proofpoint.

THREAT BRIEFING

Supply Chain Attacks

Fast Facts

DESCRIPTION

Supply chain attacks fall into two main categories: email fraud and third-party software. In these attacks, cyber criminals compromise vendors or service providers in order to attack their customers and partners. Initial supplier compromise is often by phishing or malware. Once inside a supplier system, attackers can impersonate email accounts to initiate phishing, invoicing fraud or other types of attack against customers. Once attackers have breached customer systems, they can steal confidential data, install ransomware or use access to trigger a further wave of phishing or email fraud attacks.

TOOLS OF THE TRADE

Supply chain threats typically involve phishing for credentials (account takeover), malware (Stuxnet, NotPetya, Sunburst, Kwampirs) and impostor threats like business email compromise (BEC).

TYPES

- **Business email compromise (BEC, or email fraud).** Attackers pose as someone the recipient would trust—typically a business partner, supplier or vendor. The recipient is asked to make a wire transfer, pay a fake or altered invoice, divert payroll funds or change banking details for future payments. In some email fraud schemes, the attacker may compromise the supplier's actual email account to pose as the supplier and even piggyback existing email conversations.
- **Software supply chain attacks.** Attackers gain access to the systems of a software or managed service provider and infect future builds that are then distributed on to customers and partners. Such attacks are rare compared to the forms listed above, but they can affect multiple victims from a single breach.

RISK FACTORS

- Engaging vendors for professional services and consultation
- Not employing adequate cybersecurity protection
- Providing access to staff who are negligent or untrained in security awareness
- Supply chain complexity—businesses increasingly rely on a variety of cloud platforms and SaaS services

Supply Chain Attacks in the News

Target to pay $18.5M for 2013 data breach that affected 41 million consumers

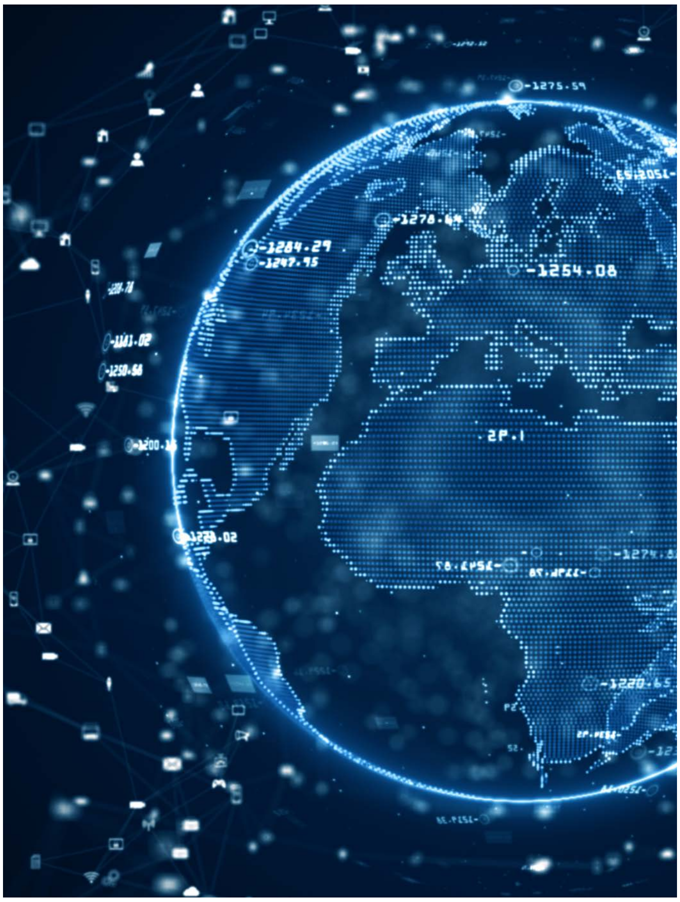
Account credentials stolen from one of Target's vendors enabled attackers to breach the retail giant's systems and steal sensitive payment information from more than 41 million customers.

Hackers are attacking the COVID-19 vaccine supply chain

A phishing attack targeted executives at 44 companies across several continents in an attempt to compromise the global COVID-19 vaccine supply chain.

Community Housing Nonprofit Hit with $1.2M Loss in BEC Scam

Attackers spoofed a vendor domain to steal almost £1 million in rent from a cooperative housing association near London, U.K.



Anatomy of a Supply Chain Attack

1. **Infiltration**

   Attackers use a variety of methods for the initial breach:

   - Brute-force attacks with automated tools to try username and password pairs until a match is found
   - Impersonating a trusted contact to send phishing, impostor emails or links/ attachments containing malware such as keyloggers or stealers
   - Taking over the account of a trusted supplier

2. **Reconnaissance**

   - Once the attacker has stolen valid login credentials, they can begin exploiting the supplier's network and reputation. They monitor communications between the supplier and their customers, prospecting for targets.

