**Report by**

**Cyber Guardians**

****

**Laboratory #3**

**Case study on Lenovo Superfish Adware -2022**

**Team members:**

1. **Basil Paul**
2. **Dharshana Boopathy**
3. **Litty Thomas John**
4. **Paul Jose**
5. **Ujunwa Dimejesi**

Table of Contents

[Executive Summary 2](#_Toc210644555)

[As-Was Analysis: Lenovo Superfish Adware Vulnerability 3](#_Toc1316791118)

[The As-Was Response: 3](#_Toc1582171169)

[Impact of the As-Was Scenario: 4](#_Toc1781800272)

[Types of MitM attacks 4](#_Toc1310458604)

[TO BE – Explore the lessons the client learned and how their cybersecurity structure differs today from before the incident. 5](#_Toc240184235)

[SWOT Analysis of the Preparation phase of Incident Response 6](#_Toc1942417408)

[Strengths: 6](#_Toc627366122)

[Weaknesses: 6](#_Toc836921064)

[Opportunities: 6](#_Toc451514487)

[Threats: 6](#_Toc877050956)

[Recommendations and Conclusions. 7](#_Toc673506111)

[References: 8](#_Toc1194086829)

# **Executive Summary**

This report delves into the critical cybersecurity incident involving the Lenovo-Superfish adware in 2015, offering insights into the **man-in-the-middle** attack vector it exploited. Commencing in September 2014, Lenovo PCs were equipped with pre-installed Superfish VisualDiscovery software, designed to intercept user web traffic for targeted advertisements (CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY [CISA], 2016, para. 2).

The adware implemented a classic man-in-the-middle attack by installing a trusted root Certificate Authority (CA) certificate, allowing it to intercept and decrypt encrypted connections (HTTP). The inherent risk lies in the fact that Superfish's CA-signed certificates masked the interception, rendering the browser incapable of displaying warnings about tampered web traffic. This vulnerability created a breeding ground for potential cyber-attacks, enabling attackers to generate certificates using Superfish's private key. Exploiting this, an attacker could intercept traffic on shared networks, like public Wi-Fi, and impersonate users, spoofing sensitive information such as email and banking details without triggering browser warnings (CISA, 2016, para. 2).

In response to the discovered vulnerability, Lenovo ceased pre-installing Superfish VisualDiscovery. However, existing systems with the software remained susceptible until users actively uninstalled it (CISA, 2016, para. 3).

This report emphasizes the severity of man-in-the-middle attacks and the nuanced vulnerabilities they exploit, as illustrated by the Superfish case study. Additionally, it provides recommendations for effectively countering such attacks.

# **As-Was Analysis: Lenovo Superfish Adware Vulnerability**

The As-Was analysis examines the Lenovo Superfish adware vulnerability as it existed during its discovery in 2015. This retrospective assessment aims to understand the situation, the impact, and the subsequent response during the incident.

1.Discovery of Superfish (2015):

* Superfish Visual Discovery, a pre-installed adware, was discovered on Lenovo consumer PCs.
* The adware's mechanism involved installing a non-unique trusted root CA certificate, enabling it to intercept HTTPS traffic.

2. MITM Exploitation:

* Superfish executed a classic man-in-the-middle (MITM) attack by intercepting encrypted connections, decrypting, and manipulating data, and re-encrypting it before reaching the user's browser.

3. Certificate Spoofing:

* The adware used its installed root CA certificate to generate fake certificates for any website. This meant that users were exposed to potential phishing sites without any browser warnings.

4. Detection Challenges:

* The deceptive nature of Superfish, coupled with the fact that the certificates were signed by the installed CA, made it challenging for users to detect the MITM attack.

5. Global Impact:

* The impact of Superfish was significant, affecting users globally as the adware was present on a substantial number of Lenovo PCs.

## **The As-Was Response:**

1. Public Outcry:

* Users expressed concerns over the privacy and security implications of Superfish's activities.

2. Acknowledgment by Lenovo (2015):

* Lenovo faced public backlash and admitted the security flaw, confirming the pre-installation of Superfish on their PCs.

3. Discontinuation of Pre-Installation (2015):

* Lenovo promptly ceased the practice of pre-installing Superfish on new PCs in response to the public outcry.

