Splunk® Enterprise Security Use Cases 6.1.0

Investigating potential zero-day activity with Splunk Enterprise Security

Generated: 2/07/2020 5:12 am
Investigating potential zero-day activity with Splunk Enterprise Security

Detect possible zero-day malware activity in your organization’s network with Splunk Enterprise Security. This scenario walks you through detecting malware activity that could indicate a zero-day exploit, and using the investigation results to improve your threat detection.

A sophisticated attack using zero-day malware could begin when a spearphishing email containing malware is sent to a target recipient within an organization.

1. The target opens the email and the malicious contents compromise their computer with malware.
2. After infecting the computer, the malware signals the attacker that it is ready for command and control.
4. Security analysts perform host-based forensics on the machine and identify malware that uses a zero-day exploit.
5. Security analysts use the forensic results to identify common indicators of the threat, such as malware hashes and malicious domain lists.

Required data sources

This use case relies on the following data sources that have been properly ingested into the Splunk platform in compliance with the Splunk Common Information Model.

- Asset information in the asset lookup. See Add asset and identity data to Splunk Enterprise Security in Administer Splunk Enterprise Security.
- One or more threat intelligence feeds. Splunk Enterprise Security has several threat intelligence feeds included. See Configure the threat intelligence sources included with Splunk Enterprise Security in Administer Splunk Enterprise Security.
- DNS (domain name system) data normalized to the Network Resolution CIM data model. For example, DNS queries collected by Splunk Stream. See Install and deploy add-ons in the Installation and Upgrade Manual for details on integrating Enterprise Security with Splunk Stream.
• Web surfing or Proxy logs normalized to the Proxy object of the Web CIM data model.
• Firewall activity logs normalized to the Network Traffic CIM data model.
• Active Directory (AD) logs normalized to the Authentication data model.
• Audit and system logs from database servers normalized to any of the relevant CIM data models, such as Databases, Change Analysis, or Authentication.

### Review risk behavior of hosts in your environment

Assess the risk posture of your environment to determine if hosts are displaying risky behavior that could pose a higher threat to your network than others.

1. Select **Security Intelligence > Risk Analysis** to open the **Risk Analysis** dashboard.
2. Review the **Risk Score By Object** to identify hosts with high risk scores. You notice the host 10.11.20.87 with a risk score of 800 and count of 16 events associated with it is one of the highest risk systems in your environment.
3. To see what types of sources are contributing to the increased risk for this host, review the **Recent Risk Modifiers**. You see a source of **Threat - Threat Activity Detected - Rule** which means that threat intelligence correlated with this host caused the host's high risk score.
4. To get a clearer picture of the overall risk posture for this system, filter the **Risk Analysis** dashboard on the **risk_object** host 10.11.20.87 over the **Last 30 days**.
5. A visual analysis of the **Risk Modifiers Over Time** in your environment shows a large number of risk modifiers for this host from several weeks ago and a resurgence of risk modifiers over the past couple days. You decide to investigate this pattern on the **Incident Review** dashboard to see what types of notable events are being generated for this host.

### Investigate the threat risk of a high-risk host

Investigate past notable events associated with the high-risk host to further assess the risk to your environment.

1. Open **Incident Review** and search for the **src=10.11.20.87** over the **Last 30 Days** to see what types of notable events are associated with this high-risk host.
2. You see multiple notable events associated with this host that were created and closed in the past, but no new notable events.
3. Expand the event details for a notable event for **High or Critical Priority Host With Malware Detected**. This host is tagged as a high or critical asset in your environment, indicating that it could hold sensitive data or is used by administrators.

   1. Review the **History** and click **View all review activity for this Notable Event** to see what actions analysts took when the machine was infected.
   2. If necessary, review your ticketing system to determine which malware-remediation steps desktop support took at the time of infection.

4. Expand the event details for another notable event, **Threat Activity Detected**. You see a **Destination** domain of micros0ft[.]com, which seems suspiciously similar to Microsoft.com.

