



# Part 4 Cyber Terminology

Cybersecurity For Beginners

Member Exclusive Certificate Series

WOMEN CYBERSECURITY SOCIETY

All Rights Reserved Copyright © 2018-2020

All Rights Reserved Copyright © 2018-2020



# Contributing Partner



**IMMERSIVE**LABS

Thank you!

All Rights Reserved Copyright ©2018-2020



# Agenda

- ❑ Presenter Introductions
  - ❑ WCS2 Overview
  - ❑ Attendee Introductions
  - ❑ **Cyber Terminology**
  - ❑ What you'll learn in the lab
  - ❑ Practical Exercises
  - ❑ Cybersecurity & VirusTotal
  - ❑ Demo & Analysis of Trojan & Virus
  - ❑ Closing Remarks
- Copyright ©2018-2020

# Lisa Kearney





# WCS2/IWCD Founder, & CEO



During the **spring of 2018**, Lisa founded the **Women CyberSecurity Society (WCS2)** to address the **lack of support** for women and minorities within the cybersecurity industry.

WCS2 is a **non-profit organization** that *advocates and champions women while providing support, services and advocacy to women around the globe.*

# Security Consultant



For more than 2 decades, Ms. Kearney has been defending networks, systems and data by providing cybersecurity services to hundreds of companies globally while working with Canada's top service providers and Fortune 50 companies. She currently works as an independent consultant with a focus on large enterprise environments. Particular joy is found working in security operations centres, incident response activities and threat hunting exercises.



# Introduce Yourself!

Please introduce yourself in the chat with the following information:

- ❑ Your name;
- ❑ location;
- ❑ Why you are here today; and
- ❑ Anything else you would like to share.



# Cyber Terminology Part 4



All Rights Reserved Copyright ©2018-2020





# In This Lab



In this lab you will **pick a letter within the hexagon** and **answer the associated question**. You will need to create a path of correct answers from one side to the other.

During the exercise portion, Use your new found cyber terminology knowledge **(and some Internet research)** to beat the honeycomb game!



# Why is cyber terminology important?

Misconceptions abound within the cybersecurity industry and it's **often the key personnel who don't understand** the difference between various domains, roles, incident types, and repercussions and loss due to a data breach or hacking incident.

**So it's important to learn these terms and get it right to avoid misuse and further confusion.**



# Interactive Lab

**Let's**

**GO!**

# Cybersecurity & Virustotal



Today we'll **examine two cybersecurity terms related to malware.**

- ❑ Trojan Horse
- ❑ Virus

Malware, short for malicious software, is any software designed to cause damage to assets.



# NICCS Cybersecurity Glossary

National Initiative for Cybersecurity Careers & Studies

**NICCS™**  
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Training ▾ Formal Education ▾ Workforce Development ▾ About NICCS

Home » About NICCS » Cybersecurity Glossary

## Cybersecurity Glossary

### Explore Terms: A Glossary of Common Cybersecurity Terminology

The NICCS Portal's cybersecurity lexicon is intended to serve the cybersecurity communities of practice and interest for both the public and private sectors. It complements other lexicons such as the NISTIR 7298 Glossary of Key Information Security Terms. Objectives for lexicon are to enable clearer communication and common understanding of cybersecurity terms, through use of plain English and annotations on the definitions. The lexicon will evolve through ongoing feedback from end users and stakeholders.

[Acronyms](#)

[a](#) | [b](#) | [c](#) | [d](#) | [e](#) | [f](#) | [g](#) | [h](#) | [i](#) | [j](#) | [k](#) | [l](#) | [m](#) | [n](#) | [o](#) | [p](#) | [q](#) | [r](#) | [s](#) | [t](#) | [u](#) | [v](#) | [w](#) | [x](#) | [y](#) | [z](#)

Click one of the letters above to advance the page to terms beginning with that letter.

## Trojan Horse

**Definition:** A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

All Rights Reserved Copyright ©2018-2020

<https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary>



# Cybrary Cybersecurity Glossary

## What is a Virus?

**Definition:** A hidden, self-replicating section of a computer software or program, usually malicious logic, that propagates by infecting, i.e., inserting a copy of itself into and becoming part of another program. **A virus cannot run by itself and requires that its host program be run to make the virus active.**

<https://www.cybrary.it/glossary/>

A screenshot of the Cybrary Cybersecurity Glossary website. The page has a dark header with the "CYBRARY" logo and navigation links for "CATALOG", "COMMUNITY", "CAREERS", "HIRE", "BUSINESS", and "LIVE". The main title is "Cybersecurity Glossary". Below the title is a large image of a dictionary page with the word "SECURITY" highlighted. Underneath the image, the text reads "Cyber Security Glossary" followed by a brief description: "Cybrary's cyber security glossary provides the cyber security community with knowledge of and insight on the industry's significant terms and definitions. This list contains key terminology and is one of the most extensive cyber security glossary/vocabulary resources online. Start your search on the critical terms you need to know as a security professional." At the bottom, there is a search bar with the text "Search terms by letter" and a row of letters "A B C D E F G H I J K L M N O P Q R S T U V W X Y Z".

