OmegaBlack

2.0

UNDERSTANDING THIRD-PARTY AND FOURTH-PARTY RISKS IN CYBERSECURITY

SUPPLY CHAIN THREATS AND ATTACKS

INTRODUCTION

In today's interconnected digital ecosystem, organizations rely heavily on third parties and fourth parties to operate efficiently. However, these trusted relationships can introduce significant risks, particularly in the form of supply chain attacks. This white paper explores what third and fourth parties are, their role in cybersecurity, and the nature of supply chain risks and attacks, offering insights into how organizations can mitigate these threats.

THREAT INTEL PLATFORM

The OmegaBlack Threat Intelligence Platform is designed to empower organizations with actionable insights to mitigate evolving cyber threats. Our cutting-edge platform delivers continuous updates and in-depth analysis through two powerful tools: the OmegaBlack API and our Mobile App for Alerts. Together, they provide an unparalleled level of threat awareness and protection.

ENTERPRISE SOLUTIONS

OmegaBlack excels in providing actionable intelligence to enhance your team's efficiency and effectiveness. We deliver meticulously organized, step-by-step solutions to address and neutralize malicious activity. At the cutting edge of data security, OmegaBlack ensures your company remains resilient and secure during critical moments.

Words from the Founders

OmegaBlack is committed to protecting your organization by scanning the dark web for threats that are a risk to your company. We provide a wide range of external security services to uncover unforeseen threats before they are exploited by threat actors.

At OmegaBlack, we bring together over 30 years of combined experience in cybersecurity, dedicated to helping organizations navigate the complexities of today's threat landscape.

In our commitment to empowering enterprises, we recognize the critical importance of robust threat intelligence. Our mission is to provide you with the insights and tools necessary to anticipate and mitigate potential threats effectively.

This white paper represents our ongoing effort to share valuable knowledge and best practices in threat intelligence. We hope it serves as a useful resource in your journey to enhance your security posture and make informed decisions in an increasingly volatile environment. Thank you for your interest in our work. We invite you to explore the insights presented within and look forward to supporting you in your efforts to secure your organization.

Introduction

In today's interconnected digital ecosystem, organizations rely heavily on third parties and fourth parties to operate efficiently. However, these trusted relationships can introduce significant risks, particularly in the form of supply chain attacks. This white paper explores what third and fourth parties are, their role in cybersecurity, and the nature of supply chain risks and attacks, offering insights into how organizations can mitigate these threats.

1. WHAT IS A THIRD PARTY?

A third party refers to any external organization, service provider, vendor, or contractor that a company engages with to provide services, software, hardware, or other resources. These entities are not part of the company's internal operations but are trusted relationships and play a crucial role in supporting its business functions. Third parties may have access to an organization's systems, data, or networks as part of their service delivery, making them a potential target for cyber threats. (1)

Examples of Third Parties:

- Cloud Service Providers: Companies like AWS, Microsoft Azure, and Google Cloud offer cloud infrastructure and services critical to business operations.
- Software Vendors: Providers of essential business applications, such as CRM systems or enterprise software (e.g., Microsoft, Salesforce).
- Managed Service Providers (MSPs): External IT teams or cybersecurity firms that manage infrastructure, monitor networks, or provide security support.
- Consultants and Contractors: Individuals or firms hired for specialized tasks, including software development, network management, and technical support.

Cybersecurity Implications:

Third parties, due to their access to sensitive systems and data, become attractive targets for cyber attackers. If a third party is compromised, the attacker may gain indirect access to the primary organization's network, enabling data theft, ransomware deployment, or other malicious activities. The 2013 Target breach, for instance, was the result of attackers compromising a third-party HVAC vendor, allowing them to infiltrate Target's network. (2)

(1) https://attack.mitre.org/techniques/T1199/ (2) https://www.sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf

2. WHAT IS A FOURTH PARTY?

A fourth party is an organization or service provider that a third party relies on to deliver services to their clients. These are vendors or partners that support the third party but are not directly contracted by the primary organization. The involvement of fourth parties adds an additional layer of complexity and risk, as these entities also have access to the third party's resources, potentially impacting the primary organization.

Examples of Fourth Parties:

- **Subcontractors:** Companies that a third-party vendor hires to perform specific services, such as software development or maintenance.
- **Upstream Suppliers:** Providers of essential components or services that third parties integrate into their products (e.g., hardware manufacturers or niche software developers).
- **Service Providers:** Cloud or infrastructure providers that a third party uses to support their own operations (e.g., a small IT service provider using a larger cloud provider's infrastructure).

