D3 SECURITY

INVESTIGATING AND RESPONDING TO THE SUNBURST MALWARE ATTACK

WHITEPAPER

In December of 2020, a global attack campaign was revealed wherein a state-sponsored threat actor used a network monitoring product from SolarWinds to infect thousands of companies and public sector entities. The attack had been undetected for at least nine months, allowing it to spread using highly sophisticated defense evasion techniques.

This SunBurst malware attack—the name we will be using for the SolarWinds incident—has left SOC teams around the world scrambling to determine whether they were affected, to what extent, and what they can do to minimize the damage. While no vendor can claim to have a silver bullet for preventing this type of attack, D3 NextGen SOAR offers some important features to help clients investigate and respond to potential instances of SunBurst malware in their environment.

In this whitepaper, you will learn:

- The limitations of conventional security tools when addressing SunBurst
- How NextGen SOAR goes beyond IOCs to uncover and evaluate compromise
- The three SunBurst-specific playbooks that are available to D3 clients

THE RESPONSE FROM CYBERSECURITY VENDORS

Many cybersecurity vendors, including EDR and TIP companies, have offered responses that are mostly limited to analyzing SunBurst samples and determining the IOCs. Signatures have been regularly updated to help security tools detect SunBurst IOCs going forward. Vendors and analysts have also categorized the methods used into MITRE ATT&CK TTPs.

However, there are limitations to what most vendors are able to offer. Because the root cause of the SolarWinds breach has not yet been made public, the methods for preventing SunBurst attacks cannot yet be entirely determined. Furthermore, because most vendors are focused on IOC detection, they cannot offer ways to determine the impact that has been made within organizations. In other words, they cannot find out how much data has been exfiltrated or how many critical servers have been compromised.

WHAT D3 NEXTGEN SOAR CAN OFFER

D3 NextGen SOAR has advanced capabilities that can go beyond the limitations of conventional detection solutions and correlate across tools and past events to help find more elements of SunBurst attacks. We have organized these features into three SunBurst-specific playbooks that are ready for D3 clients to deploy as they search for signs of compromise and respond accordingly. Our SunBurst playbooks perform three key functions:

1

THREAT HUNTING

D3's correlation capabilities can search past events for malicious SunBurst attack patterns to identify potentially compromised hosts and signs of data exfiltration. These correlations are more effective than simple IOC searches, because they can expand out to all linked events and encompass suspicious patterns such as irregular login times or VPN access from unusual regions.

2

SURVEILLANCE

D3 's ongoing surveillance mechanisms can actively hunt for suspicious TTPs and help SOC teams to discover sunburst attacks that are already underway. This helps locate systems that were breached before the EDR was updated to detect SunBurst signatures.