# Examination of a Trojan Horse

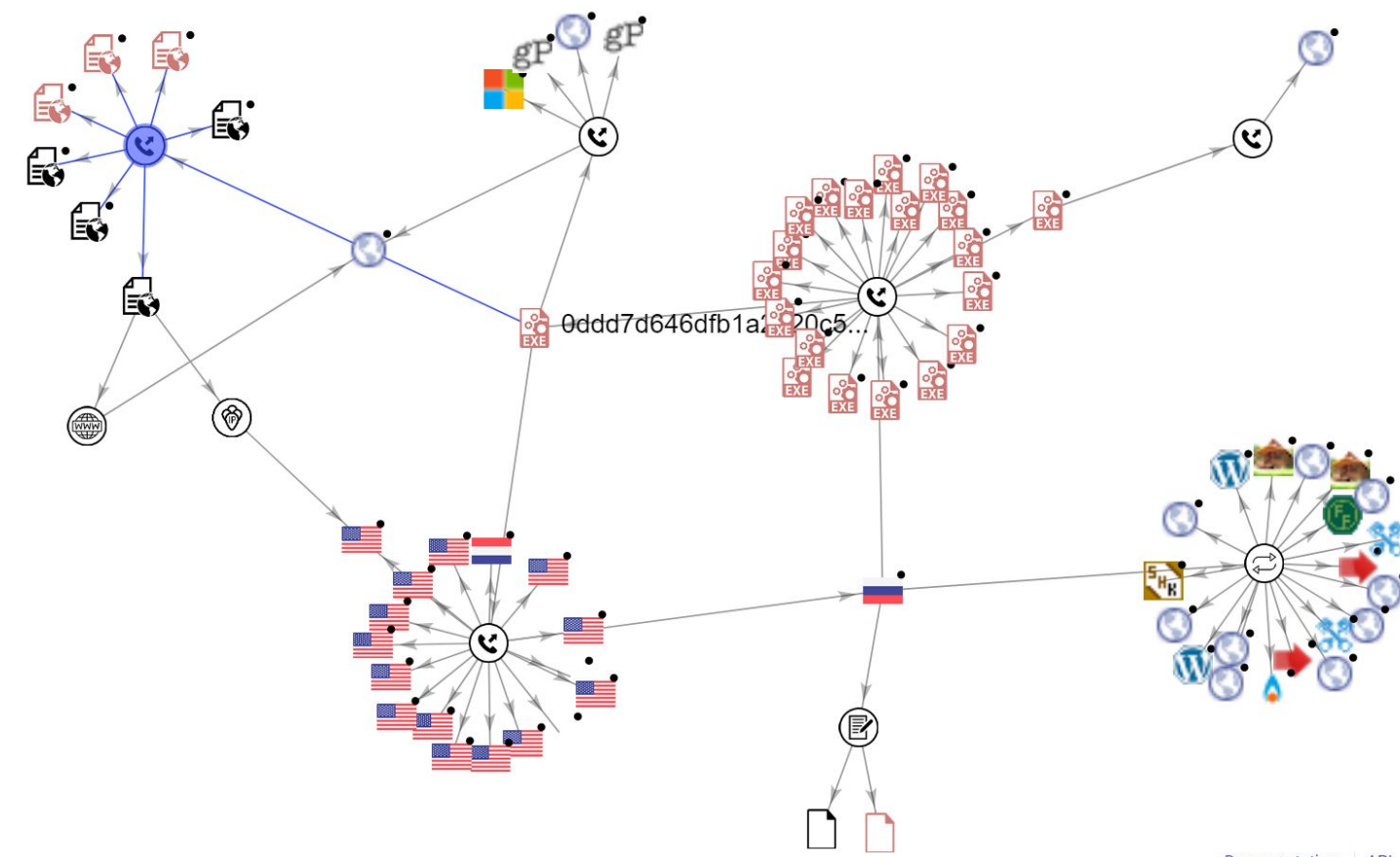
## **Trojan.Win32.Razy**

<https://www.virustotal.com/gui/file/0ddd7d646dfb1a2220c5b3827c8190f7ab8d7398bbc2c612a34846a0d38fb32b/detection>

### Trojan.Win32.Razym- Par... by cybergal

File Edit View Selection Visualization

Please, introduce 3 or more characters to perform a search in the graph



The graph visualization displays a complex network of nodes and edges. The nodes are represented by various icons: blue circles with a white 'X' (likely representing the malware), red squares with 'EXE' (executable files), and various system icons like folders, documents, and network symbols. A central node is labeled with a long alphanumeric string: '0ddd7d646dfb1a20c5...'. The graph shows a dense cluster of 'EXE' files connected to a central node, and other clusters of nodes connected to this central hub. The interface includes a search bar at the top, a 'Share / Embed' button, and a user profile for 'Lisa Kearney'. At the bottom right, there are links for 'Documentation', 'API', and 'Send feedback'.

