A List of Topics:

Task: In small groups, discuss the following guidelines questions

* What’s the threat?
* What’s the vulnerability?
* What could be the fix? Or is there a fix?
* Can you connect the topic with your own experience?
* Anything else you want to share

CD Projekt Ransomware Attack

World renowned game studio CD Projekt Red, best known for their series ‘The Witcher’ and more recently ‘Cyberpunk 2077’ suffered a ransomware attack a few short months after the release of Cyberpunk to VERY mixed reactions. The source code for Cyberpunk, the RED engine used to make that game and their other games, and unreleased content for their previous game, The Witcher 3, was leaked and sold on a dark web auction.

<https://www.theverge.com/2021/2/9/22274035/cd-projekt-hack-source-code-cyberpunk-2077-witcher-3-encrypt-data-ransom>

<https://www.bloomberg.com/news/articles/2021-02-24/cd-projekt-hack-severely-disrupts-work-on-cyberpunk-game-updates>

<https://www.engadget.com/cd-projekt-red-data-breach-online-114047285.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALJvT3uD6WHpRUO3viBB2_0G-E9tpOn7OM5xVcogqbpC4PhO1xFKrzp-tAObmuvrXGtTGWB_rCRBA9kUONahoHL-01t3fI5A2g8xUCGs0BWVk9WztSSRvWoAQZQKoumm4nn5Uy_86SBsKJuWmCSWQZS96tkAiN5nJ7As5Yspvn3Z>

<https://www.engadget.com/cd-projekt-red-cyberpunk-2077-source-code-hack-ransomware-sold-202610194.html>

|  |  |
| --- | --- |
| **Group A** | **Group B (Vicente)** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Security issues with Drone

Nowadays people use drones (unmanned aerial vehicle) to do more things, like capture beautiful traveling moments, and help the government to monitor criminals. An unmanned aerial vehicle combined aircraft body, communication module and remote controlling system can help execute some unreachable task of humans.

<https://pilotinstitute.com/drone-jobs/>

|  |  |
| --- | --- |
| **Group A** | **Group B** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Google, Mozilla Ban Hundreds of Browser Extensions in Chrome, Firefox

After discovering a wide pattern of potentially malicious behavior in browser extensions, the two search giants are cracking down. Both the Google Chrome and Mozilla Firefox teams are banning web browser extensions that steal user data and execute remote code, among other bad actions.

<https://threatpost.com/google-mozilla-ban-browser-extensions-chrome-firefox/152257/>

|  |  |
| --- | --- |
| **Group A** | **Group B** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Coronavirus Goes Cyber With Emotet

Recently, Emotet, a kind of banking trojan malware program has spread in Japan camouflage as email using the scare of Coronavirus, reported by IBM X-Force and Kaspersky. These emails are titled as the notification and warning of coronavirus, which is an ongoing global scale health crisis beginning in Japan's neighbor, China. To lure victims to open malicious attachments, these emails are masked as official notifications and say there are more details on prevention against coronavirus.

<https://threatpost.com/coronavirus-propagate-emotet/152404/>

|  |  |
| --- | --- |
| **Group A** | **Group B** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Social Captain exposes thousands of Instagram passwords.

Social Captain is a social media boosting service that helps Instagram users to increase their followers. This tool promises to help gain real followers and engagement. Social Captain accomplishes this through automated targeted marketing and artificial intelligence. In order to do this, the user has to enter the username and password of their account. Turns out Social captain was storing the passwords in an unencrypted plain text.

<https://techcrunch.com/2020/01/30/social-captain-instagram-passwords/>

|  |  |
| --- | --- |
| **Group A** | **Group B** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Smart Toys

From video games with VR to turning lifeless stuffed animals into technology ridden robots. Even hot wheels are starting to have sensors placed inside them. The new age of smart toys has quickly emerged and toys today have sensors, speakers, microphones, and sometimes even the ability to connect to the internet. It was intended to customize the child's experience with the toy but it has since turned into a very big security risk for the parent and the child's safety.

<https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/>

|  |  |
| --- | --- |
| **Group A** | **Group B** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Unpatched supply-chain flaw

An Unpatched vulnerability in the Linux Pling Store can be abused for supply-chain attacks and achieve remote execution. PlingStore allows users to search and install Linux software, themes, icons, and other add-ons that may not be available for download through the distribution's software center.

<https://thehackernews.com/2021/06/unpatched-critical-flaw-affects-pling.html>

|  |  |
| --- | --- |
| **Group A** | **Group B** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Is TikTok a National Threat?

In November, 2019, Tiktok (a short video APP), which is very popular among young people in the United States, was investigated and rectified by the US security team. On December 12, 2019, The U.S. Department of Defense ordered employees to remove Tiktok from their devices. In 2021 TikTok is now collecting biometric data? Is TikTok Safe?

<https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collect-biometric-data-on-u-s-users-including-faceprints-and-voiceprints/>

<https://www.businessinsider.com/is-tiktok-safe>

|  |  |
| --- | --- |
| **Group A** | **Group B** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Colonial Pipeline Ransomware Attack:

<https://securityboulevard.com/2021/05/the-colonial-pipeline-ransomware-attack-everything-we-know/>

|  |  |
| --- | --- |
| **Group A** | **Group B** |
|  | Andrew |
|  |  |
|  |  |
|  |  |
|  |  |