SUNBURST indicator detection in QRadar

Back to Blog List

By Gladys Koskas posted Sat December 19, 2020 12:25 PM

Estimated reading time: 6 minutes

This week, and based on current information as of the time of publication, SolarWinds announced a cyberattack that inserted a vulnerability into the SolarWinds® Orion® Platform software builds for versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1. This vulnerability could enable an attacker to compromise the server(s) on which SolarWinds runs, and thus gain a foothold in the victim's network. Post compromise, the attacker can conduct lateral movement, data exfiltration and other threat activity.

The United States Cybersecurity and Infrastructure Security Agency (CISA) has published Emergency Directive 21-101, advising Federal agencies to disconnect or power down all SolarWinds Orion products until further notice.

As with the 'FireEye Red Team Tools detection in QRadar' blog, in this blog we'll provide guidance that can help you use QRadar to respond quickly.

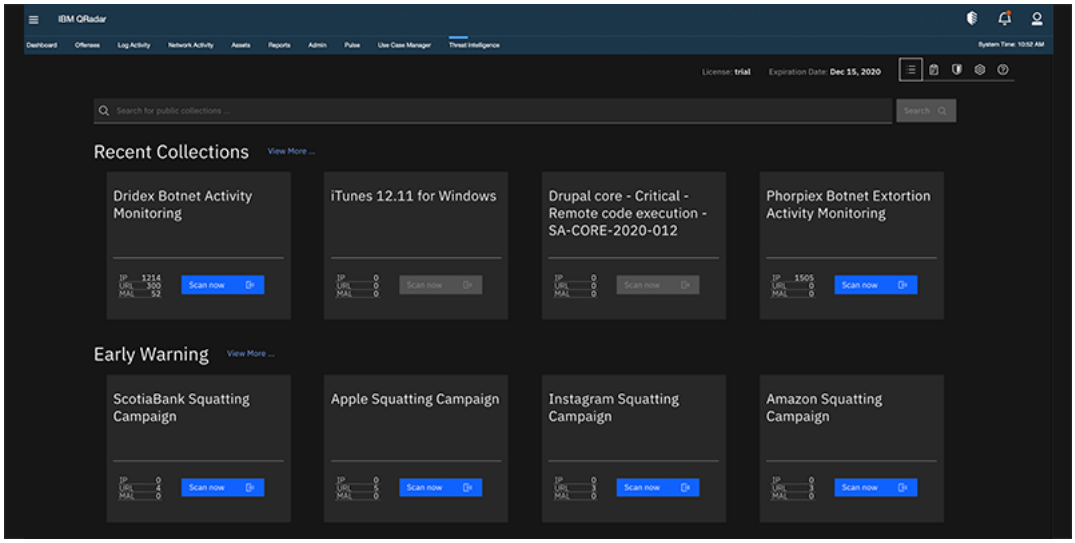
This blog will cover the following topics and content extensions:

- Threat Intelligence
- Snort Rules
  - IBM Security QRadar Custom Properties for Snort
- MD5, SHA-1 and SHA-256
- Pipe creation and Sysmon
  - IBM QRadar Custom Properties for Microsoft Windows
- Endpoint content extension
  - IBM QRadar Endpoint Content Extension
  - IBM QRadar Custom Properties for Microsoft Windows
  - IBM QRadar Custom Properties for Linux
- Threat Monitoring Content Extension
  - IBM QRadar Security Threat Monitoring Content Extension

Threat Intelligence

IBM Security X-Force researchers published a collection of IOCs, including malicious file hashes, IP addresses and URLs, connected to this on-going threat. These IOCs can easily be brought into QRadar using the Threat Intelligence App, which can be downloaded either from IBM Security App Exchange or natively via the QRadar Assistant. Threat indicators can be added to a reference set so that they can be used within building blocks, rules and searches to detect the presence of these IOCs within your environment. Public X-Force Collections, including this one, are free to existing QRadar customers.