 4. Providing Uninstallation Tools (2016):

* Lenovo provided tools for users to uninstall Superfish and remove the associated root CA certificate from their systems.

## **Impact of the As-Was Scenario:**

* User Vulnerability: Users were exposed to potential security threats, including phishing attacks, due to the deceptive MITM activities of Superfish.
* Reputational Damage to Lenovo: The incident led to a significant dent in Lenovo's reputation, with users questioning the integrity and security of their devices.

# **Types of MitM attacks**

To gain access to devices and sensitive information, cybercriminals use the following ways to conduct MitM attacks:

1. Internet Protocol spoofing. Like identity theft, IP spoofing takes place when cybercriminals alter the source IP address of a website, email address or device for the purpose of masking it. This dupes the users into believing that they are interacting with a legit source and the sensitive information they share during the transaction gets transferred to the cybercriminals instead.
2. Domain Name System spoofing. This is a type of man-in-the-middle attack where cybercriminals alter domain names to redirect traffic to fake websites. Users might think that they are reaching a secure and trusted website, but instead, they land on a website operated by cybercriminals. The main aim behind DNS spoofing is to reroute traffic to a fake website or to capture user login credentials.
3. HTTP spoofing. The HTTP protocol is the embodiment of secure internet communications. HTTPS indicates a safe and trusted website. During an HTTPS spoofing attack, a browser session is redirected to an unsecured or HTTP-based website without the user's knowledge or consent. Cybercriminals can monitor user interactions and steal shared personal information through this redirection.
4. Secure Sockets Layer hijacking. SSL is a protocol that establishes an encrypted connection between a browser and the web server. During SSL hijacking, a cybercriminal might use another computer and a secure server to intercept all information traveling between the server and the end user's computer.
5. Email hijacking. This is a type of MitM attack where cybercriminals gain control of email accounts of banks and other financial institutions to monitor any transactions that users conduct. Cybercriminals may even spoof the bank's email address and send instructions to customers that lead them to unknowingly transfer their money to the cybercriminals.
6. Wi-Fi eavesdropping. This MitM attack is one of the many risk factors posed by public Wi-Fi. During this attack, public Wi-Fi users get tricked into connecting to malicious Wi-Fi networks and hotspots. Cybercriminals accomplish this by setting up Wi-Fi connections with names that resemble nearby businesses.
7. Session hijacking. Also known as stealing browser cookies, this malicious practice takes place when cybercriminals steal personal data and passwords stored inside the cookies of a user's browsing session. Sometimes, cybercriminals can gain endless access to users' saved resources. For example, they might steal users' confidential data and identities, purchase items or steal money from their bank accounts.
8. Cache poisoning. Also known as Address Resolution Protocol, or ARP cache poisoning, this popular modern-day MitM attack enables cybercriminals who are on the same subnet as the victims to eavesdrop on all traffic being routed between them.

# **TO BE – Explore the lessons the client learned and how their cybersecurity structure differs today from before the incident.**

* The Superfish incident underscored the risks associated with pre-installed third-party software, emphasizing the need for thorough vetting and security assessments.

To fix the Superfish issue, Lenovo offers a tool to uninstall the software and delete associated certificates. Remember, just uninstalling won't remove certificates. Microsoft has instructions on managing certificates in the Windows store to ensure thorough removal.

* Lack of user awareness and consent regarding Superfish raised concerns about transparency.

Now, they talk to users more clearly about pre-installed software. Users can choose what gets installed and know why during the setup.

* Before Superfish the interception of HTTPS traffic through SSL decryption raised serious security concerns.

After Superfish, they might have changed. They could have stricter rules against decrypting or inspecting encrypted traffic in their software to keep user data safe.

# **SWOT Analysis of the Preparation phase of Incident Response**

### Strengths:

**Global Presence:** Lenovo is a well-known global brand with a widespread customer base. This presence allows them to address issues globally but also poses a challenge due to the extensive impact of the incident.

**Responsive Action:** Lenovo took prompt action in discontinuing the pre-installation of Superfish and providing uninstallation tools. This responsiveness demonstrates a commitment to addressing security concerns.

### Weaknesses:

**Security Oversight:** The initial inclusion of Superfish highlights a weakness in Lenovo's security protocols and quality control processes. The oversight allowed a potentially harmful adware to be pre-installed on many PCs.

