

WELCOME TO CLASS!
WHILE YOU'RE WAITING...
DON'T FORGET TO:

- ☐ DOWNLOAD THE [MILESTONE DOCUMENT](#) IN THE HANDOUTS SECTION
- ☐ PERFORM A [NEW INGESTION OF THE DATA](#) TO ELASTIC (SEE CONFIG GUIDE)
- ☐ [LOGIN TO HUNTER](#) TO MAKE SURE YOU HAVE ACCESS
- ☐ JOIN OUR [DISCORD COMMUNITY](#): [HTTPS://DISCORD.GG/DR4MCW4ZBR](https://discord.gg/dr4mcw4zbr)

*NOTE: IF YOU HAVEN'T CREATED YOUR HUNTER ACCOUNT, GO TO [WWW.CYBORGSECURITY.COM](http://www.cyborgsecurity.com) AND HIT THE "SIGN UP" BUTTON IN THE UPPER RIGHT, AND USE PROMOCODE: 'EXFIL'

THREAT HUNTING WORKSHOP: HUNTING FOR EXFILTRATION

WWW.CYBORGSECURITY.COM

31 MAY 2023



LET'S GO OVER A FEW THINGS:

- CONFIGURATION
- LOGIN TO HUNTER + HUNT PACKAGES
- QUESTIONS
- WORKSHOP RECORDING
- FINAL CHALLENGE

INTRODUCTIONS



LEE ARCHINAL
(INSTRUCTOR)

- 10+ YEARS IT
- 5 YEARS SOC
- 3 YEARS THREAT HUNTING



[HTTPS://WWW.LINKEDIN.COM/IN/LEE-ARCHINAL/](https://www.linkedin.com/in/lee-archinal/)



@ARCHINALLEE

INTRODUCTION TO EXFILTRATION

WHAT IS EXFILTRATION?

- Exfiltration consists of techniques adversaries use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption.
- There are many different ways to accomplish the goal and you can find more here:
 - <https://attack.mitre.org/tactics/TA0010/> [1]
- The technique discussed today will be
 - T1048 – Exfiltration Over Alternate Protocol

RESOURCE LIST

- We will be using the **Elastic SIEM** (Security Information and Event Manager)
 - Collects logs from different log sources and provides a central location that is searchable.
- We will be using multiple languages
 - **Kibana Query Language (KQL)**
 - Process.id:4444
 - **Lucene**
 - Wildcard for "evil.exe"
 - '/*[Ee][Vv][Ii][Ll]\.[Ee][Xx][Ee].*/'
 - **Domain specific language**
 - These are the hunts that we are going to extract from Hunter.
- Milestone document
 - This contains some artifacts that we will find along the way as well as your challenges.

HUNT PACKAGES USED

WinSCP Session Created - Possible Data Exfil

- Process CommandLine contains both:
 - *sftp://*
 - *scp://*
 - *ftps://*
- AND
 - Keywords contains
 - console

HUNT PACKAGES USED

Potential Exfiltration - Common Rclone Arguments

- The process_cmdline for Rclone_arguments (ALL) contains
 - *copy*
 - *-q*
 - *ignore-existing*
 - *auto-confirm*

EARN YOUR THREAT HUNTING CREDENTIALS!



- In your threat hunting platform there is one more example of execution.
- Use what you have learned today to find the method and answer the challenge questions using data from the log file.
- There are no time limits and you can submit as many attempts as you like.
- https://info.cyborgsecurity.com/exfil_flag

Q & A

HUNTER

THE THREAT HUNTING CONTENT PLATFORM

GET ACCESS FOR FREE WITH PROMO CODE: **EXFIL**



[HTTPS://WWW.HUNTWITHCYB.ORG/HUNTER](https://www.huntwithcyb.org/hunter)

FOLLOW US



@CyborgSecInc



cyborg-security



Cyborg Security



@CyborgSecInc



Cyborg Security



@CyborgSecInc