COSC540 - COMPUTER NETWORKS AND NETWORK SECURITY

Assessment – 5

BIKASH NEUPANE
220245756
bneupan2@myune.edu.au

Table of Contents

Article 1

Link to Article: Five Australians arrested over cybercrime in global policing operation

Link to Forum: Five Australians arrested over cybercrime in global policing operation

CIA Classification: (Confidentiality and Integrity) This incident breaches the confidentiality and integrity aspects of the CIA triad. Confidentiality is compromised as personal information, such as online banking logins, credit card details, and passwords, was stolen from victims. Additionally, the integrity aspect is affected through the creation of fraudulent websites impersonating legitimate entities, potentially leading victims to trust and disclose their sensitive information.

Severity of Attack: The severity of the attack is significant, involving over 94,000 Australians and a potential harm estimated at $28 million. This operation had a global reach, with around 10,000 cybercriminals implicated worldwide. The dismantling of LabHost's infrastructure, including 207 criminal servers, underscores the seriousness of the situation.

When and Where Reported: The incident was reported by various news outlets, including 9News Australia, on April 18, 2024, at 5:48pm (Sydney Time).

Description of Attack: The cybercrime operation utilized a platform known as LabHost, which facilitated phishing attacks to steal personal information from victims. Cybercriminals employed fraudulent links sent via texts and emails to trick victims into providing sensitive details such as online banking logins, credit card information, and passwords. LabHost enabled the creation of over 170 fake websites mimicking reputable banks and government portals, including the myGov online service. Australian offenders, among others globally, allegedly used LabHost to conduct phishing attacks, resulting in significant financial losses and ongoing security risks for victims.

Actions to Prevent/Recover:

- Enhanced Cybersecurity Measures: Implement robust cybersecurity measures, including regular security audits, penetration testing, and the use of advanced threat detection systems to identify and mitigate phishing attempts.
- User Education and Awareness: Educate users about phishing techniques and how to identify suspicious emails, texts, and links. Encourage the practice of verifying the authenticity of websites before entering sensitive information.
- Law Enforcement Collaboration: Strengthen international collaboration among law enforcement agencies to track and dismantle cybercrime

operations like LabHost. Coordinated efforts can lead to more effective disruption and prosecution of cybercriminal networks.

- Multi-factor Authentication (MFA): Encourage the use of MFA for online accounts, which adds an extra layer of security beyond passwords, making it harder for cybercriminals to gain unauthorized access even if credentials are compromised.
- Prompt Incident Response: Establish protocols for swift incident response in case of a phishing attack. This includes immediately notifying affected users, blocking access to compromised accounts, and working with law enforcement to investigate and prosecute perpetrators.

Article 2

Link to Article: Russian hackers steal US government emails from Microsoft

Link to Forum: Russian hackers steal US government emails from Microsoft

CIA Classification: (Confidentiality) This incident primarily breaches the confidentiality aspect of the CIA triad. The theft of email correspondence between US government agencies and Microsoft compromises the confidentiality of sensitive information exchanged via email. Additionally, there may be concerns regarding the integrity of the stolen emails if they have been tampered with or manipulated by the hackers.

Severity of Attack: The severity of the attack is high due to the theft of sensitive email correspondence between US government agencies and Microsoft. Although there is currently no evidence of the hackers using the stolen credentials to access federal computer systems actively, the breach poses a significant risk to national security and the integrity of government communications.

When and Where Reported: CNN updated this incident on 5:52 PM EDT, Thu April 11, 2024. It was also reposted by 9News Australia as well on 8:22am Apr 12, 2024, AEDT.

Description of Attack: Russian state-backed hackers breached Microsoft's systems, stealing email correspondence between US government agencies and Microsoft. The stolen emails included login information such as usernames and passwords. While there is no evidence yet of the hackers using the stolen credentials to compromise federal computer systems actively, the breach has prompted concerns about potential further damage and the need for enhanced cybersecurity measures. The attack highlights the ongoing threat posed by state-sponsored cyber-espionage groups targeting critical infrastructure and sensitive government communications.

Actions to Prevent/Recover:

- Enhanced Cybersecurity Measures: Microsoft and US government agencies must implement enhanced cybersecurity measures to prevent further unauthorized access and mitigate the impact of the breach. This includes strengthening authentication protocols, conducting thorough security assessments, and implementing robust intrusion detection and prevention systems.
- Emergency Directives: CISA issued an emergency directive ordering affected civilian agencies to shore up their defenses and mitigate the risk of further exploitation. Agencies must prioritize the protection of sensitive information and promptly address any vulnerabilities identified in their systems.

- International Collaboration: The US government should engage in international collaboration efforts to address the threat posed by state-sponsored cyber-espionage groups. Collaboration with allies and partners can enhance threat intelligence sharing, facilitate coordinated response efforts, and deter future attacks.
- User Training and Awareness: Enhancing user training and awareness programs is crucial to mitigating the risk of phishing attacks and social engineering tactics used by hackers. Educating users about cybersecurity best practices and raising awareness about the evolving threat landscape can help prevent future breaches.
- Regulatory Compliance: Microsoft and other technology companies must comply with regulatory requirements and industry standards to protect customer data and ensure the integrity of their systems. Compliance with regulations such as the GDPR and the NIST Cybersecurity Framework can help organizations enhance their cybersecurity posture and mitigate the risk of data breaches.