**Impact on Reputation:** The incident caused significant reputational damage to Lenovo, raising questions about the trustworthiness and security of their products. Rebuilding this trust becomes a crucial challenge.

### Opportunities:

**Enhanced Security Measures:** The incident presents an opportunity for Lenovo to strengthen its security measures and regain customer trust. Implementing robust security protocols can prevent similar incidents in the future.

**Improved Communication:** Lenovo can improve communication with its user base by being transparent about security measures, reassuring users, and regaining their confidence.

### Threats:

**Legal Consequences:** The adware's impact on user security might lead to legal challenges, including potential lawsuits. Lenovo faces the threat of legal consequences, which could result in financial losses.

**Competitive Disadvantage:** The reputational damage may give competitors an advantage in the market. Customers may turn to alternative brands that are perceived as more secure, impacting Lenovo's market share.

**Continued Security Concerns:** The incident may create a lasting perception of security concerns around Lenovo products, affecting sales and brand loyalty.

# **Recommendations and Conclusions.**

The Super fish malware posed a serious threat to the user’s privacy by actively listening https requests without them knowing.  This case highlights the importance of user’s knowledge about the preinstalled applications in the device and how do they process it. Also, it highlighted the encryption vulnerabilities and activities of adware’s. The main point to be noticed is the use of root CA certificate which can be exploited by attackers to gain sensitive information.  Below are the recommendations our team learned from this case study.

* Users should be clearly communicated about the preinstalled application and their security issues that have access to the user’s data by the vendors. Users must have the access to remove the unwanted programmes.
* Establish Clear Adware Policies: Develop and communicate clear policies regarding the use of ad-supported software within your organization. Ensure that employees understand the potential security risks associated with adware and the importance of obtaining approval before installing any software on company devices.
* Implement Network-Level Adware Blocking: Consider using network-level security solutions that can identify and block adware before it reaches individual devices. These solutions can help prevent the spread of adware across the network. Configure the best settings in browsers to block the adware.

To prevent the Man in Middle attacks organization should consider all the possible methods of eavesdropping and establish the defence that includes stronger encryption protocols, stronger authentication methods and regular security audits.

* Implementation of monitoring mechanism like IDS can help detect the breach in earlier stage.
* Ensure the usage of strong wi-fi protocols such as WPA2/WPA3 for the usage of Wi-fi. Avoid using public Wi-fi for financial transactions.
* Establish VPN connections which encrypt the transmission of data.
* Educate users about the usage of VPN and identification of the http websites.
* Always give importance to patch management to identify and remediate the vulnerabilities in the system.

# **References:**

*Lenovo Superfish Adware vulnerable to HTTPS spoofing | CISA*. (2015, February 20).

Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/newsevents/alerts/2015/02/20/lenovo-superfish-adware-vulnerable-https-spoofing>

*Lenovo Superfish Adware vulnerable to HTTPS spoofing | CISA*. (2016b, September 30).

Cybersecurity and Infrastructure Security Agency CISA.

<https://www.us-cert.gov/ncas/alerts/TA15-051A>

*CERT/CC Vulnerability Note VU#529496*. (n.d.). https://www.kb.cert.org/vuls/id/529496

[VU#529496 - Komodia Redirector with SSL Digestor fails to properly validate SSL and installs non-unique root CA certificates and private keys](https://www.kb.cert.org/vuls/id/529496)

*How to prevent a Man-in-the-Middle Attack*. (n.d.).

<https://www.byos.io/blog/how-to-prevent-man-in-the-middle-attack>

Rosenblatt, S. (2015, February 20). Lenovo’s Superfish security snafu blows up in its face.

*CNET*. [https://www.cnet.com/news/privacy/superfish-torments-lenovo-owners-with-more-](https://www.cnet.com/news/privacy/superfish-torments-lenovo-owners-with-more-than-adware/" \l "google_vignette.%20Accessed%203%20Feb.%202024.)

[than-adware/#google\_vignette.%20Accessed%203%20Feb.%202024.](https://www.cnet.com/news/privacy/superfish-torments-lenovo-owners-with-more-than-adware/" \l "google_vignette.%20Accessed%203%20Feb.%202024.)

Yasar, K., & Cobb, M. (2022, April 28). *man-in-the-middle attack (MitM)*. IoT Agenda. <https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM>