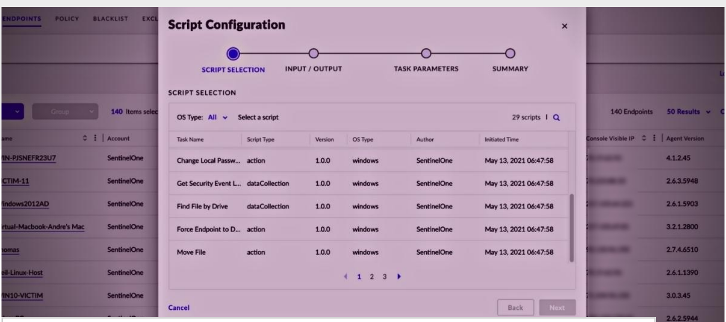


Revolutionize Incident Response and Endpoint Management with Remote Script Orchestration

November 8, 2021
by Resha Chheda & Noa Frankel

A successful cyber attack can compromise your data and cripple business operations within mere hours or even minutes. Therefore, the speed with which your organization can contain and recover from an attack is critical to limit business disruption and reduce financial costs. Delays during investigation and remediation leave organizations highly vulnerable to security risks.

SentinelOne Remote Script Orchestration (RSO) allows enterprises to investigate threats on multiple endpoints across the organization remotely and enables them to easily manage their entire fleet.

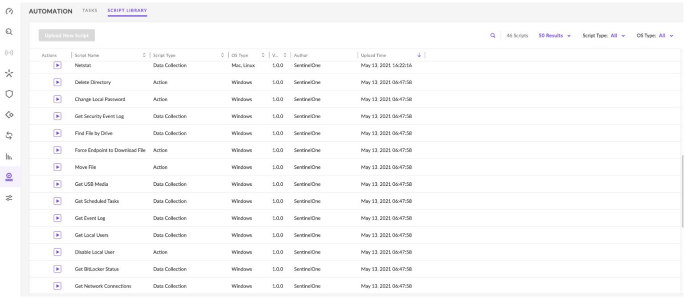
It lets incident responders run scripts to collect data and remotely respond to events on endpoints. They can collect forensic artifacts, execute complex scripts and commands, install and uninstall IR tools and more on hundreds of endpoints simultaneously—Windows, Mac, and Linux—via the UI or API, to simplify forensic data collection and accelerate triage.

Revolutionize Incident Response & Endpoint Management with Remote Script Orchestration
By Resha Chheda & Noa Frankel
SentinelOne

How Remote Script Orchestration Works

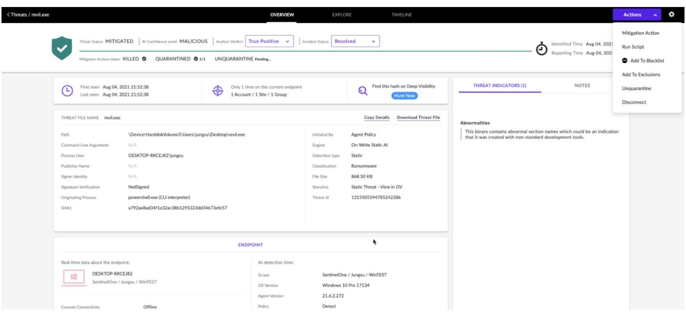
Remote Script Orchestration includes a Script Library from SentinelOne with scripts for all platforms. Customers can run remote scripts via multiple points from the console. Regardless of whether a single endpoint is compromised or multiple endpoints are associated with a threat or a group of machines that need to be investigated, RSO is available from different entry points to serve the user's diverse needs.

