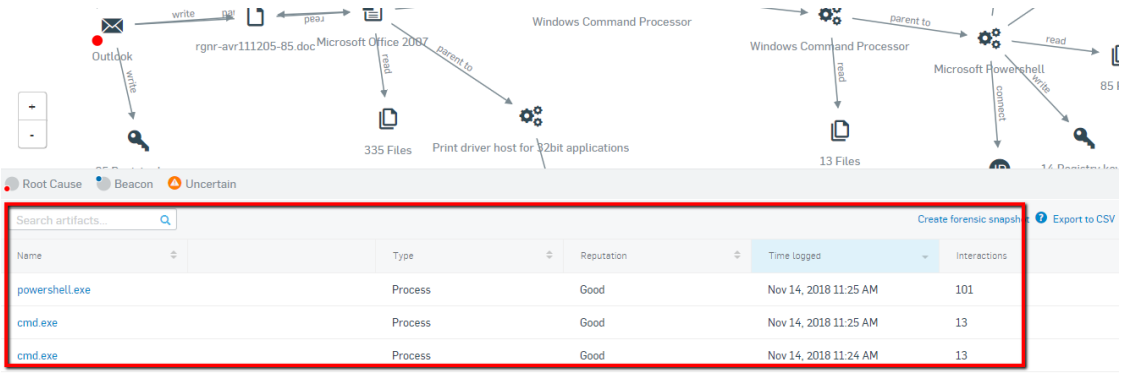
By clicking on an event in the attack chain, a menu on the right-hand side will be displayed, this will include additional information and options for that event. For example, in the picture below, we have selected a file called `431.exe`. In the right-hand menu, we can see the path of this file.

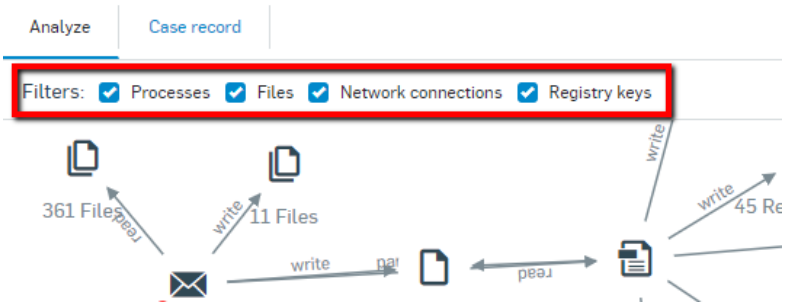


The information and options provided are covered in more detail later, in the **Threat Intelligence** section.

Artifacts

All of the information provided in the attack chain graph is also listed in a table. This can be found below the graph on the Analyze tab. The items in the table are referred to as Artifacts. By selecting artifacts their additional information is displayed in the right-hand menu. You can also search the artifacts list and use the filter options to help your investigation.





Create forensic snapshot

The ability to create Forensic Snapshots means that customers with Sophos XDR can request endpoints to generate a snapshot on demand so that you can perform a detailed analysis on an endpoints activity. To analyze the snapshot, you will need to convert it into a usable format using a tool that we provide. For more information, see Sophos Intercept X Advanced with XDR: Help with Forensic Snapshots (KB-000038358)

Export to CSV

The export to CSV option is available in the top right of the artifacts list. It will export all the event information including file names, paths, registry keys, PIDs, SHA-256 and other information. Below is an example of exported CSV data in Microsoft Excel.

	B	C	D	E	F	G	H	
1	Name	Type	Start Date Time	End Date Time	Pid	Path	Is Business File	SHA256 Hash
2	outlook.exe	process	2018-11-14T11:24:41Z		3840	c:\program files (x86)\microsoft office\office12\outlook.exe		0ca1c4ac482b92652
3	winword.exe	process	2018-11-14T11:24:56Z		1720	c:\program files (x86)\microsoft office\office12\winword.exe		6c959cfb001fbb900
4	splwow64.exe	process	2018-11-14T11:24:58Z		3544	c:\windows\splwow64.exe		232f4854a70cfa982
5	cmd.exe	process	2018-11-14T11:24:59Z		3488	c:\windows\syswow64\cmd.exe		17f746d82695fa9b3
6	cmd.exe	process	2018-11-14T11:25:00Z		1588	c:\windows\syswow64\cmd.exe		17f746d82695fa9b3
7	powershell.exe	process	2018-11-14T11:25:01Z		1484	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe		6c05e11399b7e3c8
8	rgnr-avr111205-85.doc	path				c:\users\worker\appdata\local\microsoft\windows\temporary int	TRUE	
9	431.exe	path				c:\users\worker\appdata\local\temp\431.exe	FALSE	

Threat Intelligence

By selecting events in the analyze graph the right-hand menu will be displayed providing additional information. If you select the root cause, beacon, or any of the processes, you will be presented with SophosLabs Threat Intelligence information.

