Blue Team Level 1 Certification (Standard)

~~Management Principles~~

4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

✓ ~~PA1) Introduction to Emails and Phishing~~

7 Topics | 1 Quiz

✓ ~~PA2) Types of Phishing Emails~~

10 Topics | 2 Quizzes

✓ ~~PA3) Tactics and Techniques Used~~

12 Topics | 2 Quizzes

✓ ~~Section Introduction, Tactics and Techniques~~

✓ ~~Spear Phishing~~

✓ ~~Impersonation~~

✓ ~~Typosquatting and Homographs~~

✓ ~~Sender Spoofing~~

✓ ~~HTML Styling~~

✓ ~~Attachments~~

✓ ~~Hyperlinks~~

✓ ~~URL Shortening Services~~

✓ ~~Use of Legitimate Services~~

✓ ~~Business Email Compromise~~

✓ ~~[Video] Tactics and Techniques & Examples~~

~~Activity) Reporting on Tactics Used~~

~~Activity) End of Section Review, Tactics and Techniques~~

✓ ~~PA4) Investigating a Phishing Email~~

8 Topics | 2 Quizzes

✓ ~~PA5) Analysing URLs, Attachments, and Artifacts~~

8 Topics | 1 Quiz

PA6) Taking Defensive Actions

12 Topics | 1 Quiz

○ PA7) Report Writing

7 Topics | 1 Quiz

○ PA8) Phishing Response Challenge

3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence

7 Topics

○ TI2) Threat Actors & APTs

6 Topics | 2 Quizzes

○ TI3) Operational Threat Intelligence

7 Topics | 1 Quiz

○ TI4) Tactical Threat Intelligence

7 Topics | 1 Quiz

○ TI5) Strategic Threat Intelligence

5 Topics | 1 Quiz

○ TI6) Malware and Global Campaigns

6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics

Use of Legitimate Services

Blue Team Level 1 Certification (Standard) > PA3) Tactics and Techniques Used > Use of Legitimate... COMPLETE

In this lesson we will cover how attackers can utilize legitimate services to conduct phishing campaigns, and why this can often be a very effective tactic, working to avoid defenses put in place by security teams.

EMAIL DELIVERY

Phishers will make use of legitimate services such as free email providers, to bypass defensive measures that can be implemented by defenders. Whilst we will go into detail about email blocking in the Defensive Measures section of this domain, organizations will typically not block webmail domains, such as:

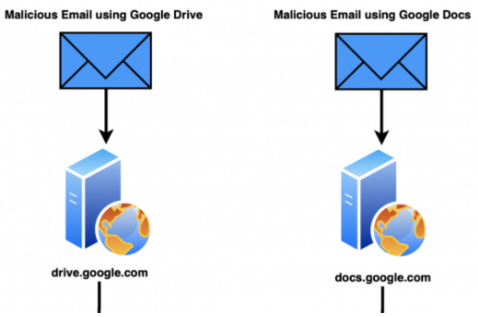
- **@gmail.com**
- **@outlook.com**
- **@hotmail.co.uk**

This is because, whilst a good amount of phishing emails will come from these domains (because anyone can create a free account and send mail), employees will likely use these domains to send messages to, or receive them from the organization's domain with out-of-hours queries such as contact with HR for on-boarding or off-boarding, payroll queries, or communicating with customers.

This can happen with malicious actors taking advantage of email marketing services that allow emails to be sent to huge audiences, such as MailGun and MailChimp. This can be an effective tactic as organizations will typically not block the sending IP addresses of email marketing companies as the organization will likely receive legitimate emails from these services.

FILE HOSTING

Malicious actors can also host malicious files, typically Microsoft Office Word and Excel documents with malicious macros, on free platforms such as Dropbox, One Drive, and Google Drive, and then send links to download these files in phishing emails. Anyone can register for these services in a matter of minutes, and including a hyperlink in an email to a domain that people recognize is likely to be much more effective than a domain that no one has heard of before. Let's look at an example below.


Malicious Email using Google Drive
drive.google.com
Malicious Email using Google Docs
docs.google.com

● 5 Topics

○ DF2) Forensics Fundamentals

● 10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection

● 8 Topics | 1 Quiz

○ DF4) Windows Investigations

● 3 Topics | 3 Quizzes

○ DF5) Linux Investigations

● 4 Topics | 2 Quizzes

○ DF6) Volatility

● 3 Topics | 1 Quiz

○ DF7) Autopsy

● 4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ SI1) Introduction to SIEM

Microsoft Office document with malicious macros
Google Docs files with URL lures to malicious domains

Google Drive and Google Docs have security controls in place, so attackers can't simply upload blatantly malicious scripts or executable files (.exe). Utilizing Google Drive, attackers can upload Microsoft Word or other documents that include malicious macros that will download malicious software to the system. With Google Docs a typical technique is to create a styled document that contains a hyperlink to a malicious page, instead of including it in the original email which can be easily detected by email security controls.

Previous Topic

Back to Lesson

Next Topic