XPOSE SECURITY

CASE STUDY

Supply Chain Attack Simulation

How We Expose Hidden Vulnerabilities Across Your Vendor Ecosystem

TARGET	DURATION	ATTACK TYPE	OUTCOME
Logistics & Manufacturing	**4 Weeks**	**360° Supply Chain**	**Full Compromise Path**

www.xposesecurity.com · Belgium & New York

01 - EXECUTIVE SUMMARY

The Threat Your Perimeter Can't See

Your firewall is hardened. Your internal network is segmented. Your SOC monitors 24/7. But how secure are the 40 vendors, suppliers, and SaaS platforms with a trusted connection into your environment?

Supply chain attacks have become the preferred entry point for nation-state actors and ransomware groups precisely because they bypass the security investments organizations make in their own perimeter. The attacker doesn't need to break through your door - they walk in through a trusted partner who already has the keys.

XPOSE Security's Supply Chain Attack Simulation answers one question: if a sophisticated threat actor compromised one of your vendors today, how far could they go?

The SolarWinds Lesson

Over 18,000 organizations - including Fortune 500 companies and US federal agencies - were compromised through a single trusted software vendor. The attackers didn't need to attack each target individually. They attacked once, at the supply chain level, and gained simultaneous access to thousands of environments. XPOSE replicates this exact threat model against your organization.

In this engagement, a fictitious logistics company ("CompanyX") commissioned XPOSE Security to simulate a full supply chain attack across their vendor ecosystem. Within four weeks, our team had identified a complete compromise path from a third-party software provider to CompanyX's domain controllers - without triggering a single alert.

KEY OUTCOMES

6	1	0	14
Critical vendor misconfigurations identified	Full domain compromise path demonstrated	Security alerts triggered during engagement	Days to achieve initial foothold via vendor

02 - WHAT WE TEST

The Supply Chain Attack Surface

A supply chain attack occurs when an adversary targets your organization by first compromising a less-secure entity in your trusted ecosystem. Modern organizations maintain dozens - sometimes hundreds - of active trust relationships that create exploitable pathways into their environment.

The Four Attack Vectors We Simulate

1. Software & SaaS Vendor Compromise

Targeting third-party software deployed in your environment - from ERP platforms and monitoring agents to DevOps tooling and security software. We assess whether a compromise of the vendor's build pipeline, update mechanism, or SaaS infrastructure could result in code execution or data access within your organization.

2. Managed Service Provider (MSP) Lateral Movement

MSPs and IT outsourcing partners typically hold privileged access - domain admin credentials, RMM agent installations, VPN certificates - across every client they manage. We simulate what happens when an MSP is compromised and test whether that access can be used to pivot into your environment undetected.

3. Physical & Logistics Partner Infiltration

For logistics and manufacturing clients, we assess whether supplier access to internal portals, logistics systems, and operational technology (OT) networks can be exploited. This includes badge access systems, supplier onboarding portals, and EDI integrations that connect directly to production environments.

4. Open Source & Dependency Poisoning

We analyze internal development pipelines for dependency confusion vulnerabilities, typosquatting exposure, and the use of unmaintained or compromised open-source packages. A single malicious npm or PyPI package pulled into a CI/CD pipeline can give attackers persistent access to your entire build environment.

Why Traditional Pentests Miss This

Standard penetration tests focus on your perimeter. They assess what an external attacker can reach from the internet. They don't test the trust relationships you've already granted to third parties - which means they leave the most dangerous attack surface completely unmapped.

XPOSE Supply Chain Simulations operate from the perspective of a vendor or supplier who already has a trusted foothold. We start where the attacker starts: inside the trusted zone.

03 - METHODOLOGY

How XPOSE Tests Your Supply Chain

Our supply chain assessment follows a structured four-phase methodology aligned with MITRE ATT&CK. Every phase produces concrete evidence - not theoretical findings - before proceeding to the next.