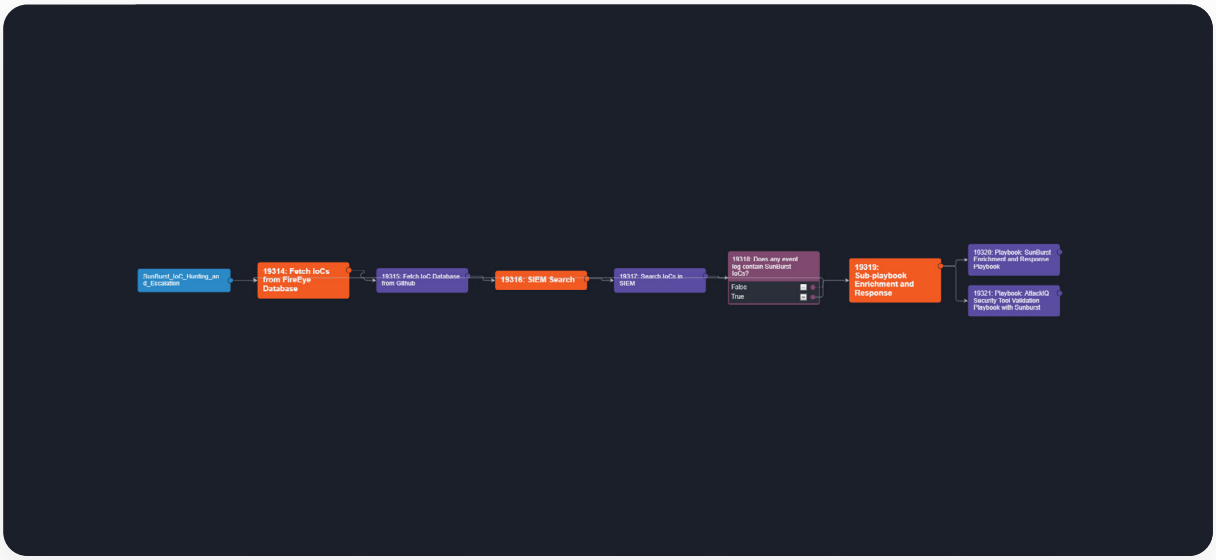
3

REMEDIATION

D3 can provide a decision-making and approval process for SOC teams to effectively take actions such as blocking the malware, quarantining hosts via EDR, blocking Sunburst C2 IPs via the firewall. In addition, D3 can automate AttackIQ's SolarWinds assessment scenarios to validate your security tools' ability to respond to SunBurst attacks.

PLAYBOOK #1

SUNBURST IOC HUNTING AND ESCALATION



OBJECTIVE

To actively hunt for the IOCs that match the malware signatures of SunBurst using the SIEM, and to create incidents in D3 SOAR when any suspicious signature is identified.

PROCESS

1. Automatically fetch updated IOCs from FireEye's shared database
2. Actively search for the IOCs in the SIEM to identify matched events

   If any IOC matches:

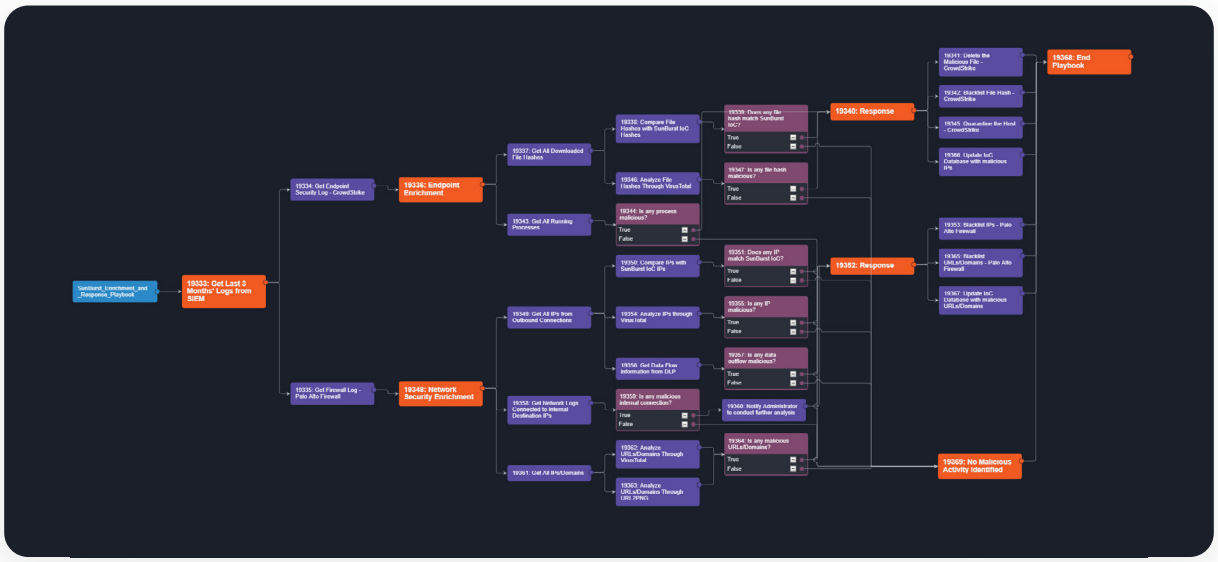
   - Create a new SunBurst incident in D3 SOAR
   - Execute **SunBurst Enrichment and Response Playbook** and **AttackIQ Security Tool Validation Playbook with Sunburst** for further analysis

   If no IOC matches:

   - Continuously monitor and hunt within the SIEM according to a predetermined schedule

PLAYBOOK #2

SUNBURST ENRICHMENT AND RESPONSE



OBJECTIVE

To coordinate multiple security tools including the SIEM, endpoint security, network security, and data loss prevention tool to further enrich and respond to the SunBurst threat.

