Deloitte.

Supply Chain Cyberattacks

BEDC 2021

Contacts

Brett Henshilwood

Partner, Risk Advisory

E: Brett.Henshilwood@Deloitte.com

T: 441.299.1395

Contents

Supply Chain Cyberattacks

What are Supply Chain Cyberattacks?

A supply chain cyberattack refers to when a **malicious actor infiltrates an organization through vulnerabilities in the supply chain to infect their clients**.

Third-party vendors who have access to the organization's systems and data expose these vulnerabilities through poor security practices in their operations.

With just one well-placed intrusion, such attacks cause monumental damage once they gain access to hundreds or even thousands of networks.

When a supplier is compromised, their entire distribution network faces jeopardy from the attack, so that even software purchases or updates can be used as a means of deception

Common Attack Techniques

Hijacking updates

- Most modern software receives routine updates to address bugs and security issues. Software vendors typically distribute updates from centralized servers to customers as a routine part of product maintenance.

- Threat actors can hijack an update by infiltrating the vendor's network and either inserting malware into the outgoing update or altering the update to grant the threat actor control over the software's normal functionality.

- For example, the NotPetya attack occurred in 2017 when Russian hackers targeting Ukraine spread malware through tax accounting software popular in Ukraine. What would later be called the NotPetya malware spread well beyond Ukraine and caused major global disruptions in crucial industries, including

Common Attack Techniques

Undermining Codesigning

- Codesigning is used to validate the identity of the code's author and the integrity of the code. Attackers undermine codesigning by self-signing certificates, breaking signing systems, or exploiting misconfigured account access controls.

- By undermining codesigning, threat actors are able to successfully hijack software updates by impersonating a trusted vendor and inserting malicious code into an update.

- For example, APT 41, a China-based threat actor, routinely undermines codesigning while conducting sophisticated software supply chain compromises against the United States and other countries.

Common Attack Techniques

Compromising Open-Source Code

- Open-source code compromises occur when threat actors insert malicious code into publicly accessible code libraries, which unsuspecting developers—looking for free blocks of code to perform specific functions—then add into their own third-party code.

- For example, in 2018, researchers discovered 12 malicious Python libraries uploaded on the official Python Package Index (PyPI). The attacker used typosquatting tactics by creating libraries titled “diango,” “djago,” “dajngo,” etc., to lure developers seeking the popular “django” Python library.

- The malicious libraries contained the same code and functionality of those they impersonated; but they also contained additional functionality, including creating a backdoor for remote workstations.

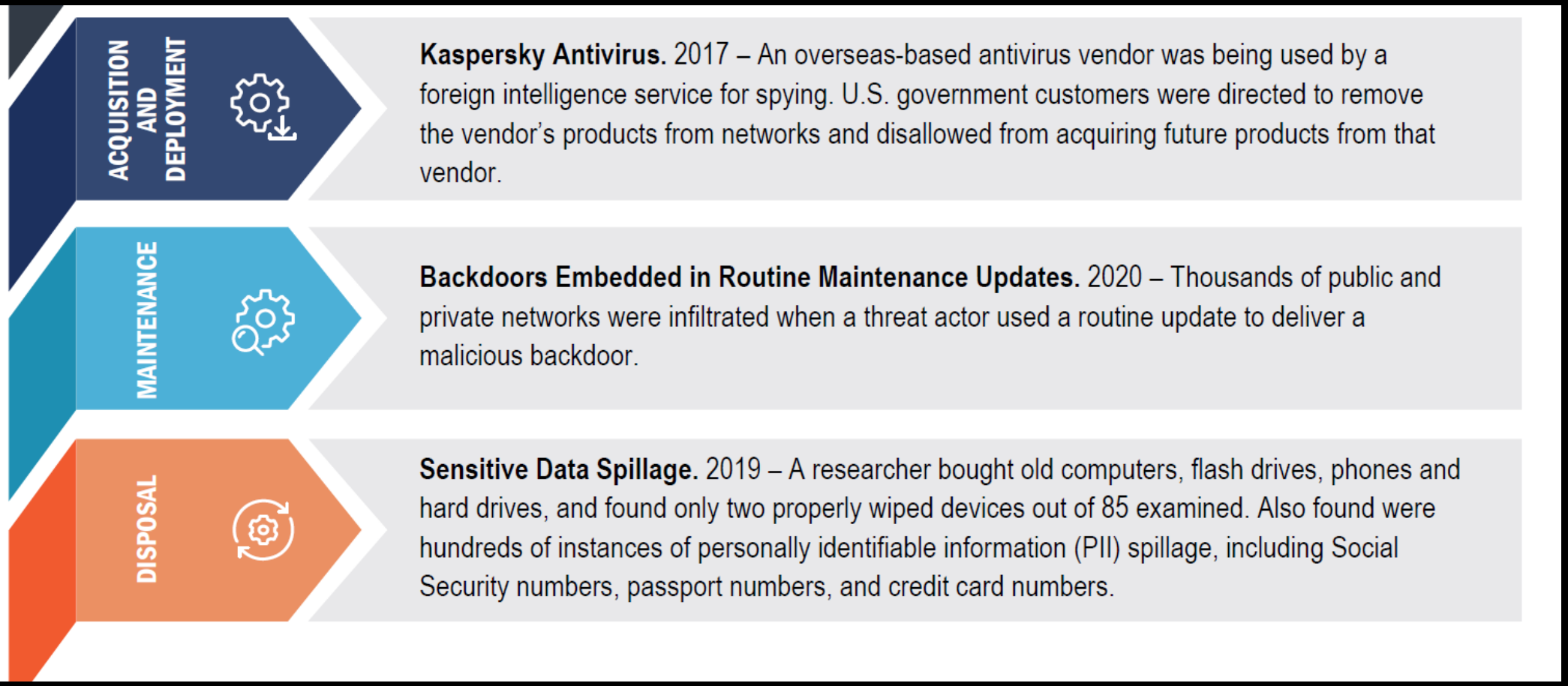
Examples of Recent Supply Chain Attacks

Hijacked Cellular Devices. 2016 – A foreign company designed software used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.