QRadar customers who also subscribe to the IBM Security X-Force Advanced Threat Protection Feed have access to a built-in "Am I Affected?" featured with the Threat Intelligence app. This tool can be used in tandem with other forms of threat intelligence that may become available in this developing situation to help assess known IOCs. With this subscription, new X-Force collections are loaded directly into QRadar, and users can simply click 'Scan now' to automatically search for all IOCs associated with a collection. The query results will show you which systems and users may have been connected to this threat, assisting you to initiate investigation, remediation and response.



If you do not currently subscribe to the Advanced Threat Protection Feed, a 30-day free trial is available.

Snort Rules

Once again, FireEye and Cisco Talos teams provided a new set of Snort rules to implement. QRadar users can easily create a new rule based on these signatures, correlate these insights with other events, or optionally be alerted directly via email. The steps to implement this are:

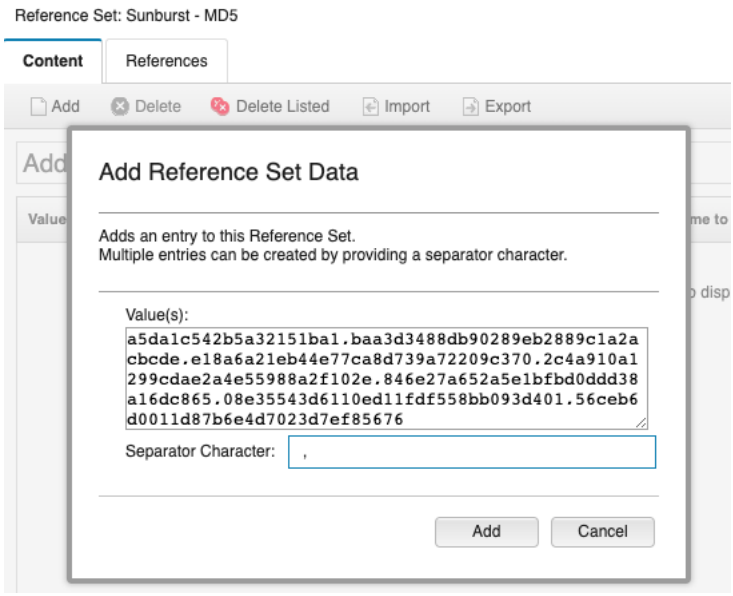
1. Install the IBM Security QRadar Custom Properties for Snort content extension
2. Create a new Event rule

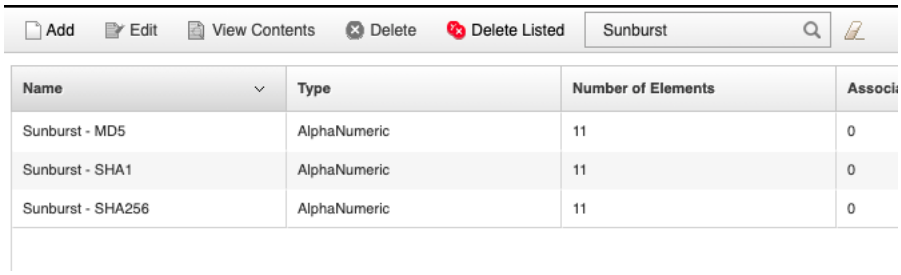
Apply **Sunburst - Snort Rules** on events which are detected by the Local system
and when the event(s) were detected by one or more of **Snort Open Source IDS**
and when the event matches **"Rule ID" in**
(77600832,77600833,77600842,77600843,77600844,77600845,77600846,77600847,77600848,77600850,77600851,77600852,77600853,7760
77600840,77600863,77600864,77600865,77600837,77600856,77600857,77600858,77600859,77600860,77600866,56660,56661,56662,56663,
AQL filter query

MD5, SHA-1 and SHA-256

We talked about it, file hashes are a great source to improve threat detection. Once again, you can have a quick implementation by enabling detection with MD5, SHA-1 and SHA-256 through three reference sets and one custom rule.

1. Create three Reference Sets, one per hash type, and populate them with the Sunburst_md5, Sunburst_sha1, Sunburst_sha256 files (comma separated).