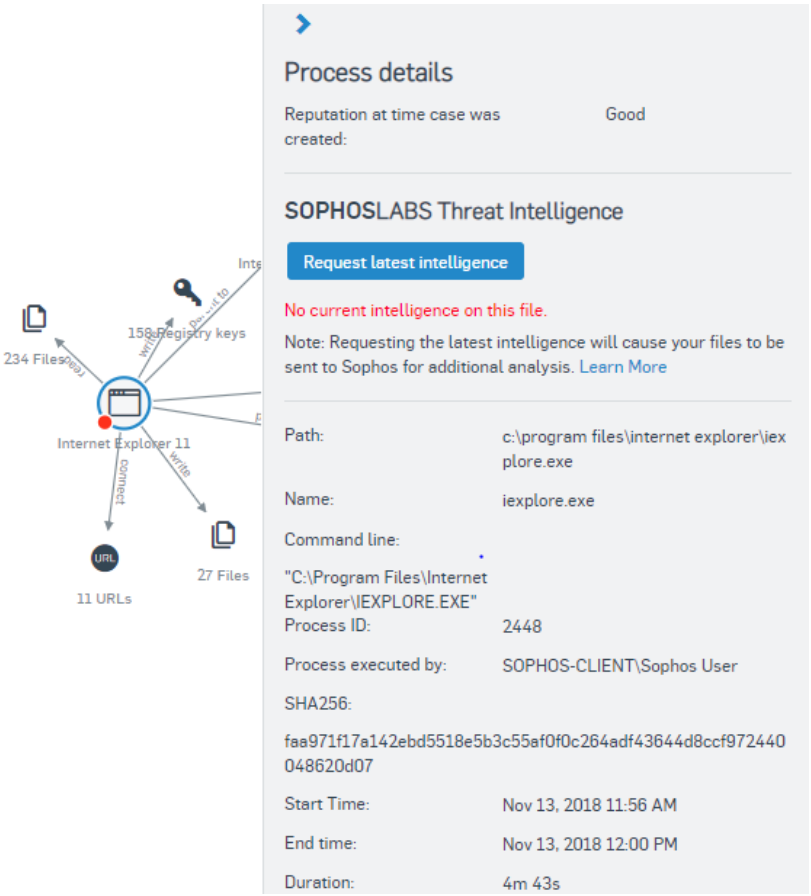
Note:
The information provided to customers using Intercept X is limited compared to customers who additionally have XDR. For this reason, the sections below have been split into two categories:

- Intercept X without XDR
- Intercept X with XDR

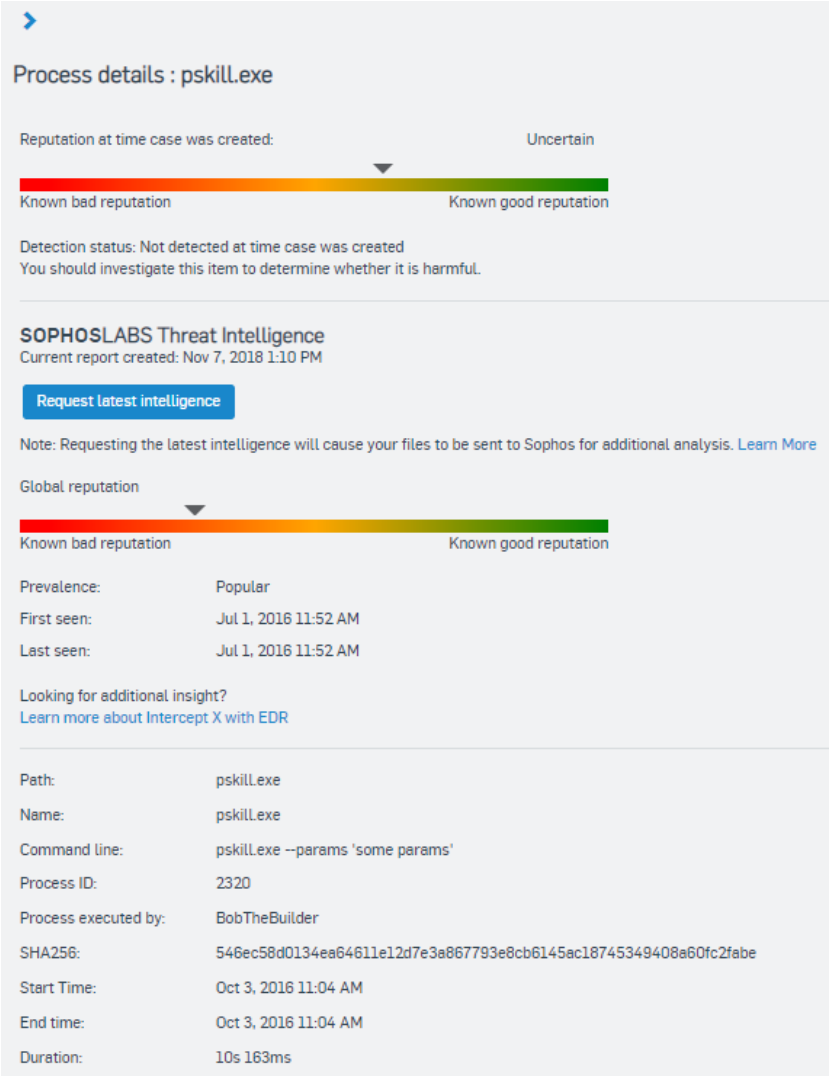
For more information, please see Intercept X Advanced with XDR (https://www.sophos.com/medialibrary/PDFs/factsheets/intercept-x-edr.pdf)

Intercept X without XDR

For any processes that ran and are displayed in the attack chain, you will have additional options available to you in the right-hand menu when you select the process in the graph. These options are also available for the beacon event. For example, below we have selected the root cause event, which has already been identified as the browser Internet Explorer. On the right-hand menu we can see the reputation of the file at the point the threat graph was generated, as well as information such as the filename, path, SHA-256 hash, when the file was run, and for how long.