0ddd7d646dfb1a20c5...

Documentation | API | Send feedback



# Examination of a Virus

## Melissa/I Love You Virus

These kinds of viruses are the ones that **run inside specific application** files that **allow macro programs in order to extend the capabilities of a given software.**

<https://www.virustotal.com/gui/file/8cc9935c6b75dbcfa669af936a060de8886d048c6f94ef179468a23b447c73f6/detection>



Detail info: C:\Users\Administrator\AppData\Local\Temp\~DF0D70307E752FC6C3.TMP  
C:\Users\Administrator\AppData\Roaming\Microsoft\Templates\~\$Normal.dot  
C:\Users\Administrator\AppData\Local\Temp\~DF255023B905DDC2EC.TMP  
C:\~\$sample.doc  
C:\Users\Administrator\AppData\Local\Temp\~WRF0000.tmp  
C:\Users\Administrator\AppData\Local\Temp\VBEMSFForms.exd  
C:\~WRD0001.tmp  
C:\Users\Administrator\AppData\Local\Temp\~DF350D88EBB592E8D0.TMP  
C:\Users\Administrator\AppData\Local\Temp\~DFAA7682395E70F0E1.TMP

Behaviour: Overwrite existing file

Detail info: C:\Users\Administrator\AppData\Local\Temp\outlook logging\firstrun.log

Behaviour: Copy file

Detail info: C:\PROGRA~2\MICROS~1\OFFICE\DATA\OPA11.BAK ---> C:\PROGRA~2\MICROS~1\OFFICE\DATA\opa11.dat  
C:\PROGRA~2\MICROS~1\OFFICE\DATA\OPA12.BAK ---> C:\PROGRA~2\MICROS~1\OFFICE\DATA\opa12.dat

Behaviour: File remove

Detail info: C:\Users\Administrator\AppData\Local\Temp\~DF0D70307E752FC6C3.TMP  
C:\Users\Administrator\AppData\Local\Temp\~DF255023B905DDC2EC.TMP  
C:\Users\Administrator\AppData\Local\Temp\~DF350D88EBB592E8D0.TMP  
C:\Users\Administrator\AppData\Local\Temp\~DFAA7682395E70F0E1.TMP  
C:\~WRL0002.tmp

Behaviour: Find file

Detail info: FileName = C:\Program Files\Common Files\Microsoft Shared\office11  
FileName = C:\Program Files\Common Files\Microsoft Shared\office11\mso.dll  
FileName = C:\Program Files\Common Files\Microsoft Shared\office11\\*. \*  
FileName = C:\Program Files  
FileName = C:\Program Files\Microsoft Office  
FileName = C:\Program Files\Microsoft Office\OFFICE11\Normal.dot  
FileName = C:\Users\Administrator\AppData\Roaming\Microsoft\Templates\Normal.dot  
FileName = C:\Windows  
FileName = C:\Windows\WinSxS  
FileName = C:\Windows\WinSxS\x86\_microsoft.vc80.crt\_1fc8b3b9a1e18e3b\_8.0.50727.4940\_none\_d08cc06a442b34fc\M  
FileName = C:\sample.doc  
FileName = C:\PROGRA~1  
FileName = C:\PROGRA~1\COMMON~1  
FileName = C:\PROGRA~1\COMMON~1\MICROS~1  
FileName = C:\PROGRA~1\COMMON~1\MICROS~1\WBA

Behaviour: File rename

Detail info: C:\sample.doc ---> C:\~WRL0002.tmp  
C:\~WRD0001.tmp ---> C:\sample.doc

# Cybersecurity Roles Related to Malware

**Malware Reverse Engineer**

**Malware Analyst**

**Threat Researcher**

**Threat Hunter**





# Further Training From Our Partners



<https://immersivelabs.online/labs/intro-to-malware-static-analysis>

**EC-Council**

<https://iclass.eccouncil.org/our-courses/malware-memory-forensics/>



**INTERNATIONAL**

**WOMEN**

**IN**

**CYBER**

**DAY**

All Rights Reserved Copyright ©2018-2020

<https://www.change.org/internationalwomenincyberday>



# Community





# Join A Chapter & Slack

**Join or lead a local chapter to receive discounts and special offers**

- ❑ <https://womencybersecuritysociety.org/join-or-lead-a-chapter>

**Connect with other women in our Slack Community**

- ❑ [https://join.slack.com/t/womencssociety/shared\\_invite/zt-e3uf3ksn-xlMky5~l3wQjacYlbvs8zm](https://join.slack.com/t/womencssociety/shared_invite/zt-e3uf3ksn-xlMky5~l3wQjacYlbvs8zm)



# Q&A

All Rights Reserved Copyright ©2018-2020





Thank you!



All Rights Reserved Copyright © 2018-2020