PHASE	ACTIVITY	OBJECTIVE	KEY FINDING TYPE
Phase 1	Vendor Ecosystem Mapping	Identify all third-party trust relationships, access grants, and integration points	Attack surface inventory
Phase 2	Vendor Targeting & Reconnaissance	Identify the weakest link in the vendor ecosystem as a realistic attacker would	Initial access vector
Phase 3	Simulated Compromise & Lateral Movement	Demonstrate exploitation from vendor foothold to target environment	Privilege escalation path
Phase 4	Crown Jewel Access & Impact Proof	Reach defined target objectives (DC, data exfiltration, OT access)	Business impact evidence

Phase 1: Vendor Ecosystem Mapping

Before attacking, we build a complete map of your supply chain exposure. This is intelligence an attacker would spend weeks gathering through OSINT - we do it in collaboration with your team to accelerate the engagement.

We identify and categorize every vendor with a trust relationship into your environment, including:

- Software vendors with agents, sensors, or integrations deployed in your infrastructure
- SaaS platforms with SSO or OAuth access to your identity provider
- Managed service providers with RMM agents or privileged access
- Logistics and operational partners with access to internal portals or OT systems
- Development tools with access to your CI/CD pipeline and code repositories

Each vendor is scored by access level, detection difficulty, and public vulnerability surface to identify the highest-value attack entry points.

Phase 2: Vendor Targeting & Reconnaissance

We select the three to five highest-risk vendors and conduct external reconnaissance: exposed admin panels, leaked credentials on dark web sources, unpatched known vulnerabilities, and weak authentication configurations. We are not simulating what could happen - we are finding what would actually work.

Real-World Finding: CompanyX Engagement

During reconnaissance on a logistics software vendor used by CompanyX, our team identified an exposed Swagger API documentation portal with test credentials embedded in the documentation. Those credentials provided authenticated API access to a staging environment that shared database infrastructure with production.

Phase 3: Simulated Compromise & Lateral Movement

With an established foothold in the vendor's environment or via their trusted access vector, we execute lateral movement toward the target. This phase follows the MITRE ATT&CK kill chain and documents every technique used - including evasion methods that bypass your existing detection tools.

Typical lateral movement techniques in supply chain scenarios include:

- Abusing RMM agent privileges to execute commands on managed endpoints
- Extracting API tokens and OAuth credentials from vendor management consoles
- Exploiting implicit trust in signed software update packages
- Pivoting through VPN tunnels established for vendor support access
- Leveraging shared Active Directory trusts between vendor and client environments

Phase 4: Crown Jewel Access

The engagement concludes by reaching pre-agreed target objectives that demonstrate real business impact. We don't stop at initial access or a foothold on a single workstation. We demonstrate the full blast radius.

Target objectives are defined in scope during kickoff and typically include domain controller access, access to financial or operational data, the ability to deploy ransomware, or disruption of OT/production systems.

04 - SAMPLE FINDINGS

What We Found: CompanyX Engagement

The following represents a representative sample of findings from a four-week supply chain engagement in the logistics sector. All client details have been anonymized.

FINDING	SEVERITY	ATTACK PATH
RMM Agent with Domain Admin Credentials	CRITICAL	MSP RMM console compromise → credential extraction → domain controller via pass-the-hash
Logistics Portal with Implicit Vendor Trust	CRITICAL	Supplier credential phishing → portal access → OT network lateral movement via trusted VLAN
Exposed Vendor API with Hardcoded Test Credentials	HIGH	OSINT discovery → API authentication → database query for production credentials
SaaS OAuth Token with Excessive Permissions	HIGH	SaaS vendor breach scenario → OAuth token theft → M365 mailbox and SharePoint access
Unsigned Software Update Mechanism	HIGH	Vendor build pipeline compromise → malicious update deployment → code execution on 240 endpoints
Dependency Confusion in Internal npm Registry	MEDIUM	Malicious public package → CI/CD pipeline execution → environment variable exfiltration

Complete Compromise Path: Domain Controllers Reached in 14 Days

Starting from the MSP's RMM console - which had been misconfigured with a domain admin service account - our team extracted cached credentials during a simulated operator session. Those credentials were valid across the client environment due to shared Active Directory infrastructure. From initial vendor access to domain controller takeover: 14 days. Alerts triggered: zero.