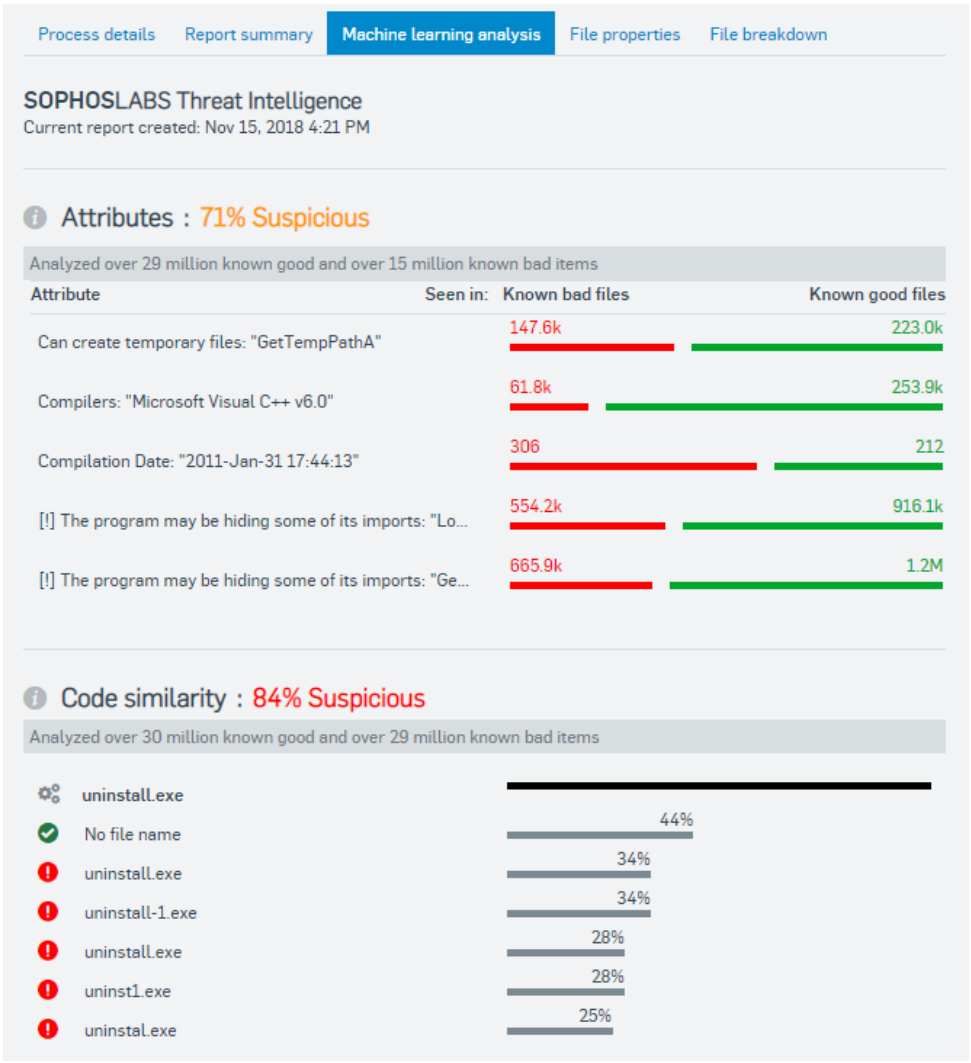
By selecting the Request Latest Intelligence button, the file will be submitted to SophosLabs. This will result in a report being generated a couple of minutes later and additional information being displayed. Below is an example of a SophosLabs Threat Intelligence report for a Sophos Intercept X customer (without XDR).