3. **Attack**

   - When reconnaissance is complete, the attacker can use the compromised supplier's systems to phish for credentials, submit fraudulent invoices or send malware to customers.

Research Insights

Over a one-week period in February 2021, Proofpoint analyzed data from 3,000 organizations across various verticals in the U.S., U.K. and Australia. During that time, the vast majority experienced supply chain attacks.

98% received a threat from a supplier who was either impersonated or compromised.

Attacks were equally likely across all countries and industry sectors in the sample.

Of those threats, almost three quarters involved phishing or impersonation.

<30% of emails sent from supplier domains contained malware.

HOW CRIME-AS-A-SERVICE HAS FUELED SUPPLY CHAIN ATTACKS

The dark web is a notorious marketplace for exploit kits and custom malware used to sell services like botnet rentals and ransomware software. Just like most SaaS providers, cyber criminals provide tools and platforms to those carry out supply chain attacks, ransomware attacks and other cyber crime. Threat actors who lack advanced technical skills can now easily carry out attacks.

How to protect your organization

To address supply chain fraud and software supply chain attack, here are some key security controls organizations should consider implementing.

Supply chain fraud

For supplier invoicing fraud, organizations should take a holistic, multi-layered approach, as attackers often leverage both supplier impersonation and compromised supplier accounts jointly.

> For supplier invoicing fraud, organizations should take a holistic, multi-layered approach, as attackers often leverage both supplier impersonation and compromised supplier accounts jointly.

BEC often starts with an email in which the attacker poses as someone the target trusts or "actually becomes" that person by compromising their account. Because there is no malicious payload, BEC attacks are hard for legacy gateways that only rely on reputation and malware sandboxing to detect.

Here's how to stop the most common—and costly—supply-chain attacks.

Get visibility into your supplier email fraud risks

To help you better understand, communicate and mitigate, get answers to the following questions:

- What are our BEC risks?
- Which users are the most vulnerable?
- Which suppliers are posing risk to our organizations?
- What should we do to mitigate the risks?

You should know which of your users are most attacked by impostor threats and who is most likely to fall for these types of threats.

At the same time, having granular visibility into BEC threat details and identifying common BEC themes, such as supplier invoicing fraud and payroll diversion, can help you better understand and communicate BEC risk.

Detect and block impostor threats before they enter

Stopping supplier attacks that play out over email means uncovering all email fraud tactics, including display name spoofing, look-alike domains and sophisticated supplier fraud. Look for a solution that dynamically analyzes messages for numerous tactics associated with supplier invoicing fraud such as:

- Reply-to pivots
- Use of malicious IPs
- Use of impersonated supplier domains
- Words or phrases commonly used in these supplier fraud attacks

(Most email security products only rely on static rule matching or limited contextual data which requires manual tuning.)

Make users resilient against BEC supply chain attacks

BEC targets people and relies on them to unwittingly carry out the attack. Because these impostor attacks leverage social engineering and impersonation, your users are often left as the last line of defense. That's why mitigating BEC risks requires both technology and training.

Train your users to identify and report suspicious impostor email. This will give them the knowledge and skills they need to protect your organization against these human-activated threats.

Email warning tags can help surface the risk each email poses. For example, warning users when a message is sent from an external sender or a newly registered domain can help them make more informed decisions on uncertain email.

Protect your own brand from being used in email fraud attacks

While you're concerned about the risk your suppliers might pose, your own customers may have similar concerns about you.

Attackers can turn you against your customers and business partners by using your company's name and brand to steal from them. While brand spoofing may not cause direct financial loss to your organization, it can damage your organization's reputation, erode customer trust and ultimately hurt business.

Prevent fraudulent emails from being sent using DMARC email authentication, whether sent by you directly or a designated third party.

Software supply chain attacks

Beyond the more common supply chain attacks discussed above, the increased use of third-party and managed software has created an additional type of supply chain risk.

If a compromised supplier provides software or cloud services, attackers can alter source code and inject malware into the build and update process. Infected programs or services are then distributed to customers and partners, along with the malicious payload included by the attacker.

Users often lack the capacity to inspect the third-party programs they use, meaning they must depend on their software vendors and suppliers to have strong protections in place. If compromised software is delivered to an organization, they can then find themselves open to a full range of attacks, from data theft to ransomware infection.

This sort of attack is especially difficult to prevent. Unpatched software vulnerabilities are one of the most common vectors for cyber attack, so updating software to the latest versions is always considered a best practice. But now, it's also an attack vector.

Learn More

With supply chain attacks dominating the headlines, it is clear that third-party services, vendors and contractors pose a serious risk to the security posture of organizations. A people-centric security solution that detects new attack tools, targets and tactics can help to mitigate that risk.

To learn more about how to effectively stop supply chain attacks, visit **www.proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.