

Parsing Sysmon Events for IR Indicators

February 23, 2015 | mchurchill | Threat Hunting & Intel • From The Front Lines



Intro and Installation

A dedicated endpoint monitoring tool is quickly becoming a necessity among organizations to increase visibility, logging, and alerting to combat targeted attacks and commodity malware. Sysmon is a free endpoint monitoring tool by Microsoft Sysinternals and was recently updated to version 2.0. Sysmon is a great tool for home use, as another way to track malware in a sandbox<1>, and for anyone interested in discovering the value of endpoint monitoring. Sysmon monitors a computer system for several action: process creation with command line and hash, process termination, network connections, changes in file creation timestamps, and driver/image loading. Sysmon logs this information in a standard Windows event log format that can also be sent to a SIEM if used in an enterprise. While Sysmon does provide some monitoring capabilities, it can be easily shut down by attackers and provides no automated alerting. Sysmon is available at <http://technet.microsoft.com/en-us/sysinternals/dn798348> While logging is nice, it provides no value if the log is not reviewed. The purpose of this post is to provide an easy and automated way to present the Sysmon event log for review and a batch script using the tools and techniques described in this post will be available for download. If Sysmon is not already installed, download from Microsoft Sysinternals and install using a command line such as: `sysmon -i -accepteula -h md5 -n -l` This installs Sysmon as a service that will survive reboots, collect network connection information, record MD5 hashes for all created processes, and record loading of modules.

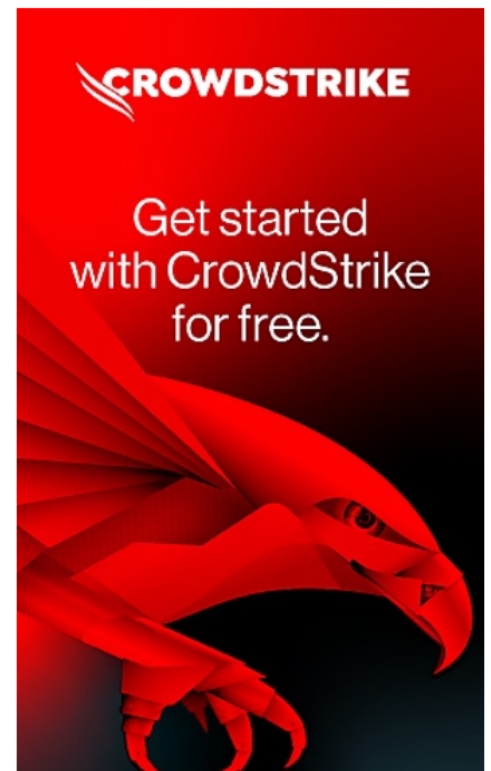
The Log File

Once Sysmon is installed, it records everything to a standard Windows event log. On a Windows

CATEGORIES

	Artificial Intelligence	44
	Cloud & Application Security	136
	Data Protection	18
	Endpoint Security & XDR	331
	Engineering & Tech	84
	Executive Viewpoint	176
	Exposure Management	110
	From The Front Lines	197
	Next-Gen Identity Security	61
	Next-Gen SIEM & Log Management	107
	Public Sector	40
	Small Business	11
	Threat Hunting & Intel	205

CONNECT WITH US



GoSecure, Inc.
Exhibit 2048
CrowdStrike v. GoSecure
IPR2025-00070

The Log File

Once Sysmon is installed, it records everything to a standard Windows event log. On a Windows 7 system and above, this file is located here: C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx This log file is in a standard event log format and thus not easily read. A sample log entry can be seen on the Sysinternal's Sysmon page^{<2>}. Microsoft Event Viewer can open the log, but each entry must be individually reviewed; proper analysis requires something a little more automated. To see examples of using Event Viewer and further Sysmon information in general, see Carlos Perez's post^{<3>}. To copy the log file for further parsing, use a command like this: robocopy C:\Windows\system32\winevt\Logs\ C:\Users\User\Desktop\sysmon Microsoft-Windows-Sysmon%4Operational.evtx This command will simply copy out the log file and place it on the user's desktop in a folder named sysmon.