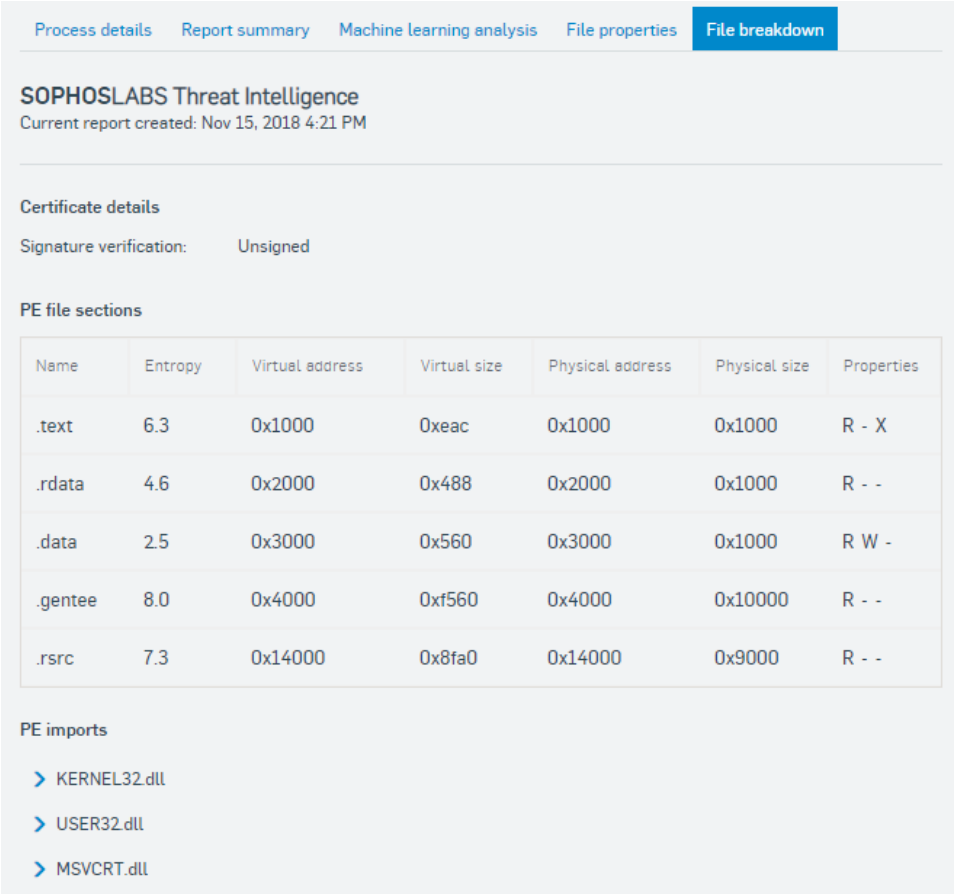


Intercept X with XDR

Customers licensed for Sophos XDR benefit from several additional features. One of these is the detailed SophosLabs Threat Intelligence reports. These reports provide you with a more in-depth analysis of the file, which can help you decide if the file is malicious or clean. Full details of what is available in these reports can be found here Sophos Central: Threat intelligence overview (KB-000038426)

Below are some examples.


Process details
Report summary
Machine learning analysis
File properties
File breakdown
SOPHOSLABS Threat Intelligence
Current report created: Nov 15, 2018 4:21 PM
Attributes : 71% Suspicious
Analyzed over 29 million known good and over 15 million known bad items
Attribute
Seen in:
Known bad files
Known good files
Can create temporary files: "GetTempPathA"
147.6k
223.0k
Compilers: "Microsoft Visual C++ v6.0"
61.8k
253.9k
Compilation Date: "2011-Jan-31 17:44:13"
306
212
[!] The program may be hiding some of its imports: "Lo...
554.2k
916.1k
[!] The program may be hiding some of its imports: "Ge...
665.9k
1.2M
Code similarity : 84% Suspicious
Analyzed over 30 million known good and over 29 million known bad items
uninstall.exe
No file name
44%
uninstall.exe
34%
uninstall-1.exe
34%
uninstall.exe
28%
uninst1.exe
28%
uninstal.exe
25%



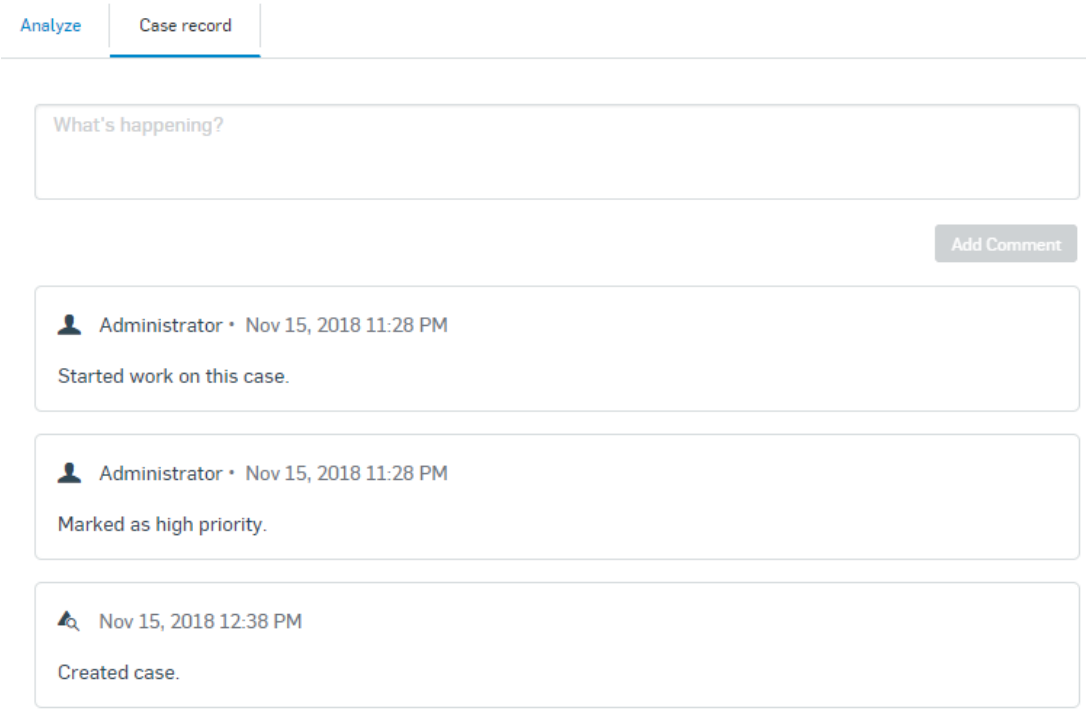
Clean and block

Sophos customers licensed for XDR are able to use the clean and block feature. This allows you to immediately detect and remove potentially malicious files from every Sophos-protected computer in your environment. This feature is currently limited to PE files that have an uncertain or bad reputation.

Any PE file that has an uncertain or bad reputation that is marked for **Clean and block**, will be added to the **Blocked items** list in **Global Settings**.

Case record

A case record is created for every threat graph. It can be used by admins to add comments about the investigation. This can be useful if you have multiple admins looking at a threat graph and wanting to record notes.



