

**Blue Team Level 1 Certification
(Standard)****Introduction to BTL1** Welcome to Blue Team Level 1!

4 Topics

 Lab and Forum Access**SECURITY FUNDAMENTALS DOMAIN** Introduction to Security Fundamentals

1 Topic

 Soft Skills

7 Topics

 Security Controls

5 Topics 1 Quiz

 Networking 101

6 Topics 1 Quiz

 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

 Section Introduction: Phishing Emails Reconnaissance Spam False Positives Credential Harvester Social Engineering Vishing, Smishing Whaling Malicious Files [Video] Types of Phishing Attacks & Examples Lab) Categorizing Phishing Emails Activity) End of Section Review: Phishing Emails PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

 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

Malicious Files

Blue Team Level 1 Certification (Standard) > PA2) Types of Phishing Emails > Malicious Files

COMPLETE



Along with credential harvesters, emails that convince targets to open malicious files are the most common phishing email classifications. This lesson will cover how malicious actors can get recipients to open malicious files, and what these can include. There are two main methods of delivering malware via phishing, as an attachment, or as a hyperlink taking the target to a web server that is hosting malware available for download.

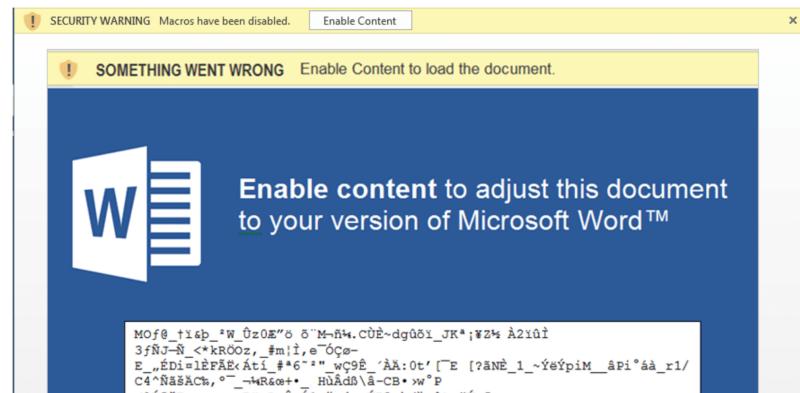
MALICIOUS ATTACHMENTS

It's not as easy as spamming random email addresses with your latest malware .exe file. Not only will most email providers prohibit sending attachments with certain file types, they can also perform basic attachment scans that can identify malware, and prevent you from sending it. If you received an email from a random address with a .vbs file, would you open it? The chances are that you don't deal with .vbs files, and because it's unexpected you'd immediately be cautious.

But what if someone sent you a Microsoft Office document, such as a Word or Excel document – these files are used daily within organisations, and receiving these would be less immediately suspicious. These files can't be malware right? They can – kinda.

Microsoft Office Macros

MS Office documents such as Word and Excel offer the ability to include macros. These are a series of commands and instructions that can be run automatically once enabled. Macro malware was fairly common several years ago because macros ran automatically when a document was opened. However, in recent versions of Microsoft Office, macros are disabled by default. This means malware authors need to convince users to enable macros so their malware can execute. They do this by showing fake warnings when a malicious document is opened.



The above screenshot shows an example of a malicious Microsoft Word document. At the top we have the legitimate ribbon, where users can click "Enable Content" to unlock the document, allowing macros to run automatically. Everything below this ribbon is fake, and has been crafted by the malicious actor, including the second ribbon titled "SOMETHING WENT WRONG". The attack is trying to convince the recipient that this