Parsing

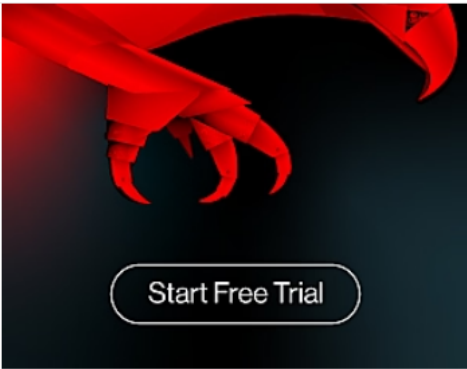
To turn the XML event log into an easier to digest file, we can use Microsoft Logparser^{<4>}. Logparser will parse the event log into a CSV file using this command: logparser -i:evt -o:csv "Select RecordNumber,TO_UTCTIME(TimeGenerated),EventID,SourceName,ComputerName,SID,Strings from %src% WHERE EventID in ('1','2','3','4','5','6','7')" > sysmon\sysmon_parsed.txt Now we have a plain text file we can easily open in Excel or use for further automated parsing. If reviewing in Excel, open as a delimited file with both "," and "|" chosen as delimiters. To pull further information out of the file, we can turn to TekDefense's TekColle^{<5>} python script. This script will help us gather all IP Address, MD5 hashes, domain names, and executable names. TekCollect requires Python 2.7 and we can launch the script using a command like: python tekcollect.py -f sysmon\sysmon_parsed.txt -t MD5 > sysmon\Hashes.txt This command will automatically search the parsed Sysmon log for any MD5 hashes it can find. The resulting Hashes.txt will contain a de-duplicated list of all the MD5 hashes found. The -t switch also allows us to designate the information we want to pull from the file. We can repeat the command using "ip4", "exe", and "domain" to finish collecting the desired information and create additional easy to read text files for review.

Analysis

Now we have nice and neat text files parsed from the Sysmon event log, suitable for analysis. A manual review of the text files created could lead to a discovery or previously unknown indicators. However, since manual review can sometimes be time consuming, there are a few automated tricks we can employ to make our job easier.

Keyword Search

Included with the script that accompanies this blog post is a file called "sysmon_keywords.tx". This file contains 15 example keywords that might warrant further follow-up. The keywords include searches for terms like "whoami", "tasklist", and "quser" as well as file extensions like ".bat", ".cmd", and ".rar". Any results for these terms will be placed in a separate file named Keywords.csv. The "sysmon_keywords.txt" file is easily editable and can contain IP Addresses, domain names, file names, or any other Regex search term you might want to monitor for quick



FEATURED ARTICLES

October 01, 2024

CrowdStrike Named a Leader in 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

September 25, 2024

Recognizing the Resilience of the CrowdStrike Community

September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection

September 18, 2024

SUBSCRIBE

Sign up now to receive the latest notifications and updates from CrowdStrike.

Sign Up

See CrowdStrike Falcon® in Action

Detect, prevent, and respond to attacks— even malware-free intrusions—at any stage, with next-generation endpoint protection.

See Demo

Included with the script that accompanies this blog post is a file called "sysmon_keywords.tx". This file contains 15 example keywords that might warrant further follow-up. The keywords include searches for terms like "whoami", "tasklist", and "quser" as well as file extensions like ".bat", ".cmd", and ".rar". Any results for these terms will be placed in a separate file named Keywords.csv. The "sysmon_keywords.txt" file is easily editable and can contain IP Addresses, domain names, file names, or any other Regex search term you might want to monitor for quick and easy wins when reviewing the activity taking place on the system. This type of automated search could help narrow down the hunting process Jack Crook describes in his recent blog post[6](#).

See Demo

Hash Analysis

The first file to examine is the list of MD5 hashes. While a list of hashes on its own does not mean much, we can use an automated VirusTotal lookup to determine if any of the hashes warrant a closer look. I prefer to use WoanWare's [virustotalchecker7](#), however, it does require Net 4.5 and a VirusTotal API key[8](#). Another option is to use Didier Stevens' [virustotal-search.py script9](#), but an API key is still needed. The great thing about this tool is the use of caching. If you use caching and have searched the same hash in the past 30 days, you get the cached result, which can greatly speed up analysis. This is an excellent option if you end up completing this Sysmon analysis process once a week. After the initial run, the tool will only need to search new hashes it hasn't checked recently. Using this command will automate the VirusTotal lookups and give us two files to review: `virustotalchecker.exe -m c -f sysmon\Hashes.txt -o .`. This produces two CSV files, one file contains matches and one file contains hashes without matches. Searching the file with matches will tell us if there were any hashes on VirusTotal with a high confidence of positive anti-virus detects. If a hash is deemed suspicious, copy the hash and search the `sysmon_parsed.txt` file to see which process and command line are responsible for the entry. Keep in mind that not all suspicious hashes will have matches on VirusTotal.

