Following the Trail of a Spear Phishing Campaign

Industry: Oil and Gas

Attacker Objective

Steal credentials

Background

A multi-billion dollar oil and gas company identified a phishing campaign that targeted 80 people within the organization, and learned that nearly half of them clicked a link in the deceptive email.

The security team was first alerted to this attack by a user who called the help desk to report the suspicious email. After receiving that call, Arista NDR enabled a swift and efficient response that would have taken days to accomplish for analysts using traditional tools.

Arista NDR detected this threat by:

- Identifying in seconds, the 35 users who clicked on the phishing link as well as the subset that gave up their credentials
- Highlighting the fake Microsoft SharePoint login site that was used to harvest credentials.
- Identifying all the devices the victims were using and the different IP addresses those devices had used throughout the time period in question.

Why Arista NDR?

The company is now using Arista NDR to identify any device using any protocol to visit any domain/IP with TTPs of these attackers. This means that the company does not need to know the list of domains the attacker has registered in the past or will register in the future, nor the IPs they use. They'll simply be alerted if any of those TTPs are seen again.

While a detailed investigation like this could typically take days, it was completed in minutes with Arista NDR. And ultimately, Arista NDR turned intelligence generated during the investigation into actionable protection for the organization.

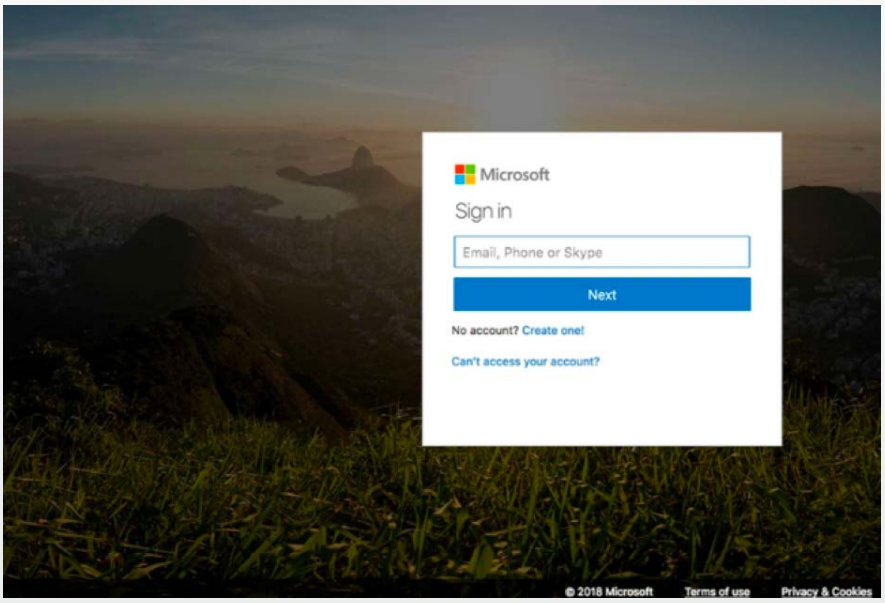

Figure 1: After clicking on a link, users were directed to this page which looked like a Microsoft SharePoint login but was harvesting credentials and sending them to the attacker.

```
<?php
$userid = $_POST['userid'];
?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>&#83;&#105;&#103;&#110;&#32;&#73;&#110; to your account</title>
<script type="text/javascript" src="https://www.sitepoint.com/examples/password/MaskedPassword/MaskedPassword.js"></script>
```

Figure 2: The look-alike Microsoft SharePoint login page had an embedded password-stealing script.

The Arista NDR platform identified an interesting traffic pattern wherein those devices that interacted with the attacker domain subsequently visited a known good domain. The good domain turned out to be providing JavaScript used to mask the password being typed into the browser to make the site look like a legitimate SharePoint login. However, this exposed the tactics, techniques and procedures (TTPs) being used by the attacker and enabled the security team to identify which users had revealed their usernames and passwords.

Further examination of the attack artifacts revealed an email address where credentials were being sent. This email address was used to identify other domains that share the same attributes such as how and when the domain was registered, where it was hosted, etc.

Most phishing investigations would stop at simply blocking the sender and the bad domain, making it very simple for an attacker to try again. But by enabling the analyst to pivot in one click to other associated domains, Arista NDR helped expose the entire attacker infrastructure.