Detecting lateral movement with Active Directory data

Scenario: An advanced adversary trojanized a legitimate dynamically linked library (dll) in your organization's software and fed that into your customers’ update cycle. Once infected, this trojanized backdoor allowed the adversary to move laterally in a victim’s network and steal their critical data. This attack was perpetrated by an advanced adversary who carefully selected targets, changed their attacking infrastructure to match geographical location, and even named attacking hosts to match their victims to disguise their traffic better. By using a trusted software partner, they spread laterally across on-prem and cloud infrastructures to capture and exfiltrate data. You need to do some damage control to your company's reputation, so you decide to help your customers by creating Splunk searches they can use on their Active Directory data to help with incident response. You can use Splunk software to find hosts where the adversary was able to gain a foothold or search for indicators of compromise related to specific lateral movement attacks. You can also use Splunk to analyze your Azure Active Directory data to hunt for techniques used in lateral movement, such as captured administrative passwords and forged SAML tokens.

Prerequisites

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

- People: Threat hunter
- Technologies:
  - Splunk Enterprise or Splunk Cloud Platform
  - Microsoft Azure Active Directory audit data
  - Microsoft Azure Add-on for Splunk
  - Splunk Machine Learning Toolkit
- Data:
  - DNS data
  - Microsoft Office 365

How to use Splunk software for this use case

You can run many searches with Splunk software to detect lateral movement with Active Directory data. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Newly added Active Directory service principals
- Newly added Active Directory credentials
- New application permissions granted through Active Directory
• Application switch to Active Directory multi-tenant access
• Changes to Active Directory custom domains
• Azure Active Directory audit events

The following are some additional searches that you might find useful in detecting lateral movement outside Active Directory data:

• Sc.exe manipulating Windows services
• First time seen Windows service
• Signs of beaconing activity
• DNS queries to randomized subdomains

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:

• Using external resources to inform yourself about the attack and possible ways to mitigate it, such as hunting for named pipes.
• Using domain lookup files for specific threats, such as Sunburst Backdoor, to find hosts that have communicated with indicators of compromise.
• Importing intelligence files for specific threats, such as Sunburst Backdoor, into your Splunk Enterprise Security application to facilitate your searches.
• Reviewing external to internal network traffic to determine if unknown IP addresses have accessed your systems

Measuring impact and benefit is critical to assessing the value of security operations. When implementing this use case, you might want to track how many of the following Active Directory objects and properties you identified that couldn't be associated with legitimate activity:

• New service principals
• New credentials
• New permissions, role assignments, or tenant access
• Custom domain changes

Additional resources

These additional Splunk resources might help you understand and implement this use case:

• Blog: Using Splunk to detect Sunburst Backdoor
• Blog: How do I add threat intelligence from the internet to Splunk Enterprise Security?
• Blog: Smoothing the bumps of onboarding threat indicators into Splunk Enterprise Security
• PDF: Splunk Security Essentials analytic stories for Sunburst Backdoor detections

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.
• App: Splunk Security Essentials
• Tech Talk: Detect SolarWinds cyber attack with Splunk Enterprise Security