SolarWinds. 2020 – An IT management company was infiltrated by a foreign threat actor who maintained persistence in its network for months. The threat actor left the network only after it had compromised the company's build servers and used its update process to infiltrate customer networks.

End-User Device Malware. 2012 – Researchers from a major U.S. software company investigating counterfeit software found malware preinstalled on 20 percent of devices they tested. The malware was installed in new desktop and laptop computers after they were shipped from a factory to a distributor, transporter, or reseller.

Examples of Recent Supply Chain Attacks



Kaspersky Antivirus. 2017 – An overseas-based antivirus vendor was being used by a foreign intelligence service for spying. U.S. government customers were directed to remove the vendor's products from networks and disallowed from acquiring future products from that vendor.

Backdoors Embedded in Routine Maintenance Updates. 2020 – Thousands of public and private networks were infiltrated when a threat actor used a routine update to deliver a malicious backdoor.

Sensitive Data Spillage. 2019 – A researcher bought old computers, flash drives, phones and hard drives, and found only two properly wiped devices out of 85 examined. Also found were hundreds of instances of personally identifiable information (PII) spillage, including Social Security numbers, passport numbers, and credit card numbers.

What are the impacts Supply Chain Cyberattacks ?

Data leaks

Data leaks refer to **sensitive data that's exposed outside of an organization into an untrusted environment**. In 2013, one of the largest data leaks in the retail industry happened to US retailer Target Corp. Hackers infiltrated a third-party vendor Fazio Mechanical Services—their heating, ventilation, and air conditioning (HVAC) supplier—with malicious code to steal customer credit card data. This breach resulted in hackers stealing 40 million credit and debit cards details and Target settling about $18 million in claims.

Security breaches

A *security breach* occurs when a hacker gets **unauthorized access to an operating system, network, computer, applications, or devices by bypassing security mechanisms**. It usually leads to tampering with the system data by deletion, corruption, or replication. Essentially, it's a break-in. In 2018, Facebook experienced a security breach when hackers gained the access tokens of 30 million Facebook users.

What are the impacts Supply Chain Cyberattacks ?

Malware attack

A *malware attack* occurs when **malicious software (malware) runs unauthorized actions on a system**. This type of attack is usually carried out to exfiltrate sensitive information, disrupt operations, or demand a payment. Malware can occur as one of three types:

- **Trojan horse**, which gains access through a back door
- **Worm**, which propagates itself into other systems
- **Virus**, which can infect a system

In just the first half of 2021, several companies have already experienced some mighty hefty demands from malware attacks.

Phishing

Phishing is based on **fraudulent messages disguised by popular brand names to trick humans into taking actions** that force them to **reveal private, personal information such as user IDs, passwords, and account details**. These messages can come as emails, text or SMS messages, and voice messages. No one is immune to phishing—not even some of the biggest tech. companies—as **human error is the biggest cause of all phishing attacks.**

Best Practices to Counter Supply Chain Attacks

Risk-level assessment

- Understand your entire environment
- Can’t treat all vendors the same
- Identify those that are more crucial to your operations
- Focus efforts on those of higher risk

Best Practices to Counter Supply Chain Attacks

Use of unverified or disreputable suppliers

For some companies, protecting their supply chain is as simple as requiring suppliers to sign off on a checklist. They base their vendor relationship—and relationship with their vendors' vendors—on a game of trust. **Without vetting their supply chain, companies take on enormous risk with this game of trust** because these vendors can have access to all the information systems of the company.

To avoid taking a gamble on your suppliers, **choose reputable companies that you can vet and verify their business practices.** Confirm they have protections in place to secure their systems and data, including how they are accessed and used. Your vendors must be both transparent and trustworthy.

Best Practices to Counter Supply Chain Attacks

Lack of cybersecurity awareness training for employees

A company's employees are the first line of defense against a cyberattack. When employees don't have regular access to effective cybersecurity awareness training, they are vulnerable to an attack and unprepared to know how to handle it.

Starting with your own company, make sure employees at all levels **receive regular cybersecurity awareness training** so they know how to deal with sensitive data and recognize a potential attack. Also, ensure your suppliers give their employees regular cybersecurity awareness training to keep more protective eyes on your supply chain.

Best Practices to Counter Supply Chain Attacks

Weak supply chain risk management

- **Create a supply chain risk management team** to take on the following responsibilities:
  - **Analyze your current vendors** and set a baseline.
  - Critically **analyze the vulnerability of the supply chain** to determine which level is the weakest and could serve as an entry point for a malicious attack.
  - **Plan for all threat scenarios** and their impact on the organization.
  - **Gather and analyze all findings** to determine the organization's risk for a cyberattack and **prepare a plan of action** to respond to that risk.

Don’t Forget the Basic’s

- Excess access privileged rights to vendors, consultants, employees, etc.
- Never us one account for all IT staff, vendors, consultants, etc.
- Make sure you assess a Vendor’s Security Posture
- Keep patching of operating systems, applications and hardware up to date
- Test systems after configuration changes or deployment of changes
- Train staff and pursue a positive cybersecurity culture
- Monitor logs for possible threats
- Secure data in transit and at rest.

Deloitte.