Detection Evasion: Why Your SOC Didn't See It

A critical component of every XPOSE engagement is understanding not just what vulnerabilities exist, but why your existing detection stack missed them. In the CompanyX engagement, our team remained undetected for the full duration for three reasons:

- Vendor access was treated as implicitly trusted - no behavioral baseline existed for what "normal" RMM agent activity looked like
- Lateral movement occurred through legitimate management channels, not malware or exploits that EDR solutions would flag

- Credential use for the compromised service account matched normal working hours and geographic origin of the MSP

This is exactly the pattern that APT groups exploit. The attack looks like legitimate vendor activity until it's too late.

05 - RANSOMWARE SIMULATION & APT-GRADE TESTING

The Full Attack: From Vendor to Ransom Note

Supply chain access is not the end goal for sophisticated threat actors - it is the entry point. Once inside through a trusted vendor, the most dangerous adversaries move toward two outcomes: ransomware deployment or long-term persistent access. XPOSE simulates both, starting from the vendor foothold established in the supply chain assessment.

Why Ransomware Groups Target Supply Chains

Groups like LockBit, BlackCat (ALPHV), and Cl0p have deliberately shifted to supply chain initial access because it scales. Compromise one MSP, one logistics software vendor, one monitoring agent - and you have simultaneous access to dozens of organizations. The 2023 MOVEit campaign exploited a single file transfer vendor and compromised over 2,700 organizations in weeks. XPOSE replicates this exact playbook against your environment.

Phase 1: Establishing a Beachhead

Starting from the vendor access vector identified in the supply chain assessment, our operators establish a persistent foothold using techniques that mirror real ransomware affiliate tradecraft. This is not a scanner finding a CVE - this is a human operator executing a deliberate, multi-step intrusion.

Initial foothold techniques used in XPOSE engagements include:

- Living-off-the-land binaries (LOLBins): using legitimate Windows tools - certutil, mshta, wscript, PowerShell with AMSI bypass - to avoid triggering EDR detections based on malware signatures
- Custom C2 infrastructure: operator-controlled command-and-control servers with domain fronting, HTTPS beaconing over legitimate cloud providers, and randomized jitter intervals to evade behavioral detection
- Process injection and hollowing: injecting shellcode into trusted processes such as svchost, explorer, or Microsoft-signed binaries to blend with normal system activity
- Scheduled tasks and service hijacking: establishing persistence mechanisms that survive reboots and look identical to legitimate administrative configurations

Phase 2: Credential Harvesting & Privilege Escalation

Ransomware actors do not deploy encryption immediately after gaining access. They spend days to weeks escalating privileges and harvesting credentials before making any visible move. XPOSE replicates this patience - because it is what makes real attacks so devastating.

LSASS Memory Dumping	Extraction of plaintext credentials and NTLM hashes from active Windows sessions - the foundation of lateral movement in most ransomware incidents
Kerberoasting	Offline cracking of service account ticket hashes to obtain domain-level credentials without touching a domain controller
DCSync Attack	Replicating the domain controller's credential database using legitimate AD replication protocols - indistinguishable from normal DC-to-DC communication
Token Impersonation	Stealing authentication tokens from privileged processes to escalate from local admin to SYSTEM or domain admin without credential theft
AS-REP Roasting	Targeting accounts with Kerberos pre-authentication disabled to extract crackable hashes without any network authentication

Phase 3: Lateral Movement & Domain Dominance

With domain credentials secured, our operators move laterally across the network using techniques that real ransomware affiliates execute during the pre-deployment phase. The objective is not just to reach the domain controller - it is to reach every target that a ransomware actor would need to encrypt, destroy, or exfiltrate before deploying.