PROCESS

1. Search the last three months (or other custom timeframe) of endpoint security logs from the SIEM:

   1.1 Search for downloaded files matching SunBurst IOC hash signatures

   If any file hash matches:

   - Delete the file using the endpoint security tool

   1.2 Search for any malicious running processes

   If any process is malicious:

   - Quarantine the host using the endpoint security tool

   1.3 Extract file hashes from the log and conduct analysis through VirusTotal

   If any file hash is malicious:

   - Delete the file and block the file hash
   - Flag the new malicious file hash as a potential SunBurst IOC and update the IOCs list

2. Search the last three months (or other custom timeframe) of network security logs from the SIEM:

   2.1 Search all outbound connections, including IP addresses and URLs/domains

   - **If any IP or URLs/domains match SunBurst IOCs:**
     - Block the IP or URL/domain using the firewall
   - Check other outbound connections for suspicious data exfiltration
   - Coordinate with the DLP tool to confirm if there are potential threats

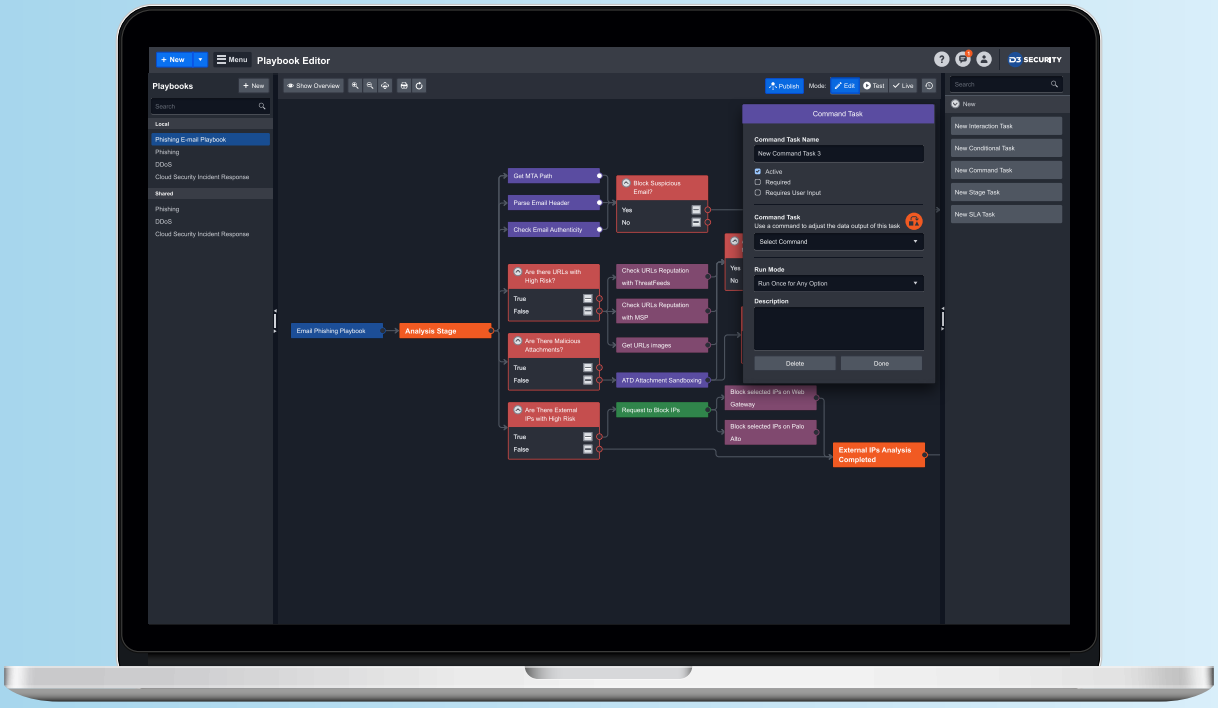
   2.2 Get all internal destination IP addresses to which this endpoint was trying to connect, in order to identify the potential lateral movement that could infect other environments and machines.

