Reconstructing a website defacement

Scenario: Potential and existing customers navigate to your company’s website one day, hoping to find the user-friendly and carefully branded homepage that your web design team worked so hard on. Instead, they are greeted with cat photos. The CEO is irate and everyone is in a panic. As a security analyst, your role is to investigate what happened, and reconstruct the steps the attacker took so that your organization can put measures in place to prevent a similar attack in the future. You can use Splunk software to identify artifacts and indicators of the defacement. Those indicators allow you to make decisions regarding containment and recovery, as well as to defend against future 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
  - Splunk Stream
  - Microsoft: Sysmon
- Data:
  - Web server data
  - Firewall data
  - DNS data

How to use Splunk software for this use case

You can run many searches with Splunk software to reconstruct a website defacement. You can investigate the origin of the attack using these searches:

- IP address sending repeated requests to a web server
- Product or software accessing web server
- Web requests to a specific system in your environment
- IP address attempting a brute force password attack
- Executable uploaded to a web server
- MD5 hash of an uploaded file
- Web server initiating outbound traffic
- FQDN associated with an IP address
You can scope the impact of the attack using this search:

- **Time elapsed between two related events**

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:

- Taking the web server offline
- Posting a temporary maintenance page
- Restoring the web server

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 defacement occurred to the time it was reported to the company
- Time to complete the investigation: The time from when the defacement was reported to the company 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:

- Blog: [I Have a Fever, and the Only Cure for It Is More Feedback](#)