# **ASUS Live Update Attack (2019)**

### **1. Core Issue**

The ASUS Live Update attack, also known as **ShadowHammer**, was a sophisticated **software supply chain compromise**. Attackers infiltrated ASUS’ update servers and distributed a Trojanized version of the **ASUS Live Update Utility**, a legitimate tool pre-installed on ASUS laptops. The core issue was the **abuse of a trusted vendor’s update infrastructure**, where malicious binaries were signed with ASUS’ legitimate certificates, bypassing traditional trust mechanisms.

### **2. Who Was Attacked**

The direct victim was **ASUS**, a major global computer manufacturer. Attackers breached ASUS’ software update system, embedding malware into the official Live Update Utility distributed to customers worldwide.

### **3. Who Was Affected**

* Millions of ASUS laptop users received the compromised utility.
* However, the malware contained a **targeted backdoor**, designed to activate only on around **600 specific MAC addresses**.
* This indicated that the attackers were focused on espionage against carefully selected high-value individuals or organizations rather than mass exploitation.

### **4. Exploit Chain Details**

1. **Supply Chain Breach** – Attackers gained access to ASUS’ update servers.
2. **Malware Injection** – A Trojanized version of the Live Update Utility was created, digitally signed with ASUS’ certificate.
3. **Wide Distribution** – The malicious utility was delivered through official ASUS channels to millions of laptops.
4. **Conditional Activation** – The malware checked victims’ MAC addresses against a preconfigured list.
5. **Payload Delivery** – Only targeted machines received additional malicious payloads for espionage and surveillance.

### **5. Prevention / Protection Steps**

* **Harden Update Servers**: Isolate and monitor vendor-side update infrastructure.
* **Stronger Code Signing Practices**: Use Hardware Security Modules (HSMs) and certificate rotation policies.
* **Zero Trust Principles**: Do not implicitly trust vendor updates; validate binary behavior after installation.
* **Anomaly Detection**: Monitor for suspicious network activity from signed binaries.

### **6. Fixes & Vendor Response**

* ASUS released **clean versions of the Live Update Utility** and revoked compromised certificates.
* Security vendors such as Kaspersky and Symantec published detailed IoCs (Indicators of Compromise) to help detection.
* ASUS collaborated with customers to ensure patched utilities were widely distributed.

### **7. If No Fix Available**

* Temporarily disable the Live Update Utility.
* Manually install BIOS and driver updates from official sources.
* Monitor for any anomalous system behavior linked to known ShadowHammer indicators.

### **8. Reference Material**

* Kaspersky Securelist – Operation ShadowHammer:  
   https://securelist.com/operation-shadowhammer/89992/
* ASUS Security Advisory – ShadowHammer:  
   https://www.asus.com/support/faq/1042466
* CISA Alert (AA19-074A) – ASUS Live Update Utility Compromise:  
   https://www.cisa.gov/news-events/alerts/2019/03/15/aa19-074a-asus-live-update-utility-compromise
* Motherboard – ASUS ShadowHammer Supply Chain Attack Explained:  
   https://www.vice.com/en/article/mbz3yx/asus-shadowhammer-hack-explained
* Kaspersky Technical Analysis PDF:  
   https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/03/26144546/ShadowHammer\_report\_final.pdf

### **9. Further Reading**

* ENISA Threat Landscape for Supply Chain Attacks (2021):  
   https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
* MITRE ATT&CK – Supply Chain Compromise (T1195):  
   https://attack.mitre.org/techniques/T1195/
* OWASP Software Supply Chain Security Guide:  
   https://owasp.org/www-project-software-supply-chain-security/
* OpenSSF Best Practices for Securing Software Supply Chains:  
   https://openssf.org/working-groups/supply-chain-integrity/
* Kaspersky ICS CERT – ShadowHammer Deep Dive:  
   https://ics-cert.kaspersky.com/publications/reports/2019/03/26/operation-shadowhammer/

### **10. Tooling**

* Sigstore / Cosign – Open-source signing and verification for software artifacts:  
   https://sigstore.dev/
* in-toto – Framework for securing the integrity of software supply chains:  
   https://in-toto.io/
* YARA – Pattern matching tool for identifying malicious patterns in compromised updates:  
   https://virustotal.github.io/yara/
* Zeek – Network analysis platform to detect malicious update activity:  
   https://zeek.org/
* Microsoft Defender for Endpoint – Detects and blocks known ShadowHammer IOCs:  
  <https://www.microsoft.com/en-us/security/business/threat-protection/microsoft-defender-endpoint>
* VirusTotal – Analyze suspicious binaries:  
   https://www.virustotal.com/