- **Script Library**



Actions	Script Name	Script Type	OS Type	V...	Author	Upload Time
▶	Netstat	Data Collection	Mac, Linux	1.0.0	SentinelOne	May 13, 2021 16:22:16
▶	Delete Directory	Action	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Change Local Password	Action	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Get Security Event Log	Data Collection	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Find File by Drive	Data Collection	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Force Endpoint to Download File	Action	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Move File	Action	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Get USB Media	Data Collection	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Get Scheduled Tasks	Data Collection	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Get Event Log	Data Collection	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Get Local Users	Data Collection	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Disable Local User	Action	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Get BitLocker Status	Data Collection	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58
▶	Get Network Connections	Data Collection	Windows	1.0.0	SentinelOne	May 13, 2021 06:47:58

- **Alerts**



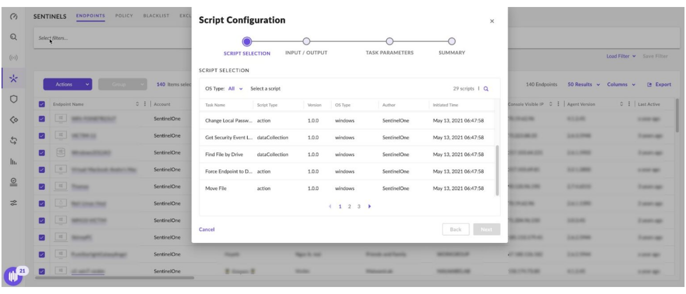
Threat Status: MITIGATED
AI Confidence Level: MALICIOUS
Analyst Verdict: True Positive
Incident Status: Resolved
Mitigation Actions taken: KILLED QUARANTINED 1/1 UNQUARANTINE Pending...
Identified Time Aug 04, 2021
Reporting Time Aug 04, 2021
First seen Aug 04, 2021 21:52:38
Last seen Aug 04, 2021 21:52:38
Only 1 time on the current endpoint
1 Account / 1 Site / 1 Group
Find this hash on Deep Visibility

THREAT FILE NAME revil.exe
Path \Device\HarddiskVolume3\Users\jungsu\Desktop\revil.exe
Command Line Arguments N/A
Process User DESKTOP-RKCEJ82\jungsu
Publisher Name N/A
Signer Identity N/A
Signature Verification NotSigned
Originating Process powershell.exe (CLI interpreter)
SHA1 a792ae8ad34f1e32ac38b1295323dd34673efe57
Initiated By Agent Policy
Engine On-Write Static AI
Detection type Static
Classification Ransomware
File Size 868.50 KB
Storyline Static Threat - View in DV
Threat Id 1215505594785242286

Abnormalities
This binary contains abnormal section names which could be an indication that it was created with non-standard development tools.

Real-time data about the endpoint:
DESKTOP-RKCEJ82
SentinelOne / Jungsu / WinTEST
Console Connectivity Offline
At detection time:
Scope SentinelOne / Jungsu / WinTEST
OS Version Windows 10 Pro 17134
Agent Version 21.6.2.272
Policy Detect

- **Sentinels**



SCRIPT SELECTION
OS Type: All Select a script 29 scripts

Task Name	Script Type	Version	OS Type	Author	Initiated Time
Change Local Passw...	action	1.0.0	windows	SentinelOne	May 13, 2021 06:47:58
Get Security Event L...	dataCollection	1.0.0	windows	SentinelOne	May 13, 2021 06:47:58
Find File by Drive	dataCollection	1.0.0	windows	SentinelOne	May 13, 2021 06:47:58
Force Endpoint to D...	action	1.0.0	windows	SentinelOne	May 13, 2021 06:47:58
Move File	action	1.0.0	windows	SentinelOne	May 13, 2021 06:47:58

How Can SentinelOne RSO Help Enterprises?

