Detecting techniques in the Orangeworm attack group

Scenario: You work in a hospital that uses outdated and insecure technology. Despite how vocal you’ve been about the need to upgrade, your hospital uses older operating systems and often neglects to patch computers. You are concerned about the attack group Orangeworm stealing patient information to sell on the black market or to engage in corporate espionage. You are also concerned that the group will infect your network computers and use malware to control medical devices, such as MRI and X-ray machines. The Splunk Security Research team developed this use case to help you detect a number of the associated techniques, such as use of command-line arguments and of sc.exe, a non-essential Windows file that can manipulate Windows services. It also helps you get more information on web hosts that you suspect have been compromised.

Prerequisites

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

- People: Security analyst, threat hunter, or security tools engineer
- Technologies:
  - Splunk Enterprise or Splunk Cloud Platform
  - Splunk Add-on for Microsoft Windows
- Data normalized to the following CIM models:
  - Authentication
  - Endpoint
  - Web

How to use Splunk software for this use case

You can run many searches with Splunk software to help with a potential Orangeworm attack. Depending on what information you have available, you’ll likely first want to run the following baseline searches:

- Previously seen command line argument
- Previously seen Windows service

After you have established baselines, you can run the following detection searches:

- First time seen command line argument
- First time seen Windows service
- Sc.exe manipulating Windows services
Finally, you can then investigate the triggered detection using these searches:

- Authentication logs for an endpoint
- Processes running on a host
- 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:

- Ingesting command-line arguments from endpoint detection and response (EDR) technologies
- Having an incident response template or automation setup for quarantining a machine as quickly as possible to avoid lateral movement

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:

- Changes in execution patterns: In a typical environment, most endpoint processes listed do not change their execution pattern. While assessing the results of these detections, the analysts should investigate the parent process that originated the execution.
- Unseen processes: Parent processes like Word.exe, Powerpoint.exe, or a process completely unseen before are the usual indicators of malicious activity.

---

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: How we built an efficient healthcare privacy monitoring platform

---