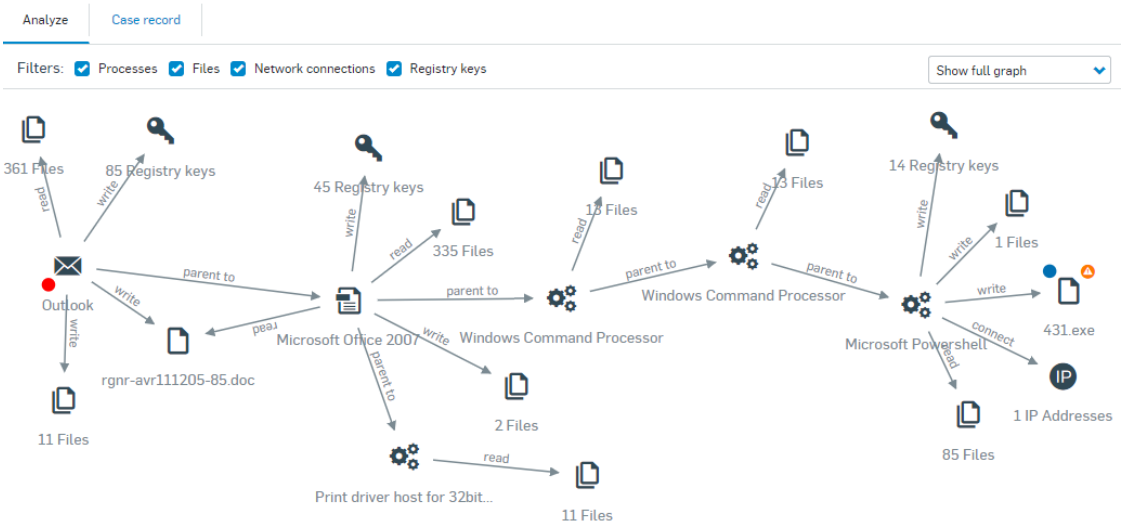
Example Threat Graphs walkthroughs

In the next section, we will take real Threat Graphs that show different types of malware detections. Using the information provided, we will investigate what additional actions could be taken to further improve your security. Please note that many real-world threat graphs will not necessarily provide options to improve your security. They can also just act as a record of what happened.

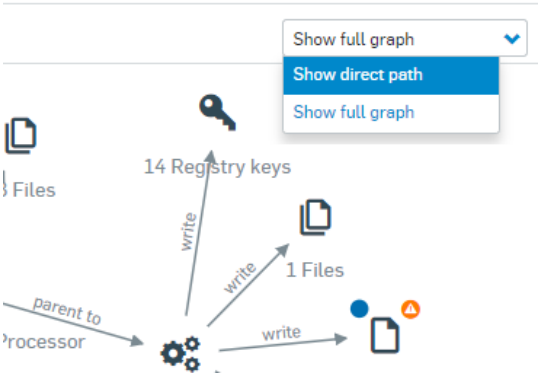
Deep learning detection: ML/PE-A

After clicking on the new threat graphs for an ML/PE-A detection we are presented with the simplified events chain. In this example, it shows the computer **WIN7** had the route cause of the email client `Outlook.exe` and a beacon event on a file called `431.exe`, this file was detected on November 14th and cleaned.

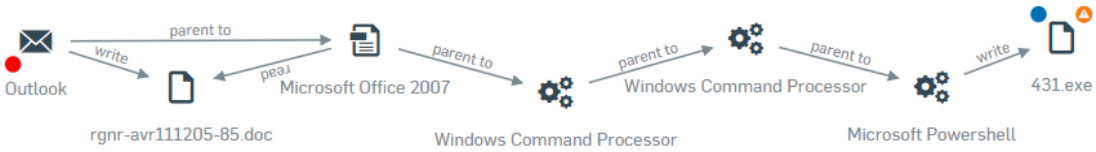
Looking at the analyze attack chain graph below we can see several events linking the root cause - Outlook on the left-hand side, to the beacon event - `431.exe` on the right. We can also see that the beacon file also has an uncertain reputation.



Before we dig any deeper into this, let us get a better overview of what happened, we can select the **Show direct path** option from the drop down menu on the right-hand side.



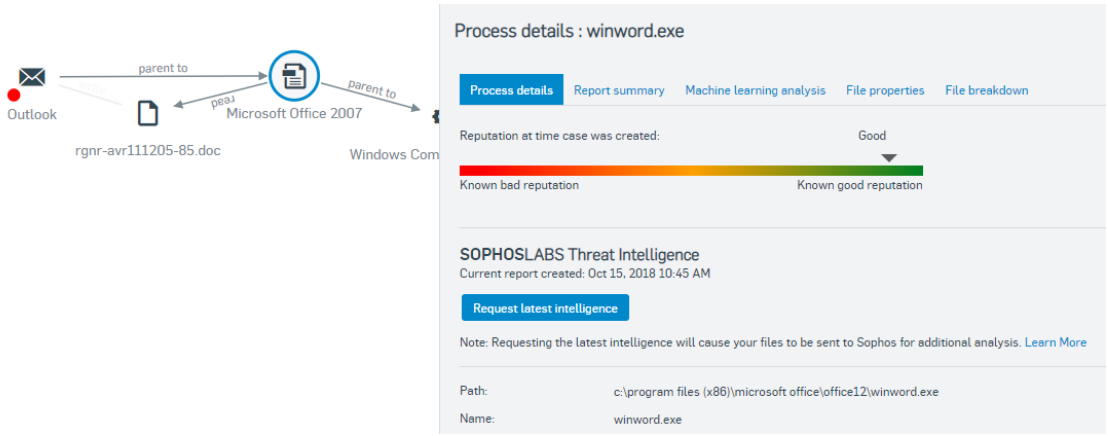
This hides most of the events leaving only the ones that directly link the root cause to the beacon. It is now easy to see that Outlook wrote a word document called `rgnr-avr111205-85.doc`. We can also see that Outlook launched a Microsoft Office application, which read the doc file.