1. **Enable Power Forensics**
   When it comes to cyberattacks, time is crucial. Instantaneous access to an infected machine is valuable but not enough. No SOC analyst wants or has the time to access hundreds of infected machines, one by one, to collect all relevant artifacts and conduct an investigation.With RSO, SOC analysts can run scripts on hundreds of endpoints simultaneously to collect anything needed for an investigation with a click of a button. RSO enables Incident Responder teams to jump start investigations with security event logs, running services, scheduled tasks, network connections, connected removable media, memory analysis, and more. New scripts can be easily created and added to the library to collect whatever is needed from remote machines.
2. **Rapid Attack Containment**
   Using RSO, IR teams can quickly identify and investigate the chain of events and immediately respond to identified attacks. In addition to the existing response actions available from the Singularity platform, IR teams can use RSO to take immediate response actions to promptly contain threats in real-time—terminate processes, remove files, delete directories, disable local users, and more.
3. **Simplify Vulnerability and Configuration Management**
   Customers don't need to manage vulnerabilities and configurations by deploying and managing a range of tools. Security teams can use RSO to rapidly identify vulnerabilities and misconfigurations across their entire fleet. They can harden endpoints by deploying packages using custom scripts and thus reduce the attack surface.RSO lets customers unify management activities within a single agent and console to perform assessments, remediation actions reporting, and audit preparation from one platform.
4. **Automate Response Capabilities**
   The timing and effectiveness of your response are critical when your organization is under attack. RSO integration with Storyline Active Response™ enables customers to take automated response actions. It allows enterprises to incorporate custom detection logic and immediately push it out to their entire fleet, to quickly remediate threats. Automated response workflow dramatically reduces the time to remediation and the impact of attacks.

Designed and built in close partnership with some of the world's leading incident response providers, RSO delivers on SentinelOne's commitment to a holistic approach to cybersecurity, arming security analysts with the power of technology — to do more for what works for them. RSO is designed with a holistic approach and flexibility to be used by people with different skill sets.

- Non technical users can use the existing out of the box script library, which contains everything needed for investigation. With a few simple clicks all the needed data is at their hands.
- Users who are moderately technical can write simple scripts or modify existing scripts to customize them for whatever they need .There is no need to write a script from scratch.
- Highly technical users can write their own scripts and upload it to the library to be shared and used by other employees.

Putting RSO to Work In Your Organization

SentinelOne RSO gives security operations teams instantaneous access to thousands of machines. This gives you the power to do in-depth investigative work and take immediate response actions to promptly contain identified threats in real-time. SentinelOne RSO can be tailored to suit your organization to fit a variety of use cases such as:

- **Zero day threat detection**
  RSO can be used to quickly determine if your organization is vulnerable to an attack or identify vulnerable endpoints affected by the latest zero day threats. For example, incident responders could quickly and easily run the published scripts to determine if the enterprise was impacted by that vulnerability. This gives you the power to take immediate response actions to promptly contain

identified threats in real-time.

- **Customize and build optimal IR tools for intel gathering**
  Different teams often have different needs and requirements to collect various forensic artifacts for deeper investigation. SentinelOne RSO has granular capabilities that can be customized to let responders use pre-built scripts or use readily available scripts and tools that automate the gathering of common information like Autoruns, File Hashes, and ARP Tables.

SentinelOne RSO is a powerful tool that opens endless possibilities for enterprises. Responders can run scripts at scale to collect data and respond to events on endpoints, run scripts directly from the console or via command-line interface to automate response actions; basically, if you can think about it and script it, it is possible.

Conclusion

Legacy tools and endpoint products still require people to manually execute commands on each machine across the network individually. The sheer amount of data, devices, and workloads in today's enterprise environments makes IT and security operations simply too big, too vast, and too fast for humans alone to deal with.

SentinelOne RSO enables security and IT teams to remotely execute customizable remediation and response actions on the entire estate across every operating system, enabling rapid containment. SentinelOne RSO is the only remote orchestration solution on the market that, in the same platform as an industry-leading EPP, EDR, and XDR, supports macOS, Windows, and Linux environments.

If you would like to learn more about RSO and the SentinelOne XDR platform, read the RSO Solution Brief, contact us for more information, or request a free demo.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Understanding the Difference Between EDR, SIEM, SOAR, and XDR
- Customize Your EDR To Adapt To Your Environment With SentinelOne Storyline Active Response (STAR)
- Moving to an Endpoint-Centric Zero Trust Security Model with SentinelOne
- Securing Hybrid Cloud Containerized Workloads in AWS ECS Anywhere with SentinelOne Singularity
- Feature Spotlight: Introducing Singularity™ Conditional Policy
- Feature Spotlight: Ease Deployment and Minimize Risk With Ranger Pro™

©2023 SentinelOne, All Rights Reserved.