Executive Summary

LogicHub Threat Detection Playbook for Windows Process Creation Events

After an adversary has compromised a system in your network, they will move laterally—that is, stealthily exploring the network, discovering what systems and services you have in place, and searching for more vulnerabilities and assets to steal or compromise. As part of this lateral movement, they will run processes on Windows endpoints, and these processes will be logged in Windows process creation logs. Millions of these log events are likely already being generated and collected in the course of everyday operations. Unfortunately, the truly suspicious and malicious events may be missed in the noise of normal activity.

Developed from the MITRE ATT&CK Framework for threat detection, the LogicHub Playbook for Windows Process Creation Events is a LogicHub playbook that identifies suspicious and malicious PowerShell events as accurately as an experienced threat hunting team would but backed by automated analysis. The LogicHub Windows Process Creation playbook eliminates the need for teams to spend months developing and tuning detection content and provides a ready-to-use automated solution for threat detection.

The LogicHub Windows Process Creation playbook automates the analysis techniques that expert threat hunters previously had to perform manually, including:

- Identifying anomalous or known malicious process parent / child relationships
- Analyzing obfuscated PowerShell commands, factoring in hundreds of patterns
- Identifying adversary use of built in tools, aka "living off the land" techniques
- Triaging suspicious URLs, by retrieving and analyzing content
- Automatically filtering out noise in the environment
This playbook provides advanced analysis capabilities, machine learning classification, pattern matching built from libraries of hundreds of known attacks that can be readily deployed to your environment. This set of content can fill significant content gaps in your threat detection immediately, while reducing triage analysis time.

The playbook runs on the LogicHub SOAR+ Security Automation Platform, the only security automation platform that delivers autonomous detection and response for security operations teams. By applying machine learning and analytics on large data sets, LogicHub automates security analyst workflows and decisions, helping teams save time, find critical threats, and eliminate false positives. LogicHub also provides a full explanation of the scoring logic to help security analysts review and validate results.

**Background**

It's difficult for SOCs to find highly skilled detection and response experts. If you are fortunate enough to have these experts on your team, too often they’re too busy with other responsibilities to build large volumes of quality threat detection data.

The LogicHub Security Automation Platform has been used in many diverse environments to automate and exponentially improve the speed of alert triage, incident response, and threat hunting. We also provide workflows for high quality threat detection, shortcutting the need for months of laborious detection development and manual tuning leveraging the power of our unique platform.

LogicHub Threat Detection Playbook for Windows Process Creation Events is a playbook that applies automated analysis and advanced decision making technology analysis to identify suspicious and malicious events with the accuracy of an experienced threat hunting team.

The playbook runs on the LogicHub SOAR+ Security Automation Platform, the only security automation platform that delivers autonomous detection and response for security operations teams. By applying machine learning and analytics on large data sets, LogicHub automates security analyst workflows and decisions, helping teams save time, find critical threats, and eliminate false positives. LogicHub also provides a full explanation of the scoring logic to help security analysts review and validate results.

**The LogicHub Solution**

LogicHub has refined and automated hundreds of threat hunting detection patterns and techniques and mapped them to the MITRE ATT&CK framework, a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations and maintained by the MITRE Corporation.¹

¹ For more information about the MITRE ATT&CK Framework, see https://attack.mitre.org/.
Some major capabilities in the LogicHub playbook include:

- **Identify Malicious Process Chains**: By baselining your environment and recognizing patterns in thousands of known malicious examples, LogicHub can automatically identify anomalous and suspected malicious parent / child process relationships.

- **Automated PowerShell Command Triage**: The playbook de-obfuscates and analyzes PowerShell commands, factoring in hundreds of patterns and a machine learning classifier trained on your organization’s data.

- **“Living Off the Land” Attack Technique Similarity**: We have identified numerous patterns of attack techniques, drawing on the MITRE ATT&CK framework. We can find new attacks through fuzzy text similarity matching on thousands of known attack examples and by matching known patterns manually created by domain experts.

- **Cut Analyst Time with Automated Suspicious URL Triage**: Integration of a URL analysis engine allows LogicHub to automatically retrieve the content behind suspicious URLs, hash the downloaded files, and scan files with a custom set of YARA file analysis rules.²

- **Putting it all together**: Combining automatic false positive reduction with a composite risk-ranked view of threats from the various analysis and enrichment engines, we provide truly advanced threat detection capabilities, while acting as a force multiplier for your analysts.

### Analysis Capabilities

LogicHub consumes process execution logs from the environment and immediately begins building baselines of activity from several vantage points. The baselines are used to eliminate noise, automatically reduce false positives, and help with the identification of anomalies. Anomalies are present in all environments, which is why LogicHub has built in extensive capabilities to enrich events with additional context and libraries of patterns and pattern-matching engines to automate identification of security-relevant anomalies.