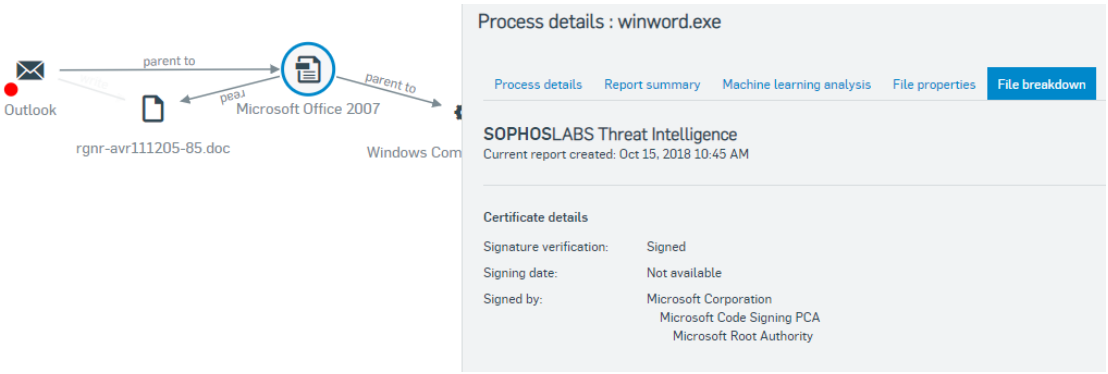
We can already see that the Microsoft Office event does not have a reputation icon, which means it has a good reputation.

Note: Reputation is only calculated for Portable Executable (PE) files, for example `.exe, .dll`. It is not shown for other file types such as `.doc, .pdf, .png`.

By selecting the Microsoft Office event, we can see that SophosLabs Threat Intelligence information is already available and confirms that it does have a good reputation. We can also see the path and name of the file indicate this is the Microsoft Word application.

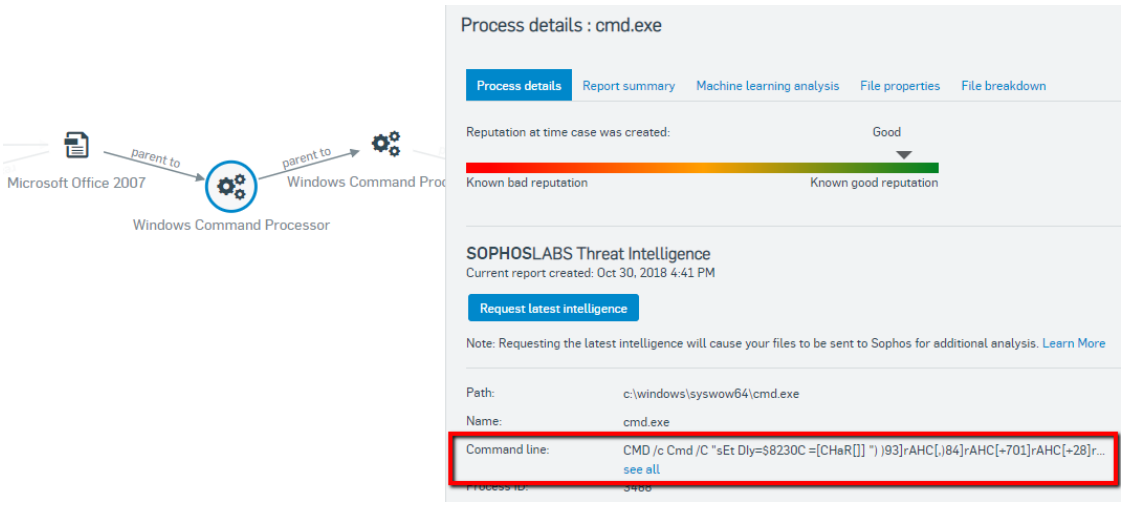


For customers using Sophos XDR, we can also see that on the File breakdown tab the file is signed by Microsoft. We could look at the other tabs to further verify the legitimacy of this file. However, it is clear this is the real Microsoft Word application.

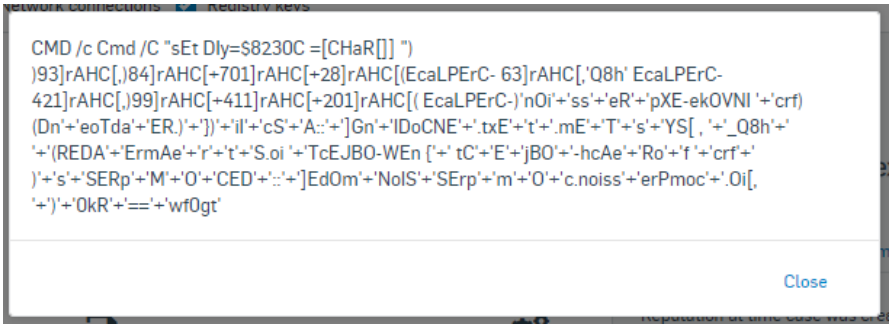


This tells us the user most likely received an email with the word document attached and that they opened the attachment. Let us look at the next event.

We can see that **Microsoft Office** launches **Windows Command Processes** (CMD), again by selecting this event we can see it has a good reputation and we are happy this is the legitimate version of `CMD.exe`. What is suspicious though is the command line information it was launched with.

