Detecting the use of randomization in cyberattacks

Lately, your network users have fallen victim to a large number of phishing attacks. The victims you interviewed said that the emails looked legitimate and didn't have the usual typos or unnatural sounding English phrases that generally allow them to easily identify phishing scams. The office of the CISO wants to put together a training on how attackers manipulate domain names to fool users. Your manager wants to know what suspicious domains or subdomains were accessed in order to determine if further investigation or action is needed to protect your network. You need to come up with a list of domains for these internal clients. You can use Splunk software to calculate the randomness of domains accessed on your network and how closely related they are to legitimate domain names. You can efficiently extract domains, subdomains, and file paths that have a low probability of being false positives.

Required data

- DNS data
- System log data
- Web server data
- Antivirus data

How to use Splunk software for this use case

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

- Typosquatting clicks on a network
- Algorithmically generated domain names
- DNS tunneling through randomized subdomains
- Processes launched from randomized file paths
- DNS queries to randomized subdomains

Next steps

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:

- Creating allowlists and blocklists to use as lookups in Splunk
- User network security education and awareness campaigns
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:

- Successful phishing attacks in your network: The ratio of successful attempts to overall attempts
- Blocked queries: The number of failed network traffic attempts as result of blocklists created from the data in this use case

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:

- Blog: UT_parsing domains like House Slytherin
- Blog: Detecting typosquatting, phishing, and corporate espionage with enterprise security content update
- Blog: When entropy meets Shannon
- Blog: Random words on entropy and DNS