Deloitte.

SolarWinds insights and actions

When will your prevention, detection, and response efforts be enough?

SolarWinds is set to be one of the most prolific cyber attacks in recent history due to its magnitude, methods of attack, and sophisticated obfuscation. Such tactics, techniques, and procedures (TTPs) allowed attackers to evade even the most mature cyber defenses, going undetected for months. As impacts from this event continue to unfold, leaders should consider programmatic changes as attacks such as this grow in prevalence and sophistication.

This attack has demonstrated that motivated threat actors are able to breach even the most secure networks and systems, leading fatigued organizations to ask, "Will our cyber efforts ever be enough?". Cyber attacks call into question an organization's ability to trust not only its cyber defenses, supply chains, and partners, but also its ability to respond effectively. When trust is a cornerstone of business operations and a strategic imperative, security decisions and efforts impact productivity, revenue, and broader organizational value. The standard of care attributed to these programs can define an organization's ability to weather future cyber storms.

A new precedent in supply chain attacks

What we know about the attack

- A supply chain attack likely executed by a nation state actor[1]
- SolarWinds customers who downloaded the Orion platform update with malware are at risk of attack[1]
  - Not everyone who downloaded the update was targeted/successfully breached but may be at risk
  - Attack primarily targeted intel gathering from government agencies and IT providers, implying that likely only a small portion of those who downloaded the update were breached
  - There have been demonstrated instances of attackers observing sensitive intellectual property and IT tools, but with only mixed success in theft attempts

What makes this breach noteworthy?

- Access likely was through manipulated accounts and deconstructed log files
- Attacks leveraged strong obfuscation in memory, enabling attackers to avoid detection and experience significant dwell time before discovery
- Attackers installed malicious code into a legitimate library running outside expected system processes
- The malware is thought to have been propagated with a patch and likely leveraged trusted code injection points
- The breadth and magnitude of the attack highlights strong interconnectivity between organizations across the public and private sectors and throughout their physical and virtual supply chains

Ongoing security challenges in the wake of the SolarWinds attack

Underperformance by baseline tools/monitoring of privileged access and user and entity behavioral analysis (UEBA) tools	Difficulties understanding impact exposure given extensive ecosystem relationships and complex infrastructure
Persistence of advanced threats requires enhanced monitoring—while many cyber security teams are already strained	Artificial Intelligence (AI)-enabled tools have allowed automation of security tasks but are often assumed to be secure without appropriate review
Confusion over contractual obligations and communications needed after breach	Struggles by (even advanced) monitoring tools to detect sophisticated obfuscation attacks
Lack of faith/trust in vulnerability and patch management	Delays and increased risk caused by insufficiently coordinated information technology silos
Lack of understanding of software supply chain, third, fourth & Nth parties, and what access they have to data, systems and networks	Preparing for unknown unknowns and employing strong risk mitigation to achieve long-term cyber resilience

[1]"Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)." Cybersecurity and Infrastructure Security Agency CISA, January 5, 2021. https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

Improve future resilience with layered response tactics

NOW: *Understand if you have likely been compromised - if you haven't done so already*

- ✓ **Determine if you have impacted version of SolarWinds platform** (versions 2019.4 through 2020.2.1 HF1)
  - Create a comprehensive asset and component inventory
- ✓ **Review privileged access management (PAM) program** (e.g., Secure username and group policies, especially for privileged accounts that may have been hijacked or compromised)
  - Evaluate changes to privileged accounts, including new privileged accounts / logs dating back to the beginning of the attack window – at a minimum the date of patch download
- ✓ **Review and analyze endpoints and network traffic** for anomalous activity that may indicate additional/lateral access as a result of extended network presence
- ✓ **Patch and remediate** identified vulnerabilities, but **assume adversary may have additional footholds** beyond the reported event
  - Search for the **presence of the injected class of malicious code** and search for **named pipes**
  - Engage in **threat hunting** activities for non-known Indicators of Compromise (IoCs)
  - Proactively review **networking infrastructure** to ensure there are no significant changes (including exfiltration of data)
- ✓ **Review and follow strategic risk plan** to coordinate stakeholder/client notification and manage public relations inquiries (establish intake capability)
  - Review agreements with vendors regarding remediation obligations and your existing cyber insurance policies

NEXT: *Take proactive steps to enhance your cyber posture in the short term*

- ✓ Assess overall **risk profile** and **risk appetite**
- ✓ **Assess organizational supply chain connections and software**
  - **Communicate with supply chain partners** to share information on compromised, shared assets
  - Review supply chain processes for the acquisition of software and hardware used for **critical infrastructure**
  - Determine other **systems or data that external parties may have access to** in direct or indirect business relationships
  - Incorporate **risk profile** considerations to procurement and supplier risk management polices and practices
- ✓ Review legal playbooks and respond **to litigation requests**
- ✓ Update **incident response strategy** considering legal requirements and how digital forensics processes can support
- ✓ Confirm **incident readiness and test back-ups** to prepare for future disruptions, including requirements to isolate critical applications or systems
- ✓ Review **vulnerability management** processes
  - Testing of patches to presume compromise, include sandbox detonation
- ✓ Evaluate **software development life cycle (SDLC) security procedures** and implement stop gaps
  - Use PAM to "check out" builds
  - Leverage platform native controls
- ✓ **Don't let your guard down-assume sustained risk** of latent threats
  - Perform proactive threat hunting, red teams, as well as heightened monitoring practices