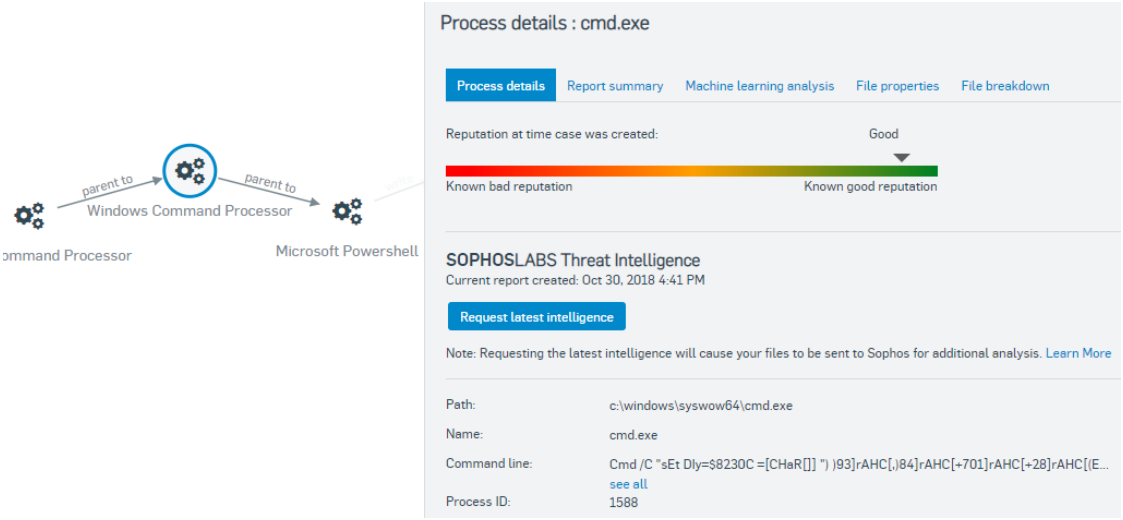


By selecting the **see all** link we can see the full command.

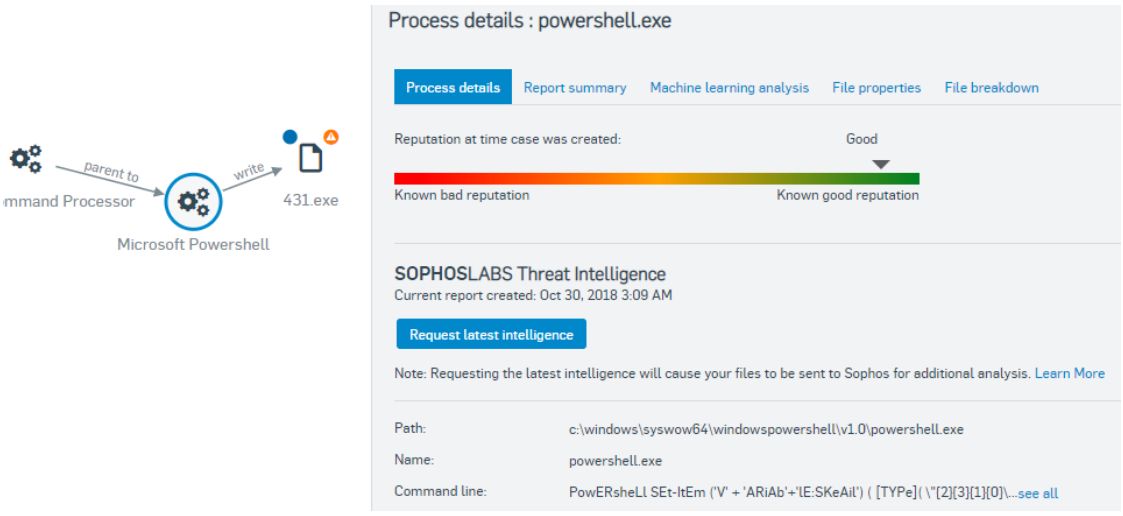


Looking at this code, you will most likely not have any idea what it is designed to do. However, that is exactly the idea. This is a heavily obfuscated bit of code. Obfuscation is very typical in malicious code and is designed to hide the true goal behind the code as well as make it harder for security software to analyze. We may not know what it is doing but we are certain it is very suspicious.

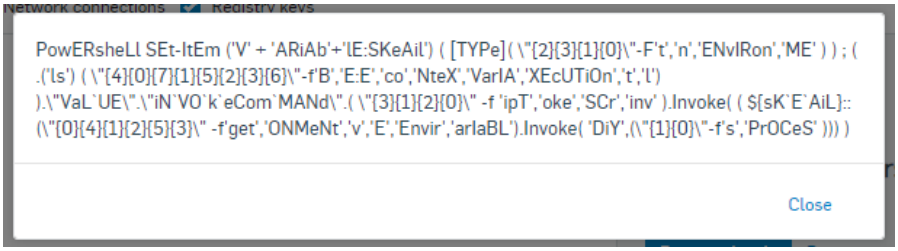
We can also see that when CMD was launched it then launched another copy of CMD, this one with a similar suspicious command line.



This second CMD is used to launch **Microsoft Powershell**.