Cybersecurity Implications:

Fourth-party risk is often less visible and harder to manage because organizations may not have direct control or insight into these relationships. A cyberattack on a fourth party can cascade, impacting the third party and, in turn, the primary organization. This interconnectedness amplifies supply chain risks and requires robust risk management practices.

3. SUPPLY CHAIN RISKS AND ATTACKS

Supply chain risks refer to the vulnerabilities and threats associated with an organization's reliance on third and fourth parties for products and services. (3) Cyber attackers exploit these vulnerabilities to infiltrate organizations indirectly, often through compromised third or fourth parties. (4) Supply chain attacks are particularly dangerous because they can impact multiple organizations simultaneously, spreading quickly through interconnected networks.

How supply Chain Attacks Work:

- **Targeting a Third Party:** Attackers identify and compromise a third party with access to the target organization's network or data. For example, they might infiltrate a managed service provider that manages network security for multiple clients.

(3) https://sot.mitre.org/overview/about.html (4) https://attack.mitre.org/techniques/T1474/

- **Infiltrating the Supply Chain:** Attackers inject malicious code or malware into a third party's software or update process. When the primary organization installs or updates this software, the malicious code spreads.
- **Exploiting Fourth Parties:** Attackers may also target fourth parties that the third party relies on. For example, if a cloud provider used by a third party is compromised, this could expose the third party and, by extension, the primary organization.

noteable examples

SolarWinds Attack (2020):
Attackers compromised the software update mechanism of SolarWinds, a third-party IT management provider, to distribute malware. This breach impacted numerous organizations, including U.S. government agencies and Fortune 500 companies. (5)

Kaseya Attack (2021): A ransomware group targeted Kaseya, an IT management software provider, using a vulnerability in its software to deliver ransomware to managed service providers (third parties) and their clients (primary organizations). (6)

The Impact of Supply Chain Attacks:

Supply chain attacks can have severe consequences, including:

- **Data Breaches:** Attackers may steal sensitive information from compromised organizations.
- **Operational Disruption:** Malware or ransomware can disable critical systems, leading to downtime and operational loss.
- **Reputational Damage:** Organizations affected by supply chain attacks may suffer reputational harm, leading to a loss of customer trust and business opportunities.
- **Regulatory Consequences:** Compliance violations and penalties may arise if organizations fail to secure their supply chain effectively.

(5) https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (6) https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers

4. MITIGATING SUPPLY CHAIN RISKS

Given the complexity and reach of supply chain risks, organizations must adopt comprehensive strategies to protect against third and fourth-party threats.

Best Practices:

- **Vendor Risk Assessment:** Perform thorough risk assessments of third parties before engaging with them. Evaluate their security policies, practices, and compliance with relevant standards.
- **Contractual Security Requirements:** Incorporate cybersecurity requirements into contracts with third parties, such as regular audits, security certifications, and data protection measures.
- **Visibility into Fourth Parties:** Ensure that third parties disclose their own critical vendors (fourth parties) and assess their security practices as part of an extended risk management process.
- **Zero Trust Architecture:** Implement a zero-trust approach to third-party access, requiring strict identity verification, access controls, and monitoring for any third or fourth party interacting with the organization's network.
- **Continuous Monitoring and Threat Intelligence:** Monitor third-party activities continuously for any suspicious behavior. Utilize threat intelligence to stay updated on emerging threats that may impact third or fourth parties.
- **Incident Response Planning:** Develop and maintain an incident response plan specifically designed to handle supply chain attacks, ensuring a quick and coordinated response in the event of a breach.

Conclusion

The reliance on third and fourth parties introduces substantial cybersecurity risks, particularly in the form of supply chain attacks. Understanding these risks and implementing robust risk management strategies is critical for organizations to protect their operations and data. By adopting proactive measures such as thorough vendor assessments, continuous monitoring, and strong contractual controls, organizations can mitigate the risks associated with their interconnected digital ecosystem.

Recommendations

Integrate Supply Chain Security:

Make supply chain security an integral part of the overall cybersecurity strategy, ensuring that both third and fourth-party risks are addressed comprehensively.

Develop Collaborative Partnerships:

Work closely with third parties to create a culture of cybersecurity, sharing threat intelligence and best practices.

Regularly Update Risk Management Policies:

Update and review risk management policies regularly to adapt to evolving threats and emerging vulnerabilities in the supply chain.