IP Address Analysis

The second file to check is the one containing IP addresses. A nice way of checking these in bulk is using the GUI program IPNetInfo from NirSoft[9](#). The program allows the user to paste a list of IP addresses as input and will automatically filter out any non-public IP Addresses. For scripting you can automatically launch the program with the list as input using a command like: `ipnetinfo.exe /ipfile sysmon\IPs.txt`. This command will still launch the GUI to allow for bulk review of the WhoIs results. With a huge list of IP Addresses to check, it might be beneficial to use the option "Pause for 30 Seconds after Retrieving 50 IP Addresses". This will limit the program from making too many requests and getting your IP Address temporarily blacklisted from making additional queries. There is also an option to retry failed queries. A second option in automatically searching IP Addresses is to use Team Cymru's server[10](#) for bulk lookups. This process involves using a NetCat connection to send the list of IP Addresses for automatic processing. The process is very quick and the command to use looks like: `ncat.exe whois.cymru.com 43 < sysmon\IPs.txt > sysmon\Whois_Results.txt`. After the IP Addresses have been resolved and the WhoIs information has been collected, it is easy to view and sort the results. After completing this process once or twice and collecting a nice baseline of results, it should be easy to pick out information that seems out of place. For instance, it is easy to sort by Country to see if any unexpected connections have been made. If an IP Address warrants further follow-up, search the `sysmon_parsed.txt` file to see which process is making the connection.

Conclusion

Country to see if any unexpected connections have been made. If an IP Address warrants further follow-up, search the sysmon_parsed.txt file to see which process is making the connection.

Conclusion

Sysmon is great for providing some simple monitoring information on the host system and the recent version allows for the use of configuration and filter files. The process outlined above gives us automated parsing for the [endpoint monitoring](#) that Sysmon completes. The data presented by the parsing is easy to review and should help when looking for indicators of attacker activity. To make this process even easier, the commands listed above are compiled into an easy to use batch script. The script will automatically collect and parse the Sysmon Event Log when run on the system to investigate or you can optionally designate an already collected log file. The script will then follow the process outlined by parsing the event log, running TekCollect to grab specific indicators, searching for keywords, launching a VirusTotal hash comparison, and completing a bulk WhoIs search. To get full access to CrowdStrike's next-gen antivirus solution for 15 days visit the [Falcon Prevent free trial page](#). The batch script can be downloaded

at <https://github.com/CrowdStrike/Forensics>. <1> <http://digital-forensics.sans.org/blog/2014/08/12/sysmon-in-malware-analysis-lab> <2> <http://technet.microsoft.com/en-us/sysinternals/dn798348> <3> <http://www.darkoperator.com/blog/2014/8/8/sysinternals-sysmon> <4> <http://www.microsoft.com/en-us/download/details.aspx?id=24659> <5> <http://www.tekdefense.com/tekcollect/> <6> <https://findingbad.blogspot.com/2016/07/my-thoughts-on-threat-hunting.html> <7> <http://www.woanware.co.uk/forensics/virustotalchecker.html> <8> <https://docs.virustotal.com/docs/api-overview> <9> <http://blog.didierstevens.com/programs/virustotal-tools/> <10> <http://www.nirsoft.net/utils/ipnetinfo.html> <11> <https://www.team-cymru.org/Services/ip-to-asn.html#whois>

 Tweet

 Share



CrowdStrike 2025 Threat Hunting Report

Adversaries weaponize and target AI at scale.

Download report →

Related Content



CrowdStrike Research: Security Flaws in



CrowdStrike 2025 European Threat Landscape



CrowdStrike 2025 APJ eCrime Landscape

http://www.malware-reports.com/blog/2017/07/07/emergency-response/ <5>
http://www.tekdefense.com/tekcollect/ <6> https://findingbad.blogspot.com/2016/07/my-thoughts-on-threat-hunting.html <7> http://www.woanware.co.uk/forensics/virustotalchecker.html <8> https://docs.virustotal.com/docs/api-overview <9>
http://blog.didierstevens.com/programs/virustotal-tools/ <10> http://www.nirsoft.net/utils/ipnetinfo.html <11> https://www.team-cymru.org/Services/ip-to-asn.html#whois>

[X](#) Tweet

[Share](#)



CrowdStrike 2025 Threat Hunting Report

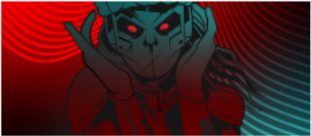
Adversaries weaponize and target AI at scale.

[Download report →](#)

Related Content



CrowdStrike Research: Security Flaws in DeepSeek-Generated Code Linked to Political Triggers



CrowdStrike 2025 European Threat Landscape Report: Extortion Rises, Nation-State Activity Intensifies



CrowdStrike 2025 APJ eCrime Landscape Report: A New Era of Threats Emerges

« Sheep Year Kernel Heap Fengshui: Spraying in the Big Kids' Pool

Cyber Kung-Fu: The Great Firewall Art of DNS Poisoning »

