T.I

OPERATION CHIMERA

CYBER THREAT INTELLIGENCE MODULE // SECURITY BLUE TEAM

CONTENTS

This information has been gathered from public sources and combined with my own knowledge and experiences for the purpose of Operation Chimera, an online, live blue-team training operation conducted by myself under the alias Known Divide, for the SecurityBlueTeam community. **Follow me on Twitter please!** https://twitter.com/knowndivide

Useful Links:

[1] https://www.forcepoint.com/cyber-edu/threat-intelligence
[2] https://www.crowdstrike.com/epp-101/threat-intelligence/
[3] https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

Sources:

[1] https://www.forcepoint.com/cyber-edu/threat-intelligence
[2] https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

If you've enjoyed this event, please consider donating whatever you can spare to buy me pizza, coffee, and help fund future events! (even £5/$5 will make a huge difference, and it only takes a few seconds).

PayPal.Me

https://paypal.me/KDMentoring

Donating £10 or more will earn you SBT VIP status for 30 days!
https://securityblue.team/get-vip/

OPERATION CHIMERA – THREAT INTELLIGENCE

This document is not 100% finished and will be updated within the next 24 hours. Thank you for your patience.

This module is designed to give a look into the world of Cyber Threat Intelligence. It is aimed at individuals who are moving in to Cyber, so the material is aimed at an entry-level student. We strongly encourage further reading using the provided sources and any that you find yourself. Want to talk to other hackers about this specific module? Join the discussion in the "threat-intel-module" channel within the "Operation Chimera" category on the SBT Discord server. There is also a Chimera mega-thread on Reddit. Please make use of this to ask questions and talk to other participants!

WHAT IS THREAT INTELLIGENCE?

"Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently targeting the organization."[1] Threat Hunting is also closely associated with Threat Intelligence, as hunting is the process of using intelligence to search for evidence of sophisticated threat actors, who are already in the network.

WHAT SKILLS ARE REQUIRED?

- **Research:** You'll always be on the lookout for new information about Threat Actors, malicious campaigns, or security developments. You'll develop your list of sources over time and know where to look for quality information. Knowledge of how the Dark-web works and can be accessed is also beneficial, as threat actors usually communicate via underground channels.

- **Communication:** You'll need to be able to communicate to a wide range of people, both internally and externally of the business. Internally, you'll provide input to security awareness training, and need to be able to explain concepts to non-technical audiences, all the way from the Finance Department to the Executive Board. Externally you'll likely collaborate with government departments, information sharing partnerships, other organizations, and intelligence vendors.

WHY IS IT USEFUL?

By identifying relevant threat actors, and consuming intelligence from a number of sources, a Threat Intelligence function can help the business better understand risks from cyber-attacks. In short, it helps security teams focus on attackers that are likely to target the organization, and work to develop defences and other measures to prevent or limit the impact of attacks.
Threat Actors have the skills, knowledge, and resources to bypass most conventional network defences. This is why it's important to keep up to date with their tactics, and develop unique solutions to stop them, or at least detect them.

INDICATORS OF COMPROMISE

Indicators of Compromise are a crucial part of Cyber Threat Intelligence. But what are they? And why are they useful?
IOCs are artifacts that have been identified as acting maliciously or attributed to malicious actors. Some of the most common ones include:

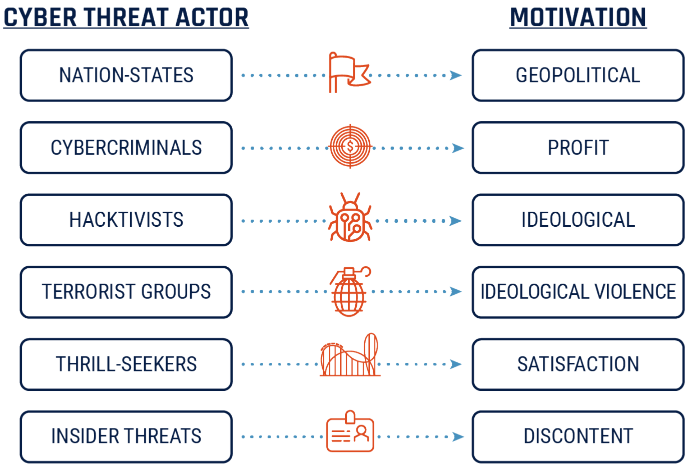
- **IP Addresses** (Ex: An IP that has been observed scanning for vulnerabilities over the Internet)
- **Domains** (Ex: A domain that hosts a credential harvesting site)
- **Email Addresses** (Ex: An email address that has been sending phishing emails with a malicious attachment)
- **File Hashes** (Ex: The unique hash of a piece of malware used by sophisticated hackers)

