Monitoring for signs of Windows privilege escalation attack

Scenario: You work for a government agency that, for security reasons, maintains tight controls over access to certain systems. The CISO is concerned about privilege escalation in which an adversary gains an initial foothold on a host and then exploits its weaknesses to increase their privileges. By increasing their privilege level, the attacker can gain the control required to carry out malicious ends. As a security analyst, you need to recommend a series of searches that will help prevent such attacks in the agency. The Splunk Security Research team developed this use case to help you detect and investigate behaviors that attackers may use to elevate their privileges in your environment.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: security analyst, threat hunter
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data: Data normalized to the following CIM models:
  - Authentication
  - Endpoint

How to use Splunk software for this use case

You can run many searches with Splunk software to monitor for signs of Windows privilege escalation attacks. Depending on what information you have available, you might find it useful to run some or all of the following:

- Child processes of Spoolsv.exe
- Windows accessibility binary modifications
- Registry keys used for privilege escalation
- Uncommon processes on endpoint

If you identify suspicious behavior, you can investigate further using these searches:

- Authentication logs for an endpoint
- Processes running on a host
- Registry activities
- Web activity to and from a host
Results

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Creating a golden image of common processes run by your organization
- Actively monitoring the registry changes happening across machines
- Quickly investigating anomalous processes using SOAR tools, if possible, to scale

Measuring impact and benefit is critical to assessing the value of security operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Number of unlikely processes and users making registry changes: A high number is an indicator of anomalous behavior that might be related to privilege escalation
- Number of hosts with uncommon processes in your organization: A high number might be an indicator of privilege escalation

Additional resources

If you have questions about this use case, see the Security Research team’s support options on GitHub. In addition, these Splunk resources might help you understand and implement this use case:

- Conf Talk: Real world cases of insider threat
- Blog: Spotting the signs of lateral movement
- Blog: Get more flexibility and accelerated searches with the new endpoint data model

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.