Monitoring employee network traffic

Scenario: The internet use policy at your organization doesn't block any websites. Your CEO prefers to treat employees like responsible adults. Nevertheless, you are concerned about employees accidentally accessing malicious websites that can damage your network. You want to monitor internet usage for traffic to new domains on the hypothesis that never-before-seen domains are the ones most likely to pose a threat. You are concerned about attacker-controlled domains that are hubs for command and control communications and for data exfiltration. You can use Splunk software to establish baselines and lookup tables of the domains typically accessed by your network users. You can then construct searches to compare daily usage against those baselines and alerts to notify you of anomalies.

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
  - URL Toolbox
  - URL Parser
- Data:
  - DNS data
  - Proxy data
  - Firewall data

How to use Splunk software for this use case

You can run many searches with Splunk software to monitor for connections to new domains. Depending on what information you have available, you might find it useful to identify some or all of the following:

- New domains accessed by network users
- Baseline of domains accessed by network users
- Typosquatting clicks on a network
- Algorithmically generated domain names
- DNS tunneling through randomized subdomains
- Uncommon top level domains
- DNS queries to randomized subdomains
- HTTP GET requests
The following procedures can also help you achieve the results you want with your data:

- **String conversion to a common format**

---

### 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:

- Establishing internet usage policies
- Configuring firewalls
- Creating blocklists and allowlists

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:

- Malicious domains identified: The number of domains alerted on that posed a threat

---

### 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: [Real-time asset discovery and identity attribution using Splunk](#)
- Blog: [Detecting dynamic DNS domains in Splunk](#)
- Blog: [UT Parsing Domains Like House Slytherin](#)
- White paper: [Operationalize machine learning to find malicious domains](#)