# **ShadowPad / NetSarang Supply Chain Attack (2017)**

### **1. Core Issue**

The ShadowPad incident was a **supply chain compromise of enterprise software**. Attackers tampered with updates for **NetSarang’s server management software suite**, inserting a hidden backdoor. The malicious update appeared legitimate and was digitally signed, which meant enterprises installed it without suspicion. The attack revealed the critical risk of **silent compromise in widely used administrative tools**.

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

The immediate victim was **NetSarang Computer, Inc.**, a South Korea-based software company providing enterprise server administration tools. Its legitimate update packages were compromised and redistributed with a malicious backdoor.

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

* Large enterprises using NetSarang’s **Xmanager, Xshell, Xftp, and Xlpd** products.
* Victims spanned **financial institutions, energy providers, telecoms, and critical infrastructure operators** in multiple countries.
* Although globally distributed, early detection limited the number of actively exploited victims.

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

1. **Build System Breach** – Attackers gained access to NetSarang’s software update process.
2. **Backdoor Injection** – A covert backdoor, later named **ShadowPad**, was embedded into official updates released in July 2017.
3. **Trusted Distribution** – Customers downloaded and installed the updates, trusting the vendor’s signed binaries.
4. **Dormant Mode** – ShadowPad remained hidden, activating only if it received specific commands from C2 servers.
5. **Espionage Functionality** – Once triggered, it allowed attackers to exfiltrate files, steal credentials, and remotely control compromised systems.

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

* **Vendor Update Verification**: Cross-check vendor binaries using multi-vendor threat intelligence feeds.
* **Network Segmentation**: Restrict administrative tools’ access to sensitive systems.
* **Code Auditing & Build Security**: Vendors must implement reproducible builds and multi-party code reviews.
* **Threat Hunting**: Deploy behavioral monitoring to detect unusual DNS or network patterns.

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

* NetSarang released **clean, patched versions** of its software in August 2017.
* Kaspersky researchers published a detailed advisory and IoCs.
* C2 domains associated with ShadowPad were shut down.
* Customers were advised to reinstall software and rotate credentials immediately.

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

* Disconnect affected administrative software from the network.
* Use alternative secure tools until trusted updates are released.
* Conduct forensic analysis to confirm if backdoor activation occurred.

### **8. Reference Material**

* Kaspersky Securelist – ShadowPad: How Attackers Hide Backdoor in Software Used by Hundreds of Companies:  
   https://securelist.com/shadowpad-in-corporate-networks/81432/
* NetSarang Security Advisory – Backdoor Found in Software Updates:  
   https://netsarang.com/news/shadowpad-incident/
* CISA Alert – ShadowPad Backdoor in NetSarang Products:  
   https://www.cisa.gov/news-events/alerts/shadowpad-backdoor-netsarang-software
* Microsoft Security Intelligence – ShadowPad Campaign Insights:  
  <https://www.microsoft.com/security/blog/2017/08/17/understanding-the-shadowpad-backdoor/>
* FireEye Threat Research – Supply Chain Compromise via NetSarang:  
   https://www.fireeye.com/blog/threat-research/2017/08/hidden-backdoor-in-netsarang-software.html
* Kaspersky Technical PDF – ShadowPad Backdoor Details:  
   https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180155/ShadowPad\_backdoor\_analysis\_Kaspersky\_Lab.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 Build and Update Mechanisms:  
   https://openssf.org/working-groups/supply-chain-integrity/
* SANS Institute Analysis – Lessons from ShadowPad:  
   https://www.sans.org/blog/shadowpad-lessons-learned/

### **10. Tooling**

* Sigstore / Cosign – Signing and verification for software artifacts:  
   https://sigstore.dev/
* in-toto – Securing build and release pipelines:  
   https://in-toto.io/
* YARA – Detection of ShadowPad payload patterns:  
   https://virustotal.github.io/yara/
* Zeek – Network detection of backdoor C2 activity:  
   https://zeek.org/
* Microsoft Defender for Endpoint – ShadowPad threat detection:  
  <https://www.microsoft.com/en-us/security/business/threat-protection/microsoft-defender-endpoint>
* VirusTotal – Analysis of suspicious installer and update files:  
   https://www.virustotal.com/