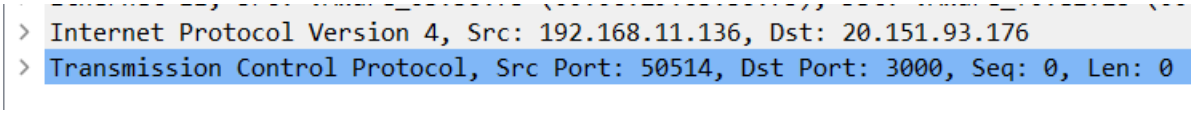
ISEC 2079

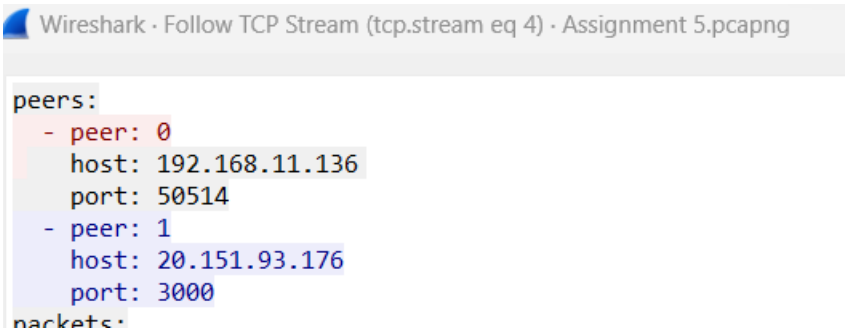
Evolving Technologies and Threats

Adeniyi Oluwashile

1. Identification of Incidents:

The user that was picked up is a keylogger and the password
Source IP address: 192.168.11.136
Source Port: 50514





2. Containment (Short Term)

- Disable the user account: The block all forms for authentication/ sign in to the user account and this can be done on Active Directory. Once this get disabled, it syncs and disable the AD User account used to sign in to the workstation, Disables the Microsoft 365 user and disables the VPN User
- Change the user password immediately: Once the password is changed on the Active Directory, it syncs across all platforms. This prevents the user from logging into the user account and performing a thorough investigation on the compromised user activities.

3. Containment (Long Term)

- Revoke Sign-in Session: This log out the user from all devices. When an user account is compromised, the attacker might have active session on their phone, computer (Outlook Client or Outlook for Web) and by revoking the sign in session, it will automatically log out the user from all platforms
- Enable and Enforce authentication (MFA): MFA adds an extra layer of security by requiring users to provide additional verification, such as a code sent to their mobile device, in addition to their password. This helps protect against unauthorized access even if the password is compromised.
- Regular security awareness training for the employees: Conduct regular security awareness training sessions for employees to educate them about the risks of phishing emails, accessing unknown USB devices, untrusted programs and suspicious links, and the importance of following security best practices. This will help employees identify and report potential threats
- Implement or update email filtering: Ensure an email filtering solution is active that can detect **and block malicious emails, reducing the risk of employees receiving phishing emails or clicking on malicious links such as Microsoft Safe links, Save attachments and review the spam filter policy**

4. Eradication of Re-Entry Points

- Isolate affected workstation: Identify and isolate the compromised workstation by disconnecting the affected workstation from the network to prevent further communication with potentially malicious servers or exfiltration of data
- Scan and clean the workstation: erform a thorough scan of the affected workstation using up-to-date antivirus software to detect and remove any malware or malicious scripts that may have been introduced through the USB or other means.
- Review security policies regarding USB acceptable usage and enhance it
- Patch and update systems: Ensure that all servers, including those relying on the same authentication (Active Directory and VPN), are up to date with the latest security patches and updates. This helps mitigate vulnerabilities that could be exploited by attacke

5. Recovery

6. Lessons Learnt

DESKTOP-39UP7VP&?bryan&?'e'DESKTOP-39UP7VP&?bryan&?'m'DESKTOP-39UP7VP&?bryan&?'a'DESKTOP-39UP7VP&?bryan&?'i'DESKTOP-39UP7VP&?bryan&?'l'DESKTOP-39UP7VP&?bryan&?Key.shiftDESKTOP-39UP7VP&?bryan&?'@'DESKTOP-39UP7VP&?bryan&?'c'DESKTOP-39UP7VP&?bryan&?'o'DESKTOP-39UP7VP&?bryan&?'m'DESKTOP-39UP7VP&?bryan&?'p'DESKTOP-39UP7VP&?bryan&?'a'DESKTOP-39UP7VP&?bryan&?'n'DESKTOP-39UP7VP&?bryan&?'y'DESKTOP-39UP7VP&?bryan&?'.'DESKTOP-39UP7VP&?bryan&?'c'DESKTOP-39UP7VP&?bryan&?'o'DESKTOP-39UP7VP&?bryan&?'m'DESKTOP-39UP7VP&?bryan&?Key.enterDESKTOP-39UP7VP&?bryan&?Key.shiftDESKTOP-39UP7VP&?bryan&?'S'DESKTOP-39UP7VP&?bryan&?'t'DESKTOP-39UP7VP&?bryan&?'r'DESKTOP-39UP7VP&?bryan&?'o'DESKTOP-39UP7VP&?bryan&?'n'DESKTOP-39UP7VP&?bryan&?'g'DESKTOP-39UP7VP&?bryan&?'p'DESKTOP-39UP7VP&?bryan&?'a'DESKTOP-39UP7VP&?bryan&?'s'DESKTOP-39UP7VP&?bryan&?'s'DESKTOP-39UP7VP&?bryan&?'w'DESKTOP-39UP7VP&?bryan&?'o'DESKTOP-39UP7VP&?bryan&?'r'DESKTOP-39UP7VP&?bryan&?'d'DESKTOP-39UP7VP&?bryan&?'1'DESKTOP-39UP7VP&?bryan&?'2'DESKTOP-39UP7VP&?bryan&?'3'DESKTOP-39UP7VP&?bryan&?Key.enter