2. Install content extensions containing Hash properties or create your own.
   On the App Exchange, you can find MD5, SHA-1 and SHA-256 parsed for the following devices:
   Carbon Black Response, Cisco AMP, McAfee ePolicy Orchestrator, Microsoft Windows Defender ATP, Microsoft Windows Security Event Log
3. Create a rule that tests the Custom Properties *MD5 Hash*, *Parent MD5*, *SHA1 Hash*, *Parent SHA1 Hash*, *SHA256 Hash*, *Parent SHA256 Hash* against the new Reference Sets.

   Apply **Sunburst - Tools Hash** on events which are detected by the Local system
   and when the event(s) were detected by one or more of **Carbon Black Response, Cisco AMP, McAfee ePolicy Orchestrator, Microsoft Windows Defender ATP, Microsoft Windows Security Event Log**
   and when the event matches **("MD5 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', "MD5 Hash")) OR ("Parent MD5" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', "Parent MD5")) OR ("SHA1 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA1', "SHA1 Hash")) OR ("Parent SHA1 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', "Parent SHA1 Hash")) OR ("SHA256 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA256', "SHA256 Hash")) OR ("Parent SHA256 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA256', "Parent SHA256 Hash"))** AQL filter query

   Enter an AQL filter query:

```
("MD5 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', "MD5 Hash"))
OR ("Parent MD5" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', "Parent MD5"))
OR ("SHA1 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA1', "SHA1 Hash"))
OR ("Parent SHA1 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - MD5', "Parent SHA1 Hash"))
OR ("SHA256 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA256', "SHA256 Hash"))
OR ("Parent SHA256 Hash" IS NOT NULL AND REFERENCESETCONTAINS('Sunburst - SHA256', "Parent SHA256 Hash"))
```

Pipe creation and Sysmon

In the blog published by FireEye regarding SUNBURST, there is a mention about the creation of a pipe named *583da945-62af-10e8-4902-a8f205c72b2e* as one of the “delivery and installation” mechanism:

> The sample only executes if the filesystem write time of the assembly is at least 12 to 14 days prior to the current time; the exact threshold is selected randomly from an interval. The sample continues to check this time threshold as it is run by a legitimate recurring background task. Once the threshold is met, the sample creates the named pipe 583da945-62af-10e8-4902-a8f205c72b2e to act as a guard that only one instance is running before reading SolarWinds.Orion.Core.BusinessLayer.dll.config from disk and retrieving the XML field appSettings. The appSettings fields' keys are legitimate values that the malicious logic re-purposes as a persistent configuration. The key ReportWatcherRetry must be any value other than 3 for the sample to continue execution.

Source: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

If you are collecting Sysmon logs, you have another opportunity for a quick way to detect another IOC.

1. Download the IBM QRadar Custom Properties for Microsoft Windows content extension
2. Create a rule that detects the pipe name mentioned in the blog

> Apply **Sunburst - Pipe Name** on events which are detected by the Local system
> and when the event(s) were detected by one or more of **Microsoft Windows Security Event Log**
> and when the event **QID is one of the following (5001836) PipeEvent (Pipe Created)**
> and when the event matches **PipeName (custom) is any of 583da945-62af-10e8-4902-a8f205c72b2e**

Endpoint content extension

This time I will be quick with this one, but I wanted to renew my recommendation to download the latest version of the Endpoint content pack.

The pack has been built to detect lateral movement, reconnaissance tools, help to make the difference between a legitimate administration task from a suspicious one... All these behaviour have been mentioned in all the blogs you've read on the topic so far.