- Pass-the-Hash and Pass-the-Ticket: authenticating to remote systems using harvested credential material without knowing plaintext passwords
- WMI and PsExec execution: remotely executing commands on target hosts using legitimate Windows management protocols that generate minimal suspicious log activity
- Active Directory enumeration: mapping all high-value targets - backup servers, domain controllers, financial systems, file servers - to build a complete pre-encryption target list
- Backup system identification and access: locating and validating access to backup infrastructure, shadow copies, and disaster recovery systems - the primary target of every serious ransomware deployment
- EDR and security tool mapping: identifying the organization's detection stack and testing whether lateral movement techniques trigger alerts before proceeding to the final phase

Critical Test: Can Your Backups Be Destroyed?

The defining question in any ransomware readiness assessment is not whether attackers can encrypt your production data - they can. The question is whether they can simultaneously destroy your ability to recover. XPOSE validates whether domain admin access translates to access to your backup infrastructure, and whether backup deletion or encryption is technically possible within the scope of the engagement. Organizations that fail this test have no viable recovery path in a real incident.

Phase 4: Data Exfiltration Simulation

Modern ransomware groups operate double-extortion models: they encrypt your data AND exfiltrate it, threatening public release if the ransom is not paid. XPOSE simulates the exfiltration phase to validate whether your DLP controls, network monitoring, and egress filtering would detect or block a real data theft operation.

Exfiltration techniques tested include DNS tunneling through legitimate resolvers, HTTPS data upload to operator-controlled cloud storage infrastructure, staged exfiltration using encrypted archives to avoid content inspection, and abuse of legitimate cloud sync tools already installed in the environment.

We define a set of simulated crown jewels - representative sensitive files - and validate whether exfiltration of those files would be detected, logged, or blocked by existing controls.

Phase 5: Ransomware Deployment Simulation

The final phase simulates the deployment decision point - the moment a ransomware actor would trigger encryption across the environment. XPOSE does not deploy actual encryption. Instead, we demonstrate technical readiness: we prove that from the access we have obtained, encryption could be deployed across all identified targets simultaneously.

What "Deployment Simulation" Means in Practice

XPOSE demonstrates ransomware deployment readiness through: (1) group policy object modification to push a harmless marker file to all domain-joined endpoints - proving GPO-based ransomware delivery is viable; (2) remote service creation on domain controllers to demonstrate SYSTEM-level code execution capability; (3) shadow copy deletion verification on a designated test system to confirm VSS destruction is possible without production impact. Every action is pre-agreed with the client and executed in a controlled, reversible manner.

The APT Simulation: Long-Term Persistent Access

Not every threat actor wants to deploy ransomware. Nation-state actors, industrial espionage groups, and advanced persistent threat actors want something more valuable: invisible, long-term access to your environment. The XPOSE APT simulation extends the supply chain engagement to test your organization's ability to detect an adversary who is actively trying not to be found.

PHASE	ACTIVITY	OBJECTIVE	KEY FINDING TYPE
Week 1-2	Initial Access & Quiet Persistence	Establish foothold via vendor vector, deploy persistent implant using signed binary	Persistence mechanism viability

		sideloading or COM hijacking	
Week 2-3	Low-and-Slow Reconnaissance	Map internal environment using only legitimate tools and protocols - no port scanners, no known-bad signatures	Detection blind spots
Week 3-4	Credential Accumulation	Harvest credentials through passive techniques: keylogging on targeted systems, monitoring LSASS remotely, abusing legitimate sync protocols	Credential exposure surface
Week 4-5	Objective Achievement	Reach defined high-value targets: IP repositories, M&A documentation, strategic planning data, OT control systems	Crown jewel accessibility
Week 5-6	Detection Assessment	Determine if any activity was flagged, investigated, or escalated during the engagement - and why or why not	SOC & detection gap report

APT Techniques: What We Use

XPOSE APT simulations use the same techniques documented in MITRE ATT&CK as being actively used by groups including APT29 (Cozy Bear), APT41, Lazarus Group, and Sandworm. This is not theoretical mapping - these are the specific techniques our operators execute.

