Artifacts We Need to Collect

Artifacts are specific pieces of information we need to retrieve from emails that allow us to conduct further searches, share intelligence with other organizations, and take defensive measures. Below we have listed the artifacts that are deemed important to phishing investigations – you'll need to remember these when it comes to the BTL1 exam!

EMAIL ARTIFACTS

Sending Email Address

This is where the email has come from, or appeared to come from. During the Tactics and Techniques section, we covered spoofing, and how malicious actors can alter what the sending address looks like to make it appear legitimate. Regardless of whether this has obviously been spoofed, we need to record the email address that has apparently sent the email. We can use this as a search term in email gateway security products to identify any other emails that have come from, or been sent to that address.

Subject Line

The subject line is a very useful artifact for both searching for other associated emails by using it as a search term in our email gateway security product, or for blocking incoming emails that are in the same attack and using the same subject line.

Recipient Email Addresses

We need to identify which mailboxes have received this same phishing email, so we can inform them not to interact with it. Usually, the malicious actor will enter the recipients into the Blind Carbon Copy (BCC) field, so that recipients can't see who else the email was sent to. To identify recipients we would typically check our email gateway, and search for emails coming from the sending address and includes the subject line we have observed, which will give us a list of any other mailboxes that received the same email.

Sending Server IP & Reverse DNS

We need to know the address of the server that has sent the email, as this will help us to identify if the sending address has been spoofed. Once we have collected the IP we can perform a reverse DNS search on it using online tools such as Reverse IP Lookup by MXToolbox, which will provide us with a hostname that should give us some more information about the server.

Reply-To Address

This is the email address that will receive any replies to the original email. In some cases, this value will be different than the sending address, as if an attacker has successfully spoofed "support@amazon.com" any replies would go to that address, which the attacker won't have access to. Instead, they can insert an email address of an attacker-controlled account, so now replies will go to "flamingo91591@outlook.com".

Date & Time

It's good practice to record the date and time an email was sent. Searching for a period of time either side of the observed time could allow for other emails to be identified that are a part of the same attack or campaign. This can also be used as a metric to see at what times the organization receives the most malicious emails.

FILE ARTIFACTS

Attachment Name

The attachment name is a useful artifact when it comes to defensive measures, as depending on the uniqueness of the name, it can possibly be blocked using an organization's Endpoint Detection and Response (EDR) platform, using the filename as an indicator of compromise. This should always include the file name and file extension.

SHA256 Hash Value

A hash, the unique string generated from a file, needs to be recorded as it represents the file in its entirety, and can be used for reputation checks using online tools such as VirusTotal and Talos File Reputation. MD5 and SHA1 hashes should no longer be used, as they have known hash collisions, so SHA256 is the current security standard for file hashing.

WEB ARTIFACTS

Full URLs

It's important that when investigating a phishing email that contains a URL that it is copied properly, and not written out by hand, as this can lead to mistakes which will impact the investigation during the analysis stage. The URL should be copied either from the email client by right-clicking the hyperlink and selecting "Copy Link Destination", or by copying it from a text editor.

Root Domain

Whilst this artifact isn't necessary if you have the full URL, sometimes the root domain can be an important artifact, as it can help show if the site has been created for malicious activity, or if it is a legitimate site that has been compromised.

Previous Topic
Back to Lesson
Next Topic