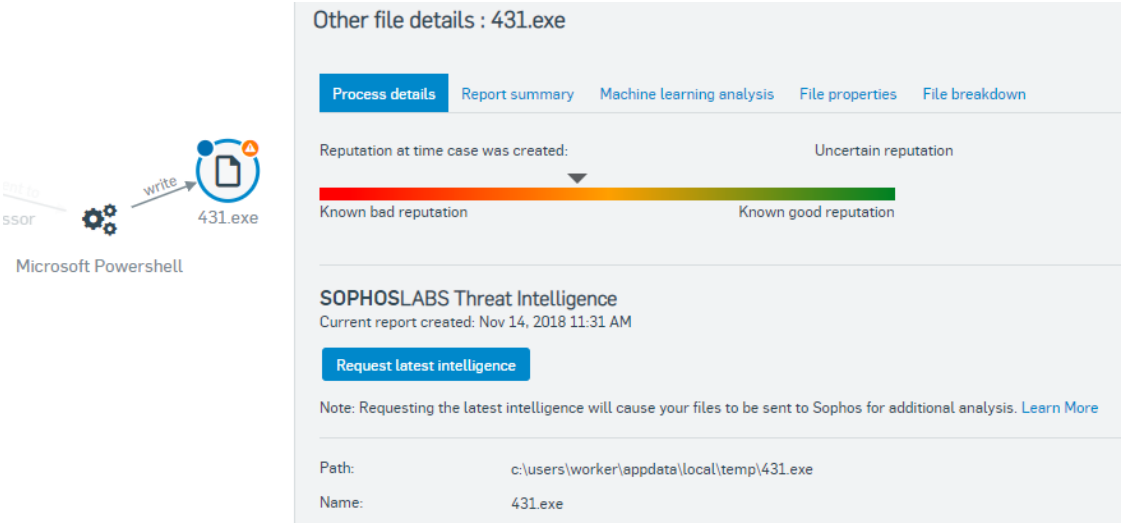


We can also see that PowerShell has been launched with an obfuscated and very suspicious command line.



PowerShell has then written the `431.exe` file which was detected by Sophos Deep Learning as ML/PE-A.

By selecting the beacon event we can see confirmation that it has an uncertain reputation, as well as that it was written to the user's AppData location, this location is typically meant for data not executables so this is also suspicious.



Important: Customers who are **not** using Sophos XDR, you will only see the one **Process details** tab.

For customers using Sophos EDR, by pressing the **Request latest intelligence** button, the file will be retrieved out of the Sophos quarantine and submitted to SophosLabs. A couple of minutes later the four other tabs (Report summary, Machine learning analysis, File properties, File breakdown) pictured will be displayed. The purpose of these additional tabs is to help display the various properties of the file in a simple way. This can be useful for various reasons, one of them is to feel confident that the file is indeed malicious and not something you want in your environment. For more information on SophosLabs Threat Intelligence, see: Sophos Central: Threat intelligence overview (KB-000038426).

Now that we understand that the file was malicious and that it came from an email, which then used Microsoft Word, CMD and Powershell to execute the attack chain, we can decide what could be done to help prevent this type of attack happening again.

Security improvement options

Firstly a spam email with a malicious attachment got into your network, which means it got past any email spam scanning software you have, as well as avoiding detection for the malicious word document. Regularly reviewing your email security policies to ensure you are following best practices and using the latest protection is recommended. If you are not already a customer we recommend the Sophos XG firewall (https://www.sophos.com/products/next-gen-firewall.aspx) to handle your email protection, combined with Sophos Sandstorm to add the protection of a sandbox environment to safely execute potential email threats before they enter your environment.

You also have a user that opened the suspicious word document on the spam email. With better user education this potentially could have been avoided. Sophos Phish Threat (https://www.sophos.com/products/phish-threat.aspx) allows you to create realistic email phishing campaigns to send to your users. Tracking which users fall for the spam email and directing them to training material.

The next layer of protection you could look at is using Sophos Application Control (KB-000035468), which is already included in all Sophos Central Endpoint and Server Advanced licenses, as well as Sophos Intercept X Advanced with EDR. With Application Control you could choose to block your users for running specific applications. While you are unlikely going to stop them from running Microsoft Word, do they really need to be able to run Powershell? This could be blocked with Application Control.

If you were concerned that the computer was still infected, or just wanted to be safe until you had spoken to the user. You could use the Isolate this computer option in the Suggested next steps section. This would disable all TCP and UDP traffic on the computer other than communication to Sophos. For more information on computer isolation please see: Sophos Central - Computer Isolation Overview (KB-000038424)

If you would like to look at other Threat Graphs examples, please see the links in the Related information section below. You can also use the Community Forum (https://community.sophos.com/products/malware/) to post questions about any threat graphs you have and would like advice on.

Trend Micro, Inc. Ex. 1016
Trend Micro, Inc., v. Webroot Inc.
IPR2024-00106

Related information
Sophos Central Admin: Overview of Threat Graphs (KB-000036336)

Sign up for the Sophos Support Notification Service (https://centralstatus.sophos.com/smscodeverification) to receive proactive SMS alerts for Sophos products and Sophos Central services.

Was this useful?

Yes No

Want to leave us some feedback?
Please visit the Product Documentation Feedback (https://community.sophos.com/product-documentation/i/feedback)

RELATED ARTICLES

Sophos Central Admin: Overview of Threat Graphs (/support/s/article/KB-000036336)	660
Sophos Endpoint Security and Control: Resolve malware detection on pagefile.sys or hiberfil.sys (/support/s/article/KB-000037996)	1.27K
Sophos Central: Expected Threat Graph behavior for Cryptoguard or Malicious behavior detection alerts (/support/s/article/KB-000044022)	201
Sophos Central Admin: Cleanup of Malware or PUA (/support/s/article/KB-000039039)	629
Sophos Anti-Virus: Remove malware threats, adware, or potentially unwanted application (PUA) (/support/s/article/KB-000033966)	1.52K

Quick Links

- Support Downloads
- Sample Submissions
- Sophos Community
- Sophos Labs
- Sophos Trust Center
- Support Portal User Guide
- Twitter Support

© 1997-2022 Sophos Ltd. All Rights Reserved.

(https://www.sophos.com/en-us/legal) (https://www.sophos.com/en-us/legal/sophos-group-privacy-notice) (https://www.sophos.com/en-us/legal/cookie-information)