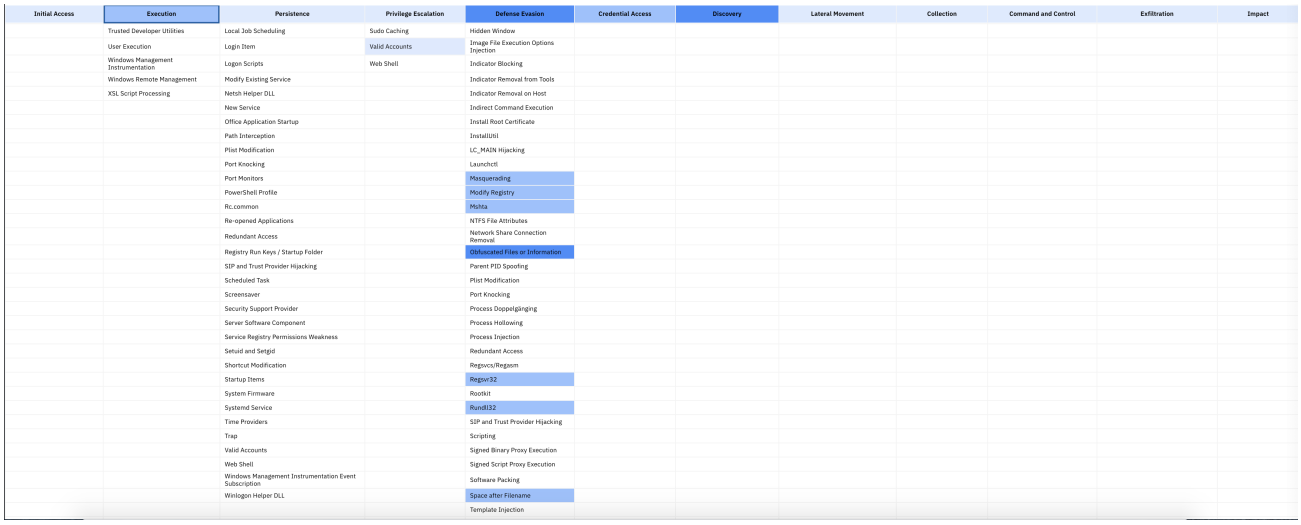
Below is the list of the rules (excluding building blocks) present in the Endpoint content extension

Attempt to Delete Shadow Copies	Ransomware IOCs Detected on Multiple Machines
Cobalt Strike Behaviour Detected	Ransomware: BadRabbit IOC in Events
Communication with a Potential Hostile Host	Ransomware: BadRabbit IOC in Flows
Communication with a Potential Hostile IP Address	Ransomware: Maze IOC in Events
Credential Dumping Activities Discovered	Ransomware: Maze Suspicious File Transfer
Critical File Deleted (Unix)	Ransomware: Petya / NotPetya IOC in Events
Critical File Permission Changed (Unix)	Ransomware: Petya / NotPetya IOC in Flows
Critical Security Tool Killed (Unix)	Ransomware: Petya / NotPetya Payload in Flows
Critical Security Tool Stopped	Ransomware: REvil IOC in Events
Detection of Malicious File or Process	Ransomware: WCry IOC in Events
Detection of Malicious IOC	Ransomware: WCry IOC in Flows
Excessive Failed Access to an Administrative Share from the Same Source	Ransomware: WCry Payload in Flows
Excessive File Deletion and Creation	RDP Hijacking Tool Detected
Excessive Login Failures via RDP	Recommended Blocked Process is Running
Excessive Login Failures via RDP to Multiple Machines	Reconnaissance Tool Detected
Excessive Nslookup Usage	Recovery Disabled in Boot Configuration Data
File Created with Right to Left Override	Search for Password Files using findstr (Windows)
File Created with Space After Filename	Search for Password Files using grep or find (Unix)
File Decode or Download followed by Suspicious Activity	Search for Password Files using Select-String (Windows)
Potential Component Object Model (COM) Hijacking	SharpHound PowerShell Detected
Potential DLL Hijacking	Suspicious Activity Followed by Endpoint Administration Task
Potential Malicious Application Shimming	Suspicious Amount of Files Deleted on the Same Machine

Process Masquerading (Unix)	Suspicious Amount of Files Renamed on the Same Machine (Windows)
Process Masquerading (Windows)	Suspicious Amount of Files Renamed/Moved on the Same Machine (Unix)
Programming Environment Spawned by a Suspicious Process	User Account Creation followed by Account Deletion (Unix)
Ransomware Decryption Instructions Created	User Account Creation followed by Account Deletion (Windows)
Ransomware Encrypted File Extension	

