Department of Information Technology

**Home Assignment 1**

| **Subject: Computer Network Security (CNS)** | **Class: TE INFT-A** |
| --- | --- |
| **Name: Durva Kadam** | **Roll No.: 47** |
| **Batch: A3** | **Academic Year: 2024-2025** |

| **Allotted Question** | **Assignment 47:** **Keylogger Case Studies**  **Objective:** To analyze real-world keylogger attacks and their  consequences.  **• Task:**  • Research and select a high-profile keylogger attack case.  • Analyze the attack methodology and the attacker's motives.  • Discuss the impact of the attack on victims and organizations  involved.  • Propose preventive measures to mitigate similar attacks. |
| --- | --- |
| **Answer**  **Details:** | **Introduction:** Keyloggers are malicious programs designed to record a user’s keystrokes. One of the high-profile and sophisticated examples is the **Snake Keylogger**. It emerged as a significant threat in November 2020, showcasing a fusion of credential theft and keylogging functionalities. Developed using .NET, its arsenal includes keystroke logging, harvesting stored credentials, and capturing screenshots. Moreover, it exhibits an adeptness in gathering clipboard data, browser credentials, and conducting system and network reconnaissance.  **Attack Methodology:**  The Snake Keylogger spreads primarily via phishing emails, often disguised as documents, PDFs, or executables. When the user opens the attachment, the malware installs itself and starts capturing keystrokes and clipboard data, which includes sensitive information such as passwords, personal identification numbers (PINs), and other confidential data.  Once installed, Snake Keylogger employs a wide range of techniques to remain undetected. These techniques include anti-analysis tactics that disable debugging and reverse-engineering tools. This makes it exceptionally stealthy, increasing its potency as a cyber espionage tool. It can also capture screenshots and steal data from various installed programs, such as browsers and email clients.  The Snake Keylogger attack involves several sophisticated techniques:   1. **Phishing Email**: Victims receive a deceptive email with an attached malicious Excel file. 2. **Malicious Excel Document**: The Excel file exploits CVE-2017-0199 to download a malicious HTA file from a remote server. 3. **Execution of Payload**: The HTA file runs obfuscated JavaScript, which decodes and executes PowerShell code to download the Snake Keylogger executable. 4. **Loader Module**: The downloaded executable (sahost.exe) acts as a loader, decrypting and extracting the core Snake Keylogger module from various resources. 5. **Deployment**: The core module is deployed using process hollowing and scheduled tasks to ensure persistence. 6. **Keylogger Functions**: The keylogger collects sensitive information (credentials, keystrokes, screenshots) and sends it to the attacker via SMTP. 7. **Anti-Analysis Techniques**: The malware uses encryption and obfuscation to evade detection and analysis.  **Attacker’s Motives:** The primary motive of Snake Keylogger is financial gain. The attackers aim to steal valuable credentials, credit card details, and other personal information that can be sold on the black market or used for further financial fraud. In some cases, the malware can be leveraged to commit corporate espionage by infiltrating business networks and gathering sensitive intellectual property or confidential information.  Furthermore, the widespread availability of Snake Keylogger in underground forums makes it an attractive tool for less-experienced cybercriminals, creating an ecosystem where even low-level attackers can launch significant cyberattacks.  Additionally, identity theft and disruption are key motives. Attackers may use stolen credentials to impersonate individuals, damaging reputations and causing personal or organizational harm. They might also aim to create chaos by disrupting business operations or harming data integrity. In some cases, motivations include political activism or creating botnets for further attacks. Understanding these motives helps in designing targeted defenses and prevention strategies. **Impact of the Attack:** The consequences of Snake Keylogger attacks are substantial for both individual users and organizations. For individuals, stolen credentials can lead to identity theft, drained bank accounts, or compromised personal accounts.   **Consequences for Individual Users:**   1. **Identity Theft**: Stolen credentials can lead to unauthorized access to personal accounts, allowing attackers to commit identity theft. This may result in fraudulent activities such as applying for loans or credit cards in the victim’s name. 2. **Financial Loss**: Access to bank accounts or financial information can lead to drained accounts, unauthorized transactions, and significant financial loss. Victims may face long-term financial consequences if the stolen data is used for fraudulent transactions or sold on the dark web. 3. **Compromised Personal Accounts**: Personal accounts, such as email or social media profiles, can be misused, leading to privacy breaches, reputational damage, and further security risks.   For organizations, the consequences are even more severe. The theft of sensitive information, including intellectual property and employee credentials, can lead to data breaches, loss of reputation, and regulatory penalties.    **Consequences for Organizations:**   1. **Data Breaches**: The theft of sensitive organizational data, including customer information, intellectual property, and employee credentials, can lead to significant data breaches. These breaches can expose confidential information to unauthorized parties and compromise corporate secrets. 2. **Reputational Damage**: Organizations suffering from keylogger attacks can face severe reputational damage. Loss of customer trust and negative publicity can impact customer retention and brand image, affecting long-term business prospects. 3. **Regulatory Penalties**: Data breaches involving personal information may lead to regulatory penalties and legal consequences, especially if the organization fails to comply with data protection laws and regulations such as GDPR or CCPA. 4. **Operational Disruption**: If the attack spreads within the corporate network, it can compromise multiple systems and disrupt operations. This can lead to downtime, decreased productivity, and loss of business continuity.  **Preventive Measures:** Organizations can protect themselves and their employees against credential stealing malware in various ways. Some malware security best practices include the following:  1. **Employee Training:** Conduct cybersecurity awareness programs to help employees recognize and handle phishing attempts. 2. **Email Security Solutions:** Deploy email filters that detect and block malicious attachments and links to prevent initial infection. 3. **Endpoint Security**: Use endpoint protection software to detect and remove malware and to prevent keylogging and credential theft. 4. **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security, making it harder for attackers to access accounts even with stolen credentials. 5. **Zero Trust Security:** Adopt a zero trust model that enforces least privilege access, reducing the impact of compromised accounts and limiting potential damage. 6. **Regular Software Updates**: Ensure that all software, including operating systems and applications, are updated with the latest security patches. 7. **Network Segmentation**: Segment networks to limit the spread of malware and contain potential breaches within specific areas.   These measures help by improving awareness and defenses against keylogger attacks, preventing initial infections, and containing any potential breaches. They collectively enhance overall security, limit access, and reduce the impact of compromised credentials.   **Conclusion:** In conclusion, the Snake Keylogger represents a significant threat due to its sophisticated attack techniques and severe consequences for both individuals and organizations. Its ability to steal sensitive information through phishing and malware highlights the need for robust preventive measures.   By implementing comprehensive cybersecurity practices such as employee training, email security solutions, endpoint protection, and multi-factor authentication, organizations can mitigate the risks associated with keylogger attacks. |
| **References:** (in IEEE format) | [1] Fortinet, “Deep Analysis of Snake Keylogger: New Variant” Available:  <https://www.fortinet.com/blog/threat-research/deep-analysis-of-snake-keylogger-new-variant>  [2] Check Point, “What is Malware: Snake Keylogger Malware” Available: [https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/snake-keylogger-malware/.](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/snake-keylogger-malware/)    [3] Splunk, “Under the Hood of SnakeKeylogger: Analyzing its Loader and its Tactics, Techniques, and Procedures” Available: [https://www.splunk.com/en\_us/blog/security/under-the-hood-of-snakekeylogger-analyzing-its-loader-and-its-tactics-techniques-and-procedures.html.](https://www.splunk.com/en_us/blog/security/under-the-hood-of-snakekeylogger-analyzing-its-loader-and-its-tactics-techniques-and-procedures.html) |