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 | 2 Quizzes

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

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

7 Topics | 1 Quiz

SI2) Logging

6 Topics | 2 Quizzes

SI3) Aggregation

2 Topics | 1 Quiz

SI4) Correlation

6 Topics | 1 Quiz

SI5) Using Splunk

5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics | 1 Quiz

IR2) Preparation Phase

10 Topics | 3 Quizzes

IR3) Detection and Analysis Phase

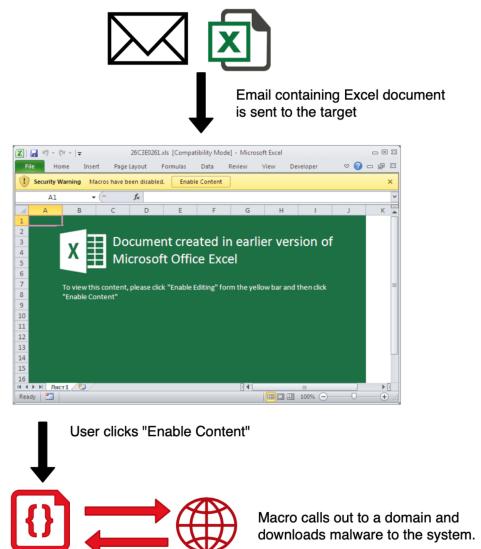
7 Topics | 5 Quizzes

IR4) Containment, Eradication, and Recovery Phase

5 Topics | 1 Quiz

SECOND PHASE ATTACK - SOMETHING VERY WRONG! THE ATTACKER IS TRYING TO CONVINCE THE RECIPIENT THAT THIS DOCUMENT IS AN OLDER VERSION, AND THAT THEY NEED TO CONVERT IT TO THE LATEST VERSION TO RUN PROPERLY.

Once run, these macros can connect to domains on the internet and download malware directly to the system. This can range from viruses to trojans, ransomware to rootkits.



It is crucial that appropriate defensive measures are taken and users are trained to spot and respond to suspicious emails. Microsoft have published some good suggestions for defending against macro malware:

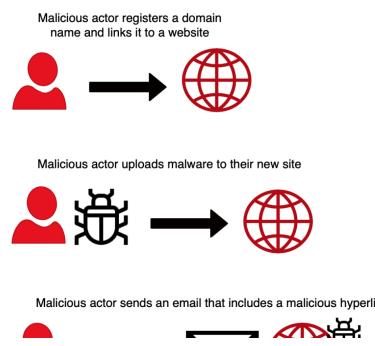
- Make sure macros are disabled in your Microsoft Office applications. In enterprises, IT admins set the default setting for macros: [Enable or disable macros](#) in Office documents
- Don't open suspicious emails or suspicious attachments.
- Delete any emails from unknown people or with suspicious content. Spam emails are the main way macro malware spreads.
- Enterprises can prevent macro malware from running executable content using [ASR rules](#).

HOSTED MALWARE

The other primarily delivery method of malware is by hosting it on websites, and convincing users to click on a hyperlink, download a file, and then run it. It's very similar to macro malware, but users need to manually visit and download the malware themselves.

Malicious Domains

Domains can be created by anyone in a matter of minutes, and for as cheap as the price of a coffee. It's no surprise that SC Magazine reported in August 2019 that 200,000 new domains are registered a day, and "70 percent of these are malicious or suspicious and used for a wide range of nefarious activities". That's 140,000 malicious domains a day. Then all the attacker needs to do is host a malicious file on a URL, and include it in phishing emails.



IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

13 Topics | 2 Quizzes

BTL1 EXAM

Exam Preparation

Using RDP and SSH

How to Start Your Exam



Recipient opens the email, clicks the link, and downloads the malicious file



Compromised Domains

Legitimate sites can be compromised by attackers, and then used to host malware. Often the legitimate site is left completely intact so that the site owner and visitors don't realise their site has been hacked and is being utilised for malicious purposes. A hyperlink to the malicious URL hosting the malware is then distributed in phishing emails.

Malicious actor attacks a legitimate domain and gains access



Malicious actor uploads malware to the compromised site



Malicious actor sends an email that includes a malicious hyperlink



Recipient opens the email, clicks the link, and downloads the malicious file



[Previous Topic](#)

[Back to Lesson](#)

[Next Topic](#)

[Privacy & Cookies Policy](#)

