

September 3, 2024

“How Do Spies Really Operate?”

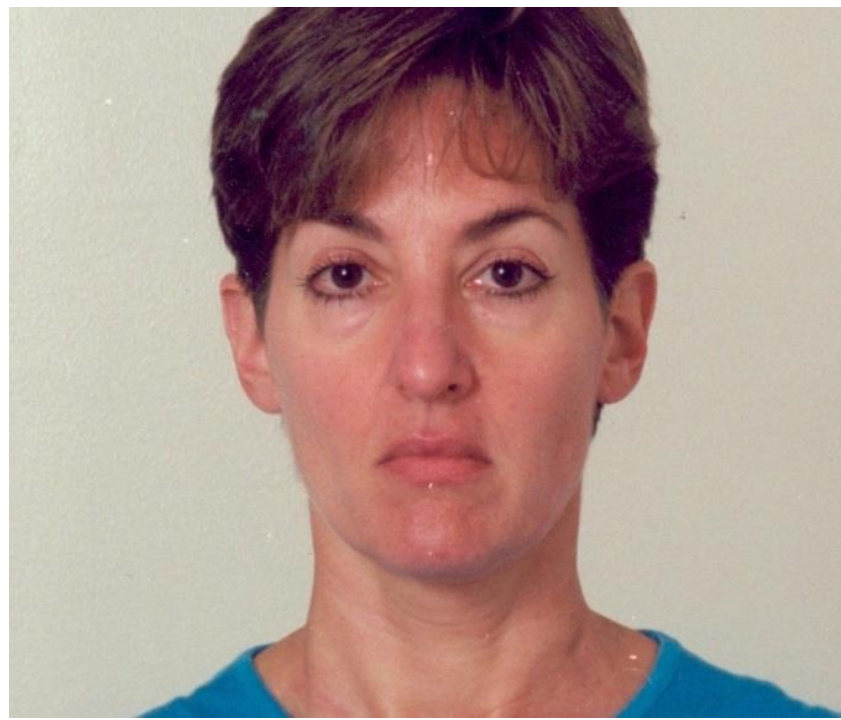
Foundations of Cybersecurity - CYBS 3213

**Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute**



Checking In

- So far we've looked at the questions, “How do people become experts?” “What is Cybersecurity?” and “What is the weakest link in Cybersecurity?” (Social Engineering)
- What have been the most important concepts that you learned in the last classes?
- What have been the muddiest (most unclear) points during the last classes?




How do spies really operate?

- Openly
- Covertly
- Non-official cover
- Successful operations are about building recruiting people, building trust, and gathering data.
(Ring a bell?)

What do they do?

- Intelligence officers recruit other people, known as agents, to obtain information that a foreign government would consider secret or confidential.



 **NBC NEWS**



Cyber Espionage

Cyber can be an attractive method of intelligence gathering for several reasons:

- It can be more cost-effective than traditional means;
- Its remote nature means that those involved have an extra layer of deniability;
- The volume of data that can be stolen is potentially immense.
- Cyber also negates the need for a human agent as information gathering can be done remotely, without an intelligence officer needing to leave their desk, let alone their country.



Malware

Malware (malicious software) is any software developed to compromise the confidentiality, integrity, or availability of data. Malware can be used to steal data, modify files, or deny user access. Malware is often spread through phishing emails.



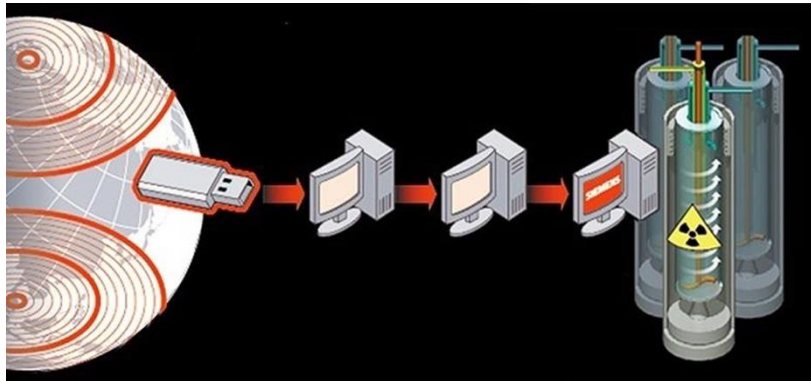
Virus

Virus – like a biological virus composed of tiny bits of genetic material enclosed by a protective shell. Waiting for a favorable environment to rapidly self-replicate. Similarly, Computer virus is malicious code attached to a file looking to self-replicate.



Worms

Worms - a malicious program that uses a computer network to replicate itself to other devices. A worm spreads by exploiting a vulnerability. An attacker may use a worm to deliver other malware, steal data, or open a backdoor on the infected device. Hacker often uses social engineering & phishing.



ILOVEYOU Virus

Trojan

Trojan – an executable program that masquerades as performing a benign activity but also does something malicious. Two types are:

- Remote Access Trojan (RAT)
- Potentially Unwanted Program (PUP)



Trojan

Trojan could do any of these:

1. Download harmful software
2. Install a key logger or other spyware.
3. Delete files
4. Open a backdoor for a hacker to use.





