Detecting a ransomware attack

This article covers techniques for detecting ransomware attacks. If you have already detected an attack and want to investigate its impact, check Investigating a ransomware attack for searches to help you investigate the origin and scope the impact of the attack.

Scenario: A new type of ransomware attack has been discovered and is affecting organizations like yours. Although you have not yet been contacted by any users letting you know their machine has been infected, you know that attackers can infiltrate a network and perform activities undetected before encrypting files and notifying users. As a security analyst, it is your goal to detect traces of ransomware attacks by investigating programs or binaries that execute on potentially infected systems, and looking for other hallmarks of ransomware attacks.

Prerequisites

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

- **People:** Security analyst
- **Technologies:**
  - Splunk Enterprise or Splunk Cloud Platform
- **Data:**
  - System log data
  - Antivirus data
  - Deep packet inspection data

How to use Splunk software for this use case

There are many searches you can run with Splunk software in the event of a ransomware attack. You can detect the attack using these searches:

- High file deletion frequency
- High process termination frequency
- Bulk creation of ransomware notes
- Bcdedit boot recovery modifications
- Shadow copies deleted
- Registry key modifications
- Wmic.exe launching processes on a remote system
- Schtasks.exe used to force a reboot

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.
• Schtasks.exe registering binaries or scripts to run from a public directory
• Server Message Block (SMB) traffic connection spikes
• File write spikes
• Wevtutil.exe abuse
• Command line string length
• USN journal deletion
• Wbadmin delete backup files
• Windows event log cleared

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:

• Notifying law enforcement and all other authorities relevant to your industry
• Implementing your security incident response and business continuity plan
• Filing cyber insurance claims with your provider

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 from when the source of the ransomware was downloaded to the user’s machine and when the user received the ransomware notice
• Time to complete the investigation: The time from when the user reported the ransomware to when the investigation was completed

Additional resources

The content in this use case comes from a hands-on security investigations workshop developed by Splunk experts. To find out what educational resources are available to you, talk to your Customer Service Manager. These additional Splunk resources might help you understand and implement this specific use case:

• Use case: Detecting Clop ransomware
• Use case: Investigating ransomware attacks
• E-book: Ransomware, malware and cyberthreats
• Webinar: Detection of ransomware and prevention strategies
• Blog: Operationalize ransomware detections quickly and easily with Splunk