Below we provide more detail and examples of just some of the analysis techniques used in this threat detection playbook.

### Identify Malicious Process Chains

Initial compromise often begins with a malicious URL or file attachment. A common attack pattern today uses phishing emails that convince the victim to open a VBA macro-enabled Microsoft Office document.

² YARA is a multiplatform tool that helps malware researchers identify and classify malware samples. For more information, see http://virustotal.github.io/yara/
Automated PowerShell Command Triage

PowerShell has become an essential tool for attackers at all skill levels. Our solution automatically decodes and decompresses suspicious PowerShell commands to identify its true intention. This step saves your analysts time and can identify malicious commands by searching for nearly 200 techniques known to be used by attackers. In addition, the playbook applies a machine-learning classifier to automatically identify malicious patterns in the commands with high accuracy.

In the example below, we see that the commands passed to PowerShell were base64-encoded. The LogicHub processing engine identifies the encoded sequence and attempts iteratively to decode and decompress it.
Through decoding, we discover that the command is attempting to download a malicious executable from an IP address and execute it.

The playbook runs a pattern-matching algorithm across the decoded PowerShell command, identifies security-relevant actions the code is trying to perform, and assigns a risk score to each of the actions. In the example below, the tags on the rightmost column draw an analyst's eye to what was found in the PowerShell event after it was decoded. This detail can then be carried forward into an alert for added context.
Finally, the playbook can classify PowerShell code as benign or malicious using a custom machine-learning model trained using your organization’s own data. The model produces a confidence score for all output, providing guidance for your team about interpreting analytical results. We can see below that not only did the manual patterns recognize this as malicious PowerShell, but our model also flagged it with the highest confidence, 1.0.

<table>
<thead>
<tr>
<th>Process_Command_Line</th>
<th>lhub_predicted_label</th>
<th>lhub_confidence_score</th>
</tr>
</thead>
<tbody>
<tr>
<td>depth_0: powershell -noP -sta -k 1 -enc SQBmAGgAJABQbMAVgBFANIAcW6pAE8ATg BUAEEAYg8sADEAlgBOAFMAVg...</td>
<td>malicious</td>
<td>1.0</td>
</tr>
</tbody>
</table>

“Living Off the Land” Attack Technique Similarity

Living Off the Land binaries and scripts (LOLBAS) are built-in or commonly installed executables and capabilities that can be abused by adversaries to achieve their objectives. The LogicHub platform includes a text-similarity-matching capability, as well as a blazing fast pattern-matching engine to compare to hundreds of examples of known Living off the Land actions.

In the examples below, we identified a user in the discovery kill-chain phase enumerating domain administrators and then creating a backdoor local administrator account.
**Cut Analyst Time with Automated URL Triage**

Many times, as in the PowerShell example above, we’ll see attackers invoking tools to download additional payloads. As part of this threat detection playbook, we parse all URLs referenced in commands and analyze the domain or IP address against a historic baseline for rarity.

To definitively determine if an event is malicious, analysts often need to retrieve the suspect file and perform static analysis. The playbook automates many of these steps by retrieving suspicious files and computing the file hash for later automated lookup from sources like VirusTotal. The playbook also captures file metadata such as content type and file size, and scans that data with custom file pattern-matching YARA rules. This rule set is extensible and is used to automatically analyze specific files referenced at the command line for a closer look.

**Putting It All Together**

Each of the analysis capabilities described above provides context and enrichment about the millions of events in your environment. The playbook reduces the millions to dozens through statistical analysis, machine learning, application of large knowledge repositories of malicious activity patterns, and a scoring scheme that considers all of these factors. The result is a composite view that can put events considered to be noise through a lens to accurately identify true malicious activity.
Below we show an example of an alert that could be output back to an analyst for additional investigation. In this example, note that the final alert flagged the execution of a command to create a local administrator account. The playbook provides a link to the associated technique in the MITRE ATT&CK framework for more information. In addition to the Expert Knowledge patterns detecting this activity, the text-similarity engine also identified this as being 86% similar to a known discovery command and included that additional context.

**Conclusion**

It typically takes months or longer and lots of work for a security team to build reliable and relevant threat detection content. The LogicHub Windows Events Creation playbook provides advanced analysis capabilities, machine-learning classification, and pattern matching built from libraries of hundreds of known attacks that can be readily deployed to your environment. This content will hone your threat detection activities, while reducing the time required for triage analysis.

For more information about this playbook or the overall features of the LogicHub SOAR+ Security Automation Platform, visit www.logichub.com.