Supply Chain: Compromise of Third-Parties Poses Increasing Risk

July 20, 2017

TLP: WHITE | The NJCCIC assesses with high confidence that capable threat actors—both politically-motivated state actors and their proxies, as well as profit-driven criminals—will increasingly leverage supply chain compromises to conduct network intrusions and attacks. These incidents could result in the exfiltration, manipulation, or destruction of data and disruption to daily operations and business continuity. Supply chain compromises commonly involve a malicious actor gaining access to a victim’s network using stolen remote access credentials belonging to a vendor or business partner. They can also occur through the injection of malicious code into third-party software used by the victim, as was the case in the June 27, 2017 attack that targeted Ukrainian organizations and severely impacted dozens of victims in numerous other countries, including the United States. The attack, referred to as Petya-NotPetya and a variety of other names, was initiated through the compromise of a server that distributed software updates for M.E.Doc, accounting software used by organizations that conduct business in Ukraine. While consensus among cybersecurity firms indicates a state-sponsored Russian hacking group was responsible for the attack, the primary motive and objectives remain unclear; however, analysis from Booz Allen Hamilton suggests the destructive nature of the attack may have been a deliberate act to cover-up network intrusions and data theft conducted in the months prior. The Petya-NotPetya attack demonstrated the unintended consequences and collateral damage that can result from supply chain attacks involving widely-used software.

− In 2016, the cybersecurity firm Symantec found that the average organization was using 928 cloud applications, up from 841 in 2015. However, according to Symantec’s survey, most Chief Information Officers thought their organizations only used approximately 30 or 40 cloud applications. As organizations become increasingly reliant on third-party products and services, the risk of attacks—whether targeted or opportunistic—will rise, potentially resulting in prolonged service outages, damages to IT or industrial control systems, or the permanent loss of data.

Recent Supply Chain Incidents

− In 2013, criminal actors gained access to Target’s corporate network using compromised login credentials belonging to an HVAC vendor and installed malware on point-of-sale (PoS) terminals in retail locations. This resulted in the theft of 41 million payment card accounts and personal information of 70 million customers. In May 2017, Target reached an $18.5 million multistate settlement, the largest to date for a data breach, and revealed it had spent at least $202 million on legal expenses and other costs associated with the breach.

− From 2013 to 2015, an unauthorized party accessed sensitive personal data of approximately 15 million T-Mobile customers through the compromise of a server owned by Experian, T-Mobile’s credit application processing vendor. Both T-Mobile and Experian were subsequently named in multiple class action lawsuits.

− In 2016, the restaurant chain Wendy’s investigated a PoS malware breach that compromised customer transactions at 1,025 franchise-operated locations. The company stated the attack resulted from the hacking of an unnamed third-party provider’s credentials. In October, a Michigan-based credit union temporarily barred the use of its payment cards at Wendy’s locations after over 38% of its issued cards were compromised in the breach.

− Last month, Sabre Hospitality Solutions began notifying its customers of a breach of its SynXis Central Reservations system, which is used by hundreds of airlines and thousands of hotel properties to manage operations, including reservations, that lasted from August 2016 to March 2017. Thus far, Google, Hard Rock Hotels and Casinos, Loews Hotels, the Four Seasons, and Trump Hotels have acknowledged they were affected.

Recommendations

The NJCCIC strongly recommends all organizations implement a robust program to proactively identify and manage risk posed by supply chain vendors and other third parties. All vendors, contractors, or businesses partners with access to an organization’s networks, computer systems, databases, or facilities must be provided with documentation of policies and required to consent to security requirements and acceptable use policies. A list of best practices for supply chain risk management, as well as additional resources, is included in the attached appendix and available on the NJCCIC website.

Traffic Light Protocol: WHITE information may be distributed without restriction.
Appendix: Recommendations to Improve Supply Chain Security

The following list of security measures is not exhaustive and is intended to provide the most basic and necessary practices to manage risk posed by vendors, suppliers, and other third-parties. For comprehensive sets of recommendations on supply chain security practices, refer to the resources provided below by the National Institute of Standards and Technology (NIST), SANS Institute, the Software Engineering Institute at Carnegie Mellon University, and others.

**Internal Controls**
- Implement a comprehensive vendor management program, beginning with audits of all current vendors.
- Prior to implementing new hardware or software products into a production environment, fully vet the product to ensure it works as expected in a test environment.
- Leverage trusted third-party security review resources including the National Information Assurance Partnership, FedRamp and Cloud Security Alliance CSTAR certifications, etc.
- If possible, conduct source code reviews of all third-party software used within your enterprise.
- Establish security controls and regularly audit vendor access to your networks, systems, and sensitive data.
- Apply the Principle of Least Privilege when creating user accounts for vendors and regularly monitor and audit accounts for abuse and privilege escalation.
- Require two-factor authentication, the use of a VPN, and/or apply IP address whitelisting for remote access to all systems and portals that contain sensitive data.
- Limit or eliminate the transmission or storage of unnecessary customer and client information.
- Maintain awareness of all compliance mandates, security standards, and reporting requirements and update policies and procedures to incorporate changes as needed.
- Ensure that all security requirements, including acceptable use policies, are clearly defined in vendor contracts.
- Implement proper network segmentation to protect systems and data from unauthorized access by vendors and other external threats.
- Block traffic to unneeded ports both at the network perimeter and on internal systems, servers, and firewalls.
- Disable, delete, or block the use of unneeded remote access tools such as PsExec, Microsoft Remote Desktop, TeamViewer, VNC, LogMeIn, etc.
- Whitelist authorized applications and proactively block the installation and usage of unauthorized software.
- Consider implementing a data loss prevention (DLP) solution that includes monitoring of all egress traffic for unauthorized data exfiltration.
- Follow established change management processes.

**Supply Chain Controls**
- All vendors must review, sign, and maintain compliance with security requirements and acceptable use policies.
- Require vendors who transmit or store sensitive data to encrypt it both at rest and in transit.
- Require vendors to provide immediate notification of any data breaches or cybersecurity incidents that may impact your organization, your clients, or your customers.
- Require that vendors perform comprehensive background checks on their employees. These background checks should be performed regularly, preferably on an annual or bi-annual basis.
- Require that all software and systems used by vendors to access your networks or sensitive data are running antivirus software and kept up-to-date with the latest security patches.

**Additional Resources**
- SANS Institute InfoSec Reading Room: [Combatting Cyber Risks in the Supply Chain](https://www.sans.org/blog/2013/09/24/combatting-cyber-risks-supply-chain).