MARK IAN E BALLESCA

BSIT – 4 BLK – 1

CYBER SECURITY

Th 10:30-12:30 1-2 PM

LABORATORY ACTIVITY 1

PART 1:

. ZEROTRACK

ZeroTrack was a sophisticated spyware attack that appeared around May 5, 2022. It mainly targeted corporate environments, exploiting weak points in VPN and remote desktop protocols. ZeroTrack gained access to networks by infecting seemingly legitimate software updates, which when downloaded by users, granted attackers access to internal systems. Once inside, the malware silently tracked employee activities, logging keystrokes and screen captures, sending sensitive data to an external server. The malware's stealth and its ability to bypass traditional security systems made it particularly dangerous. The widespread nature of the attack led to major data breaches in industries like finance and healthcare. Experts estimate ZeroTrack was responsible for billions in financial losses and exposed sensitive data of millions of users.

- **SPYWARE ATTACK**
- **EXPLOITED SOFTWARE UPDATES & REMOTE DESKTOP VULNERABILITIES**
- **ATTACKERS LURED USERS THROUGH SOCIAL ENGINEERING AND FALSE UPDATE PROMPTS**

---

2. AURORAWAVE

AuroraWave was a ransomware attack that emerged on July 15, 2021, primarily targeting small-to-medium-sized enterprises (SMEs) worldwide. This malware spread through phishing emails containing links to compromised websites. Once a user clicked the link, they were redirected to a page that tricked them into downloading a malicious file disguised as a document. Once executed, the ransomware encrypted the victim's files, demanding payment in cryptocurrency for decryption keys. What made AuroraWave particularly dangerous was its ability to spread across networks, encrypting files on network drives and cloud services. The attack caused widespread disruptions in businesses, including manufacturers, retail, and service providers. Recovery for most companies took weeks, leading to significant operational downtime.

- **RANSOMWARE ATTACK**
- **EXPLOITED PHISHING LINKS AND SOCIAL ENGINEERING**
- **TARGETED SMES AND DISRUPTED OPERATIONS WORLDWIDE**

---

3. PHANTOMBRIDGE

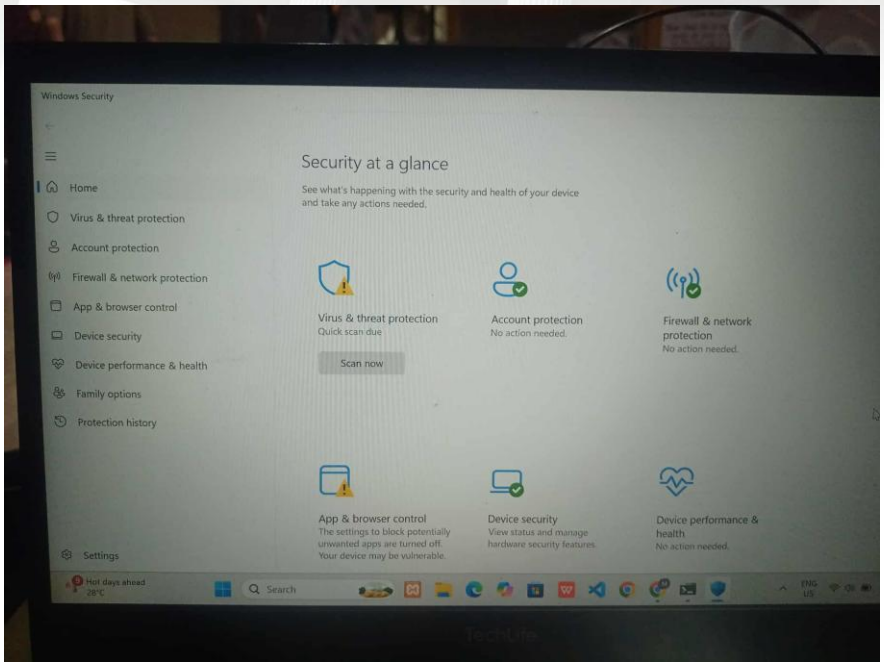
PhantomBridge was an advanced form of a botnet attack that surfaced in March 2020. This attack used a unique method known as "network tunneling" to infect IoT devices, such as security cameras, smart thermostats, and home routers. Once infected, these devices would be hijacked and used to create a massive botnet that could launch Distributed Denial of Service (DDoS) attacks on high-profile targets. The malware remained undetected for months due to its ability to mimic normal device behavior. When the botnet was activated, it flooded the target's

servers with requests, crippling their websites and services. The attacks were so widespread that multiple major websites were taken offline for hours at a time, affecting everything from online retail to government services. The malware was particularly effective at exploiting unpatched vulnerabilities in outdated IoT devices.