Spyware

Spyware - a type of malware (usually delivered via trojan horse) that collects user data without the user's consent. Could track shopping habits or gain financial information or remotely accessing a webcam. A keylogger is a good example of a spyware tool.

PEGASUS SPYWARE

THE MOST
DANGEROUS
MALWARE!

- *What is Pegasus Spyware?*
- *How is Pegasus Spyware Spread?*
- *Pegasus Spyware technical details*
- *Pegasus and the international community*



blog.gridinsoft.com



rootkit

Rootkit

Rootkit - a type of malware that provides administrative, or root access, to a computing device without permission or detection. A rootkit may be designed to:

- install, hide, or prevent the removal of other malware.
- allow an attacker to use the device to attack other devices.
- create a backdoor that allows an attacker to access confidential data.

Bots

Bots - an infected computer that enables an attacker to remotely control the device. A bot communicates with a command and control (C&C) server to receive instructions or send back information. A group of bots, called a botnet, can be used to coordinate large-scale attacks.



Logic Bomb

- A type of malware that activates an attack when specified conditions are met.



CYBERCRIME

Former Siemens Contractor Sentenced to Prison for Planting Logic Bombs

A 62-year-old man from Harrison City, Pennsylvania, has been sentenced to prison for planting logic bombs in programs he created for German industrial giant Siemens.



By [Eduard Kovacs](#)
December 18, 2019





Which of the following is NOT a type of malware that has as its primary trait to launch attacks on other computers?

a. Bot

b. Virus

c. Worm

☒ d. Trojan



Ransomware

Malicious software designed to extort money from victims in exchange for their computer being restored to its normal working state. Two types:

- (1) Cryptomalware: malware that encrypts some or all of the files on an infected device, such as passwords, until a ransom is paid
- (2) Blocker Ransomware: prevents users from using the computer in normal fashion



Expect More.

The Top 5 Ransomware Groups 2022-2023

LockBit 3.0	393 (2022) to	1,038 (2023)	(+164%)
BlackCat	245 (2022) to	422 (2023)	(+72%)
CL0P	30 (2022) to	386 (2023)	(+1,186%)
PLAY	26 (2022) to	308 (2023)	(+1,084%)
BlackBasta	172 (2022) to	210 (2023)	(+22%)

The average cost of a ransomware breach is USD \$5.13 million,
which does not include ransom payments.

Top Ransomware Targets

Sector	2022	2023	Change
Construction	153	230	+77 (50%)
Hospitals and Health Care	89	175	+86 (96%)
IT Services and IT Consulting	74	163	+89 (120%)
Financial Services	58	147	+89 (153%)
Law Practice	67	143	+76 (113%)
Higher Education	56	118	+62 (110%)

Ransomware Explained

Ransomware

Explained



Ransomware as a Service Revenue Models

There are 4 common RaaS revenue models:

1. Monthly subscription for a flat fee
2. Affiliate programs, which are the same as a monthly fee model but with a percent of the profits (typically 20-30%) going to the ransomware developer
3. One-time license fee with no profit sharing
4. Pure profit sharing

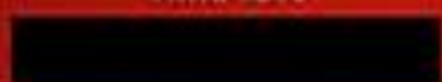
Payment for private key



Private key will be destroyed on



Time left



Choose a convenient payment method:

Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address

[Redacted Bitcoin Address] and specify the transaction ID, which will be verified and confirmed.

[Home Page](#)

[Getting started with Bitcoin](#)

Enter the transaction ID and press «Pay»:

1

BTC



What is CryptoLocker ransomware and where does it come from?

CryptoLocker ransomware is a type of malware that encrypts files on Windows computers, then demands a ransom payment in exchange for the decryption key. It first emerged in September 2013 in a sustained attack that lasted until May of the following year. CryptoLocker fooled targets into downloading malicious attachments sent via emails. Once opened, these Trojan horse attachments would execute the malware hidden inside.

Was CryptoLocker a virus? Not quite. Unlike viruses and worms, **CryptoLocker couldn't make copies of itself**. So how did CryptoLocker spread? To help it infect additional victims, the cybercriminals behind it made use of the now-notorious Gameover Zeus botnet. This was a network of malware-infected computers that could be controlled remotely by the botnet's operator, without the knowledge or consent of their owners. In other words, it was a readymade audience for a massive CryptoLocker ransomware infection.

Data Backup Strategy

Review primary questions to consider when formulating a data backup strategy:

- a. What data should be backed up?
- b. What media should be used to backup?
- c. Where should the backup be stored?
- d. How frequently the backup should be performed?

Rowan's sister called him about a message that suddenly appeared on her screen that says her software license has expired and she must immediately pay \$500 to have it renewed before control of the computer will be returned to her. What type of malware has infected her computer?

- a. Persistent lockware
- ☒ b. Blocking ransomware
- c. Cryptomalware
- d. Impede-ware



Prepare Media Article and Presentation

- Relevance to class topic (20%):
- Understanding of the issue (30%):
- Clear and organized summary (30%)
- Engagement with class (20%):
- **IMPORTANT:** Upload your article before the next class and provide a few sentences to answer each of the first three questions.