   - Add an ongoing surveillance task to actively monitor for any future potential lateral movement activities in the next three months (or other custom timeframe)

   2.3 Extract all external IPs and URLs/domains, and conduct further analysis through VirusTotal

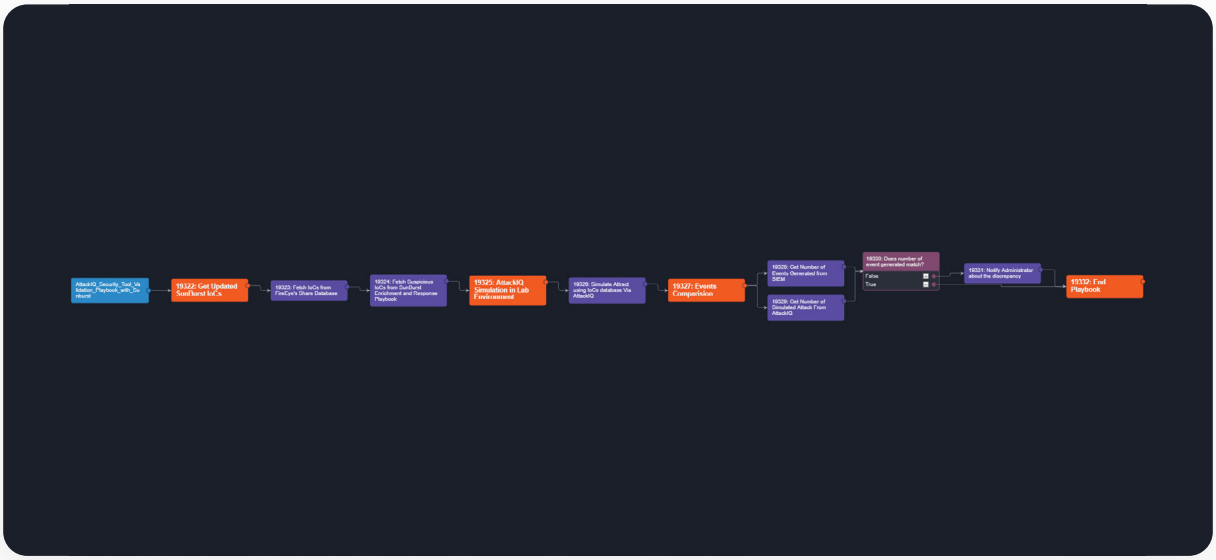
   If any IPs or URLs/Domains are malicious:

   - Block the IP or URL/domain using the firewall
   - Flag the new malicious IPs or URL/Domain as a potential SunBurst IOC, and update the IOCs list



PLAYBOOK #3

ATTACKIQ SECURITY TOOL VALIDATION PLAYBOOK WITH SUNBURST



OBJECTIVE

To confirm security tools will pick up the most updated SunBurst malware IOCs within the organization via AttackIQ simulation in a lab environment.

PROCESS

1. Automatically fetch updated IOCs from FireEye's shared database
2. Fetch other IOCs with the **SunBurst Enrichment and Response Playbook**
3. Simulate those IOCs in the lab environment via AttackIQ
4. Run assessments in AttackIQ
5. Check if the simulated threats are prevented by security tools
   - If threats are prevented, no further actions are required
   - If not, then notify administrators to reconfigure the system as necessary

ABOUT D3 SECURITY

D3 Security's Next-Generation SOAR platform combines the proactive analysis of MITRE ATT&CK with rapid, end-to-end automation, orchestration and response. Using D3's advanced capabilities, SOC operators around the world have expanded the speed and scale of their security operations, while strengthening their ability to identify suspicious behaviors, conduct efficient investigations, and remediate critical threats.

D3 SECURITY

www.d3security.com

SALES CONTACT

1-800-608-0081 (Ext. 2)
sales@d3security.com

FOLLOW US