   1. You review the **Threat Description** and **Threat Group** to understand more about the domain and the threat it poses.
   2. Determine what others on the web are sharing about the domain.

   From the **Destination** field actions, select **Google micros0ft[.]com**. Review the search results for reputable sources discussing activity associated with the domain.

   3. Return to the notable event and investigate the whois records for the domain. From the **Destination** field actions, select **Domain Dossier**. Review the domain owner, registrar, and registration date for suspicious values.

5. Return to Splunk Enterprise Security to continue investigating the domain. Select **Security Intelligence > Web Intelligence > New Domain Analysis** and search for the micros0ft[.]com domain as a type of **Newly Seen**.

6. Based on the details you collect, because the domain is newly seen in your environment, the whois details indicate that it is newly registered, and threat activity is associated with the domain, you can conclude that the domain is likely malicious.

### Open an investigation to track your work

1. From the **Incident Review** dashboard, select the notable events that are relevant to your investigation and select **Add Selected to Investigation**.
2. Start a new investigation and name it **Malicious domain activity on host 10.11.20.87**.
3. Using the Investigation Bar, add your action history from the **Risk Analysis**, **Incident Review**, and **New Domain Activity** dashboards to the investigation from your Investigator Journal.
4. Add notes about the results of your Google search and **Domain Dossier** investigation steps, including links to relevant articles and a screenshot of
the whois record.

**Perform a forensic investigation on the host**

You determine that micros0ft[.]com is a malicious domain. Perform a forensic investigation on the host to identify the zero-day malware that evaded the endpoint detection software. A forensic investigation can include steps for finding malicious dropper programs, similar malware, and mentions of command and control servers embedded in the files. After the forensic investigation is complete, collect information about the malware that can be used to identify it in the future. Common criteria for identifying malware include queried IP addresses, domains, and MD5 file hashes of the malware files.

**Detect future threats from this zero day**

Set up Splunk Enterprise Security to detect threats related to this malicious compromise in the future. Add the malware file hash and IP addresses to an existing local threat source in Splunk Enterprise Security in order to detect compromised hosts.

1. On the Enterprise Security menu bar, select Configure > Content > Content Management.
2. Find the Local IP Intel lookup and click the name of the lookup to open it.
3. Type a description of "Potential zero day malware IP addresses."
4. Add the IP address indicators to the lookup. Right-click and select Insert Row Below to add new rows as needed.
5. (Optional) Type a numeric Weight to change the risk score for objects associated with indicators on this threat intelligence source.
6. Click Save.

Repeat these steps for the Local File Intel lookup to add the malware file hashes.

**Identify additional zero-day compromises**

Use the newly-added threat indicators to identify previous compromises related to this zero-day attack.

1. Open the Threat Activity dashboard.
2. Filter the dashboard to show only threats with a Threat Group of local_ip_intel or local_file_intel.
3. Choose a time range to search over and click Submit.
4. Review the results in the **Threat Activity Over Time** panel. Investigate threat results further in the **Threat Activity Details** panel.
5. Use the `threat_match_value` to identify which indicator of compromise is associated with the host.

Continue your investigation with the new host information, or look for additional hosts associated with more **Threat Group** sources that you created.

**Summary of zero-day investigation**

To identify zero-day malware activity, start by reviewing the high-risk hosts in your environment on the Risk Analysis dashboard. Review the past malware and threat activity associated with those hosts on the Incident Review dashboard and investigate suspicious domains with the field actions and the New Domain Analysis dashboard. Track your work in an investigation and perform a forensic investigation on the host to gather valuable file hashes and determine if the malware activity and suspicious domain are associated with a zero-day vulnerability. Finally, use the results of the forensic investigation to add intelligence to the Threat Intelligence framework in Splunk Enterprise Security and track down future and past compromises associated with this zero-day activity.