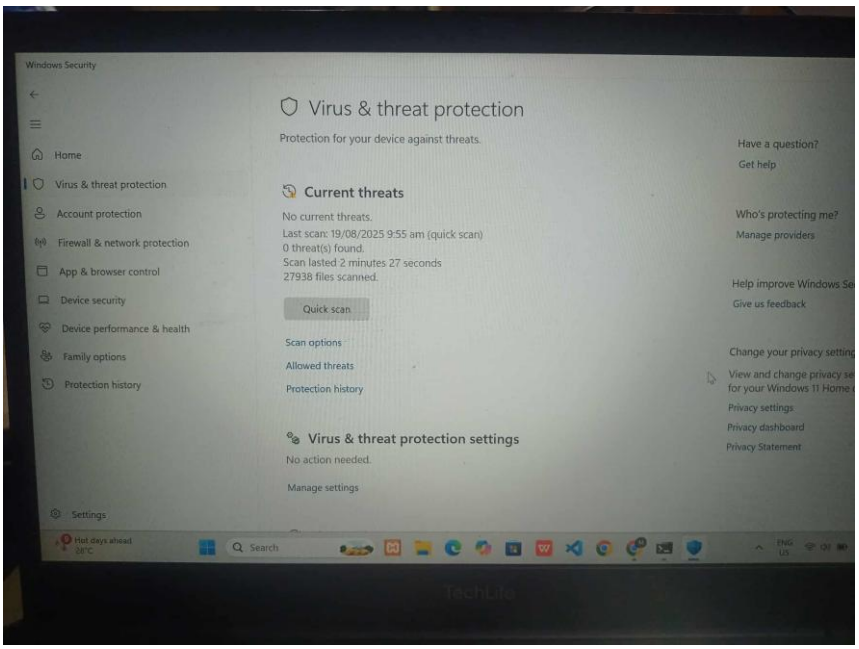
- **BOTNET ATTACK**
- **EXPLOITED IoT DEVICE VULNERABILITIES AND NETWORK TUNNELING**
- **CARRIED OUT MASSIVE DDOS ATTACKS ON GLOBAL WEBSITES**

PART 2:

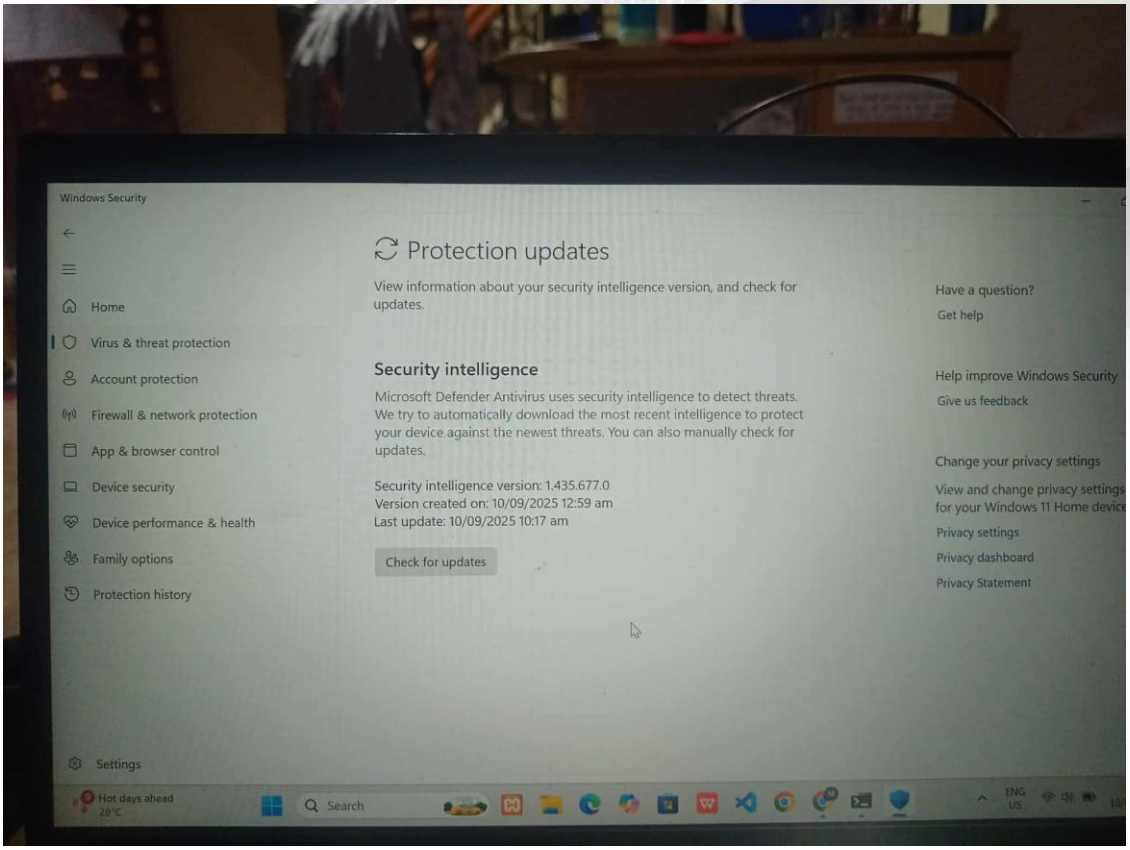
STEP 1:



STEP 2:



STEP 3:



Basic cybersecurity measures are crucial for safeguarding both personal and organizational data against common cyber threats. Simple practices such as setting up multi-factor authentication (MFA), regularly backing up data, using encryption tools, and being cautious with public Wi-Fi can significantly lower the risk of falling victim to cyberattacks like ransomware, identity theft, or data leakage. Implementing these measures builds a foundational defense against evolving threats, helping ensure sensitive information remains secure and that systems stay resilient to unauthorized access. Regularly educating individuals on the latest threats and safe online behavior also strengthens this defense.