LATER: *Pursue strategic, programmatic upgrades for long term resiliency*

- ✓ Enforce stronger **data management, governance and hygiene** to better insulate from future incidents
- ✓ Leverage **big data analytics** and **security orchestration** to establish strong baselines and derive insights from captured security data
- ✓ **Reinvigorate security logging program** to improve incident response activities and remediate gaps in coverage
  - 30/60/90-day archives aren't sufficient
- ✓ **Revisit development and supply chain processes**
  - Adopt DevSecOps across the enterprise (e.g., small, frequent code releases) that facilitate ability to identify code changes including insertion of malicious code or backdoors
  - Evaluate integrity of development processes, including reliance on third-party and open-source code bases
- ✓ Consider methods of cross-business, cross-industry **information / threat intelligence sharing** to enable better preparation and response
- ✓ Consider **organizational adoption of Zero Trust**
  - Institute robust safeguards across domains by resisting trust for every transaction or action, even if they are recurrent activities, even if they are only internal
  - Heightened credential/lateral movement monitoring, ongoing threat hunting, and network segmentation
- ✓ Establish a **mature risk management process** that uses near real time data to manage, execute and enforce against risk thresholds and maintain/improve risk profile
- ✓ Implement continuous **attack surface illumination and discovery,** and expanded ecosystem risk monitoring

While these actions are valuable, even the strongest cyber defenses may not prevent future attacks – **incident response, recovery, and resilience efforts are critical to protect your business.**

Lessons learned

Organizations should prepare for a future in which similar attacks are increasingly common. Organizations that place a vigorous emphasis on embedding **cyber + trust** "designed into" their business practices may be better poised to be resilient to relentless adversaries, strengthen relationships with customers, partners, and employees;, and reduce distractions to focus on the mission—proactively anticipating these challenges, while at the same time being nimble and resilient to a range of potentially disruptive scenarios.

Recognize your risk is unique: Your cyber and risk practices should correlate to your individual risk profile and appetite

Understand your business ecosystem: Know who you're in business with and recognize that their security and the security of their vendors may impact your organization

Adopt a Zero Trust mindset: Assume a breach is possible, verify every user, transaction or request and do not presume trust

Pioneer security by design: Embed security into the SDLC from code design to production with DevSecOps

Prioritize response and recovery: Place as much importance on response and rebound efforts as you do on prevention and detection

Take the offense: Modern security principles (e.g., AI-enhanced threat hunting) can help you take a proactive approach

Engage with Deloitte

How Deloitte can help

Deloitte helps clients design build, and operate dynamic, business-aligned security programs for each stage in their cyber journey. Services aligned to breach response efforts include, but are not limited to, the following:

- **Threat Detection & Response**
- **Cyber Threat Intelligence & Threat Hunting**
- **Cyber Incident Response & Remediation**
- **Third-Party Assessments & Program Design**
- **Zero Trust Transformation**
- **DevSecOps "Security DesignedIn"**
- **Identity & Access Management (IAM), PAM, and Credential Risk Assessment & Implementation**
- **Governance, Risk, & Compliance (GRC)**
- **Data & Privacy Centric Defense – Risk & Regulatory**
- **Forensic Investigation, Response, & Recovery**

The Deloitte difference

- **Global leadership:** Deloitte has been named a global leader in Security Consulting and Cyber Incident Response. We offer differentiated domain leadership and entrenched industry experience
- **Ecosystems & alliances:** Strong alliances with leading technology vendors, industry organizations, law enforcement and research entities to provide leading insights, intelligence, information-sharing and collaboration
- **Cutting-edge technology:** Proprietary technology platforms and accelerators, adversarial simulation, and attack surface management, providing threat detection and response managed services capabilities

Contact us

Deborah Golden
Principal
Deloitte & Touche LLP
Tel: + 1 571 882 5106
Email: debgolden@deloitte.com

Andrew Morrison
Principal
Deloitte & Touche LLP
Tel: + 1 404 220 1170
Email: anmorrison@deloitte.com

Mark Nicholson
Principal
Deloitte & Touche LLP
Tel: +1 917 952 1014
Email: manicholson@deloitte.com

Tim Li
Principal
Deloitte & Touche LLP
Tel: + 1 571 814 7679
Email: timli@deloitte.com