All these rules provide a wide spectrum of detection capabilities

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	CMSTP	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-hop Proxy		Runtime Data Manipulation
	LSASS Driver	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Service Stop
	Launchctl	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	Shared Webroot		Multilayer Encryption		Stored Data Manipulation
	Local Job Scheduling	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	DLL Side-Loading	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File Deletion		System Time Discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Process Injection	File System Logical Offsets		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File and Directory Permissions Modification							
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Scheduled Task	Gatekeeper Bypass							
	Source	LSASS Driver	Service Registry Permissions Weakness	Group Policy Modification							
	Space after Filename	Launch Agent	Setuid and Setgid	HISTCONTROL							
	Third-party Software	Launch Daemon	Startup Items	Hidden Files and Directories							
	Trap	Launchctl	Sudo	Hidden Users							
	Trusted Developer Utilities	Local Job Scheduling	Sudo Caching	Hidden Window							



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Trusted Developer Utilities	Local Job Scheduling	Sudo Caching	Hidden Window							
	User Execution	Login Item	Valid Accounts	Image File Execution Options Injection							
	Windows Management Instrumentation	Logon Scripts	Web Shell	Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		LC_MAIN Hijacking							
		Port Knocking		Launchctl							
		Port Monitors		Masquerading							
		PowerShell Profile		Modify Registry							
		Rc.common		Mshta							
		Re-opened Applications		NTFS File Attributes							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		Obfuscated Files or Information							
		SIP and Trust Provider Hijacking		Parent PID Spoofing							
		Scheduled Task		Plist Modification							
		Screensaver		Port Knocking							
		Security Support Provider		Process Doppelgänging							
		Server Software Component		Process Hollowing							
		Service Registry Permissions Weakness		Process Injection							
		Setuid and Setgid		Redundant Access							
		Shortcut Modification		Regsvcs/Regasm							
		Startup Items		Regsvr32							
		System Firmware		Rootkit							
		Systemd Service		Rundll32							
		Time Providers		SIP and Trust Provider Hijacking							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		Software Packing							
		Winlogon Helper DLL		Space after Filename							
				Template Injection							

Please refer to the documentation for more information on each rule. You can also refer to the Endpoint dedicated blog to have a better understanding of the implementation of some use cases.

Threat Monitoring Content Extension

The multi-task pack ! This pack is mentioned last in this blog because it is certainly going to need some tuning to be adapted to what you are looking for, but it is definitely a good help to know where to go.

As an example, thanks to your endpoint security software, you can increase the visibility on a threat spreading through the network. Indeed, this extension contains a series of rules alerting on security software.

	Same Threat Detected on Multiple Hosts	Threats	Custom Rule	Event
	Same Threat Detected on Multiple Servers	Threats	Custom Rule	Event
	Same Threat Detected on Same Host	Threats	Custom Rule	Event
	Same Threat Detected on Same Network Different Hosts	Threats	Custom Rule	Event
	SMB Traffic Permitted From a Compromised Host	Threats	Custom Rule	Event
	Successful Communication to a Malicious Website	Threats	Custom Rule	Event

Rule

Apply Same Threat Detected on Multiple Hosts on events which are detected by the Local system
and when an event matches any of the following BB:DeviceDefinition: AV/AM, BB:DeviceDefinition: IDS / IPS
and NOT when an event matches any of the following BB:HostDefinition: Servers
and when at least 5 events are seen with the same Threat Name (custom) and different Source Address in 5 minutes