- Custom implants with encrypted C2 communications using domain fronting through legitimate CDN providers - technique used by APT29 in the SolarWinds campaign
- DLL sideloading through Microsoft-signed executables to achieve persistent code execution that survives EDR scans and application whitelisting
- Timestomping and log manipulation to alter forensic artifacts and complicate incident response timelines
- Living-off-the-land PowerShell execution with AMSI bypass to harvest credentials and enumerate Active Directory without dropping files to disk
- Steganographic data exfiltration embedding sensitive data in legitimate image uploads to cloud storage services

– Golden and Silver Ticket attacks to forge Kerberos authentication tickets providing persistent domain access that survives password resets

Detection Challenge: The 194-Day Average

IBM's Cost of a Data Breach Report consistently shows organizations take an average of 194 days to detect an active intrusion. XPOSE APT simulations run for six weeks with operators actively avoiding detection. At the end of the engagement, we conduct a full retrospective with your SOC team: every action we took, every technique we used, and exactly which of them - if any - appeared in your logs. For most organizations, the answer is sobering.

06 - WHAT YOU RECEIVE

Deliverables & Engagement Model

What XPOSE Delivers

Executive Report	Board-ready summary: what was compromised, the business impact, and the three highest-priority actions. No technical jargon.
Technical Report	Full attack chain documentation with evidence, MITRE ATT&CK TTP mapping, proof-of-concept demonstrations, and step-by-step remediation guidance.
Vendor Risk Register	Scored inventory of every third-party trust relationship, ranked by attack viability and business impact.
Detection Gap Analysis	A precise map of where your SOC and EDR failed to detect our activity, with detection engineering recommendations.
Remediation Roadmap	Prioritized action plan organized by risk level and implementation effort - not a generic checklist.
Debrief Sessions	Separate technical debrief for your security team and executive debrief for leadership and the board.

Engagement Scope Options

Supply chain assessments are scoped based on the size of your vendor ecosystem and the depth of testing required. Typical engagements range from four to twelve weeks.

Focused Assessment	Full Supply Chain Simulation	APT-Grade Red Team
2-3 vendors, targeted scope 4 weeks	Full vendor ecosystem 6-8 weeks	Nation-state simulation 8-12 weeks

Who This Engagement Is For

Supply chain simulations are designed for organizations that have already addressed baseline security hygiene and are ready to test their real-world resilience against sophisticated, multi-vector attacks. Ideal candidates include:

– Logistics and manufacturing companies with operational technology (OT) networks

- Financial institutions with large vendor and integration ecosystems
- Organizations subject to NIS2, DORA, or TIBER-EU requirements
- Companies that have experienced a vendor-related incident and want to understand the full exposure
- Boards and leadership teams that want evidence - not assurances - about supply chain resilience

07 - WHY XPOSE

Security Is Proven When Real Attackers Fail

Compliance audits tell you what should be in place. XPOSE tells you what actually fails under attack.

Our team has executed supply chain simulations and red team engagements for organizations including Euroclear, Digitaal Vlaanderen, FOD Justitie, KBC Group, and the Belgian Prime Minister's Office. We operate at the same technical level as the threat actors targeting your organization - because understanding how attackers think is the only way to expose what they would actually exploit.

Reference Clients

Euroclear · KBC Group · Digitaal Vlaanderen · FOD Justitie · Kanselarij van de Eerste Minister · Arvesta · Starbucks

Ready to Map Your Supply Chain Exposure?

Contact XPOSE Security to schedule a scoping call. We'll identify the highest-risk vendor relationships in your ecosystem and define an engagement scope that delivers maximum intelligence about your real-world supply chain resilience.

XPOSE Security

Belgium · New York

www.xposesecurity.com

Start Your Engagement

info@xposesecurity.com

Schedule a scoping call today