Recognizing improper use of system administration tools

Scenario: System administrators in your organization sometimes use tools like PsExec and DCOM to manage systems remotely. However, because your entire organization recently began working from home, you have more concerns around the security of these tools. You want to investigate usage of these tools to make sure that bad actors aren't using them to move laterally within your network. You can use Splunk software to examine Windows security logs for unusual authentication events and then investigate events taken by those logged-in users.

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: System log data
  - Data normalized to the following CIM models:
    - Endpoint

How to use Splunk software for this use case

You can run many investigations with Splunk software to detect suspicious lateral movement with legitimate sysadmin tools. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Remote logins to a host
- Process creation events
- User account changed
- Registry activities
- Registry keys used for privilege escalation
- Sc.exe manipulating Windows services

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:

- Developing and maintaining authentication baselines for users
• Eliminating outdated or unpatched systems in your environment
• Enforcing least-privileged user policies to limit access to systems and resources
• Enforcing robust password management policies and multi-factor authentication

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:

• Time to detection: The time between when an adversary gained access to your network to when you detected their presence
• Lateral movement blocked: Number of times an adversary was unsuccessful at gaining access to systems through lateral movement

Additional resources

The content in this use case comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. These additional Splunk resources might help you understand and implement this specific use case:

• Conf Talk: Identify lateral movement and malicious backdoors with WMI
• Blog: Great (Endpoint) moments with Mr. Lincoln
• Blog: Peeping through Windows (Logs)
• Blog: ATT&CK-ing the adversary