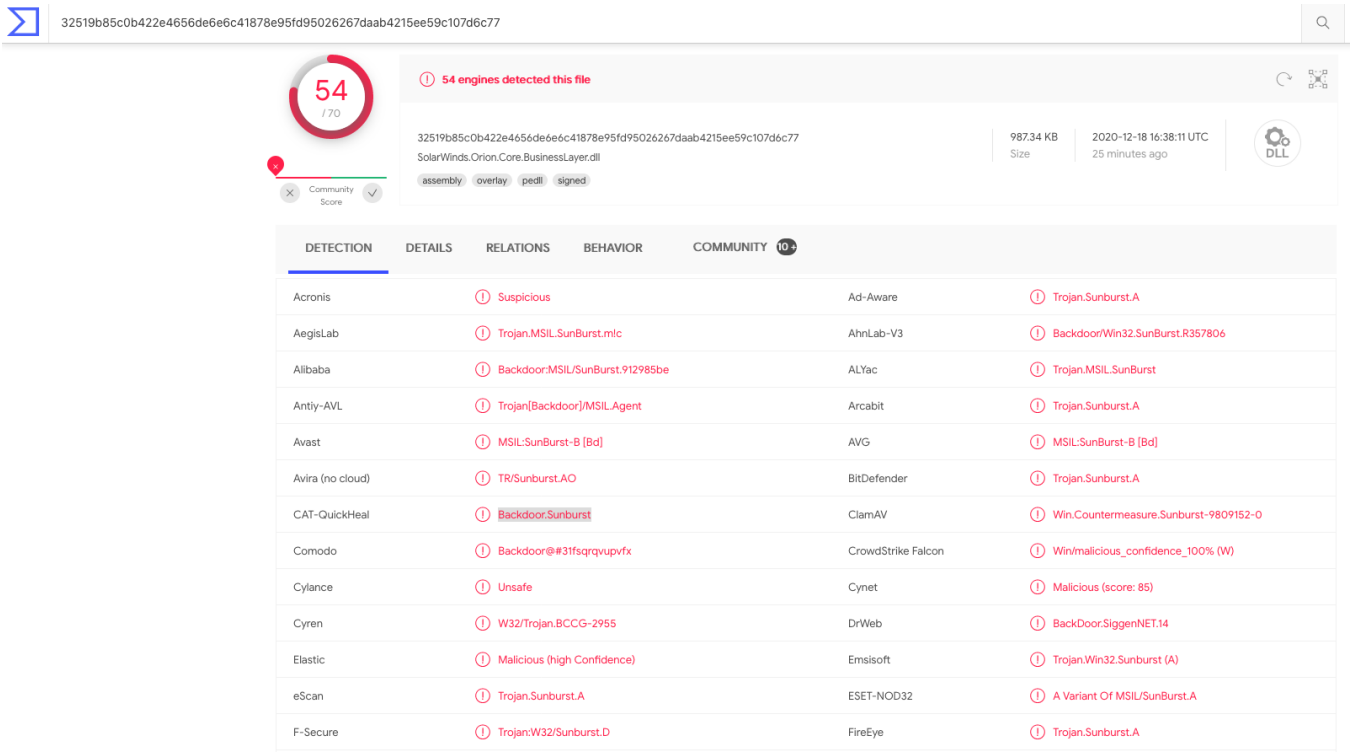
All you have to do is to:

1. Ensure your device is listed in one of BB:DeviceDefinition: AV/AM or BB:DeviceDefinition: IDS / IPS Building blocks
2. Get the Threat Name parsed either by downloading one of our content extension, or creating your own extraction.

You can decide to duplicate the rules to focus the detection on SUNBURST specifically, and have a higher priority rule response (email, SNMP trap, vulnerability scan). Simply add a new filter to the original rule, catching the specific Threat Name reported by your product:

and when the event matches **Threat Name (custom) is any of *Backdoor.Sunburst***

Please refer to your product documentation to get more information on the relevant detection name



Conclusion

The above steps can enable you to easily take advantage of the publicly available IOCs and Countermeasures to detect indicators of the SUNBURST threat within your environment. All of the QRadar apps, custom properties and content extensions mentioned above are available free of charge to all QRadar customers and can be downloaded either from the IBM Security App Exchange or natively via QRadar Assistant.

As usual, we build content for you, to save you time and effort, a content that you can use as a base and adapt to your environment and your needs. Don't hesitate to give us any feedback or ideas, tell us what you need.

If you are directly impacted and in need of expert assistance, you can contact the IBM Security X-Force Incident Response team, who is available to assist 24×7, at US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

#QRadar
#Featured-area-2 #Highlights-home

#Highlights
#Spotlight

0 comments

9050 views