When IOCs are seen and recorded, these are usually shared with other organizations, so that they can check for exposure, and take measures to ensure that they are protected from them in the future. By doing so, Defenders can keep up with malicious campaigns, and work to protect themselves and others from cyber-attacks. Some companies profit from this by having their own researchers, which collect intelligence, and offer it exclusively to their customers.

ADVANCED PERSISTENT THREATS

An advanced persistent threat (APT) is a pro-longed cyber-attack carried out by a highly sophisticated actor or group that have the knowledge and resources to conduct complex cyber operations. These attacks go undetected for a long period of time, whilst the operators complete their intended objectives within the target networks, whether that's data exfiltration, espionage, surveillance, or simply waiting for the right time.

The below graphic clearly shows the different cyber threat actors, along with their motivation for conducting operations in cyberspace. [2]



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

ASSOCIATED ROLES

The below roles generally contain work that includes certain aspects of Threat Intelligence:

- Threat Intelligence Analyst
- Senior Threat Intelligence Analyst
- Security Researcher
- Vulnerability Management Analyst

- Tier One SOC Analyst (Junior Security Analyst)
- Tier Two SOC Analyst (Security Analyst)
- Penetration Tester/Red Team Member

A DAY IN THE LIFE

Working as a Threat Intelligence Analyst is a varied role, and you'll often find yourself working on different tasks constantly. An example of some usual day-to-day tasks include;

- Gathering Indicators of Compromise from intelligence sources such as vendors, news, OSINT, and government alerts.

- Using IoCs to conduct Threat Exposure Checks (TECs), to see if any indicators have been identified within the network. All findings will be recorded within Threat Exposure Check cases for future reference.

- If any IoCs are identified, investigations will take place and recorded within a new case.

- Providing Threat Hunters with IoCs and malicious actor's Tools, Tactics, and Procedures (TTPs = Advanced IOCs), allowing targeted hunting within the network.

- IoCs can be blocked as a preventative measure. This could include blocking malicious IPs on perimeter firewalls, blocking domains or URLs on the web proxy, and blocking email senders on the email gateway.

- Keeping up to date with the latest security developments and malicious actor campaigns using OSINT, news, and paid-for intelligence services and platforms.

MODULE CHALLENGE

If you feel you're familiar with what Threat Intelligence is, and why it's important, then you may be ready for the Challenge! We suggest you still do some of your own research using the 'Useful Links' on the first page before attempting the Challenge.

Challenge Brief:

T.I

OPERATION CHIMERA

CYBER THREAT INTELLIGENCE MODULE // SECURITY BLUE TEAM

You have been asked to assist the Threat Intelligence function within the SOC to help discover and track Threat Actors, to help protect the organisation from advanced threats. Your company is based in the United Kingdom and operates within the Financial and Government industries. Your job is to write a short report, identifying 2 relevant Threat Actors, why they may affect your organisation, and any malware or vulnerabilities associated with these groups. This will be presented to the Senior Threat Intelligence Analyst for review. You will receive feedback based on your report. (Report template link coming out 16th 8PM).

It's recommended that you start with the following Threat Intelligence sites, and then perform your own searches to gather more information:

- FireEye Intelligence (http://fireeye.com/blog.html)
- ATT&CK Mitre (http://attack.mitre.org)
- AlientVault (http://otx.alienvault.com)
- APT Groups and Operations (http://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085)
- UK National Centre for Cyber Security (NCSC) (http://ncsc.gov.uk)

ELITE Challenge:
You need to gather any IOCs and TTPs (Tools, techniques, and procedures) that are associated with the groups you are reporting on. In the real-world, these would be used to conduct threat exposure checks, and potentially blocking actions would take place.