Guidacent®

Point of View: Surviving the SolarWind~*storm*

Reuters announced in December 2020 that **the Russian Foreign Intelligence Service infiltrated the US Treasury Department through a series of trojan exploits it planted into the code of** a global Managed Service Provider (MSP) called **SolarWinds, a supplier for thousands of organizations**.

Attack Overview:

Many cybersecurity professionals have called this **"the hack of the century."** The attackers **delivered malware** through the SolarWinds Remote Management System **to thousands of organizations, including multiple US government entities and more than 90% of the Fortune 500 Companies.** Many organizations have yet to realize that they were impacted by this breach.

Sun ♦ burst (hostile code)

- A sophisticated supply chain attack, resulting in a compromised infrastructure to launch further attacks on subsequent users of the Orion platform.
- Targeted government agencies and contractors, technology firms, and thousands of private sector companies.

The attackers used a combination of advanced persistent threats, or APT tactics, to compromise the Orion Remote Management System application. MSPs use Orion to gain access and manage systems and operations of clients.

Under this Orion hack, referred to as "SunBurst," perpetrators delivered malware to thousands of organizations by disguising it as legitimate third-party software updates from September through December 2020.

The **perpetrators** also **gained access to some of Microsoft's internal source code** (considered the Holy Grail by cybercrime organizations all over the world).

Guidacent®

Why it Matters

- SolarWinds "Orion" code altered
- 18,000+ organizations impacted
- State-sponsored supply chain attack
- 425 of Fortune 500 affected
- Top 10 U.S. telecoms impacted
- Top 5 accounting firms compromised

With **4.1 billion records** exposed during 2019, financial costs resulting from cybercrime will continue to rise. They are expected to reach **$6 trillion** by the end of 2021. More than **$133 billion** is expected to be **spent on cybersecurity** by 2022.

Recent data from Gartner and Ponemon project annual damages of approximately $6 trillion caused by this attack. The hackers meticulously infiltrated organizations and over several months secretly analyzed vulnerabilities to identify opportunities to steal data, disrupt operations, and cause other targeted damages to critical assets. In fact, the attackers have yet to fully execute attacks within many of their targeted organizations. This means many impacted companies have yet to realize that they are victims.

This is not an isolated incident for SolarWinds. A zero-day vulnerability in SolarWinds MSP's remote monitoring and management tool, which they documented and announced in January 2020, allowed attackers to steal the administrative credentials of an account holder. These elevated privileges provided gateways for hackers to rapidly expand their attacks.

A key target for access included exposed remote desktop protocol (RDP) ports or potentially compromised accounts, acquired through credential harvesting campaigns. Hackers like RDP, which the industry often refers to as the "Ransomware Delivery Platform" because of its ease-of-compromise.

Guidacent®

The **Threat Landscape** is changing as a result of a new class of threat actor, which is funded independently; some are referring to them as **"Digital Mercenaries"** or Hacking as a Service

How's Your Threat Appetite?

- $20 billion (2020 ransomware damages)
- 92% of all malware is delivered by email
- 70% of businesses saw increased risk in 2020
- 69% of companies don't use antivirus
- 45% of cyber-attacks target small businesses
- Yet, 14% of businesses think they're prepared

The SolarWinds supply chain attack will impact over 18,000 organizations, with hundreds of thousands (if not millions) of endpoints affected.

The hackers exploited administrative permissions acquired through on-premises compromise of SolarWinds Orion to access a targeted, trusted token-signing certificate, which allowed them to forge tokens that impersonate any of the organization's existing users and accounts, including highly privileged accounts.

The field has experienced time and time again this style of access, a Command-and-Control attack by remote management systems routed through MSPs.
Under this type of APT attack campaign, the hackers often plan a post-breach dormancy period. This allows the network to quiet back down into an unsuspecting lull of activity, followed by a planned and coordinated attack.

During the next wave of the attack, trojan-retrieved and executed commands, called 'Jobs,' transfer files, execute file commands, profile the system, reboot machines, and disable system services. All of this occurs while masquerading as part of the system's "Improvement Program" protocol.

In the background, hostile code used multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers, with a weaponized version of Cobalt Strike for further penetration into thousands of target systems.

Guidacent®

Basic Cybersecurity Hygiene

- Strong (12 alphanumeric) passwords
- Insist on multi-factor authentication
- Keep your patches verified & updated
- Don't share user accounts
- Encrypt all devices & access points
- Back-up files frequently
- Adopt a cybersecurity framework

The Sunburst attack follows classic "ATT&CK Kill Chain" patterns. In the first phase of this attack, the Orion update package was deployed to more than 18,000 organizations.

In the second phase, SUNBURST then performed DNS lookups to a subdomain encoded with information about the specific local environment. A CNAME response back to the request then initiated a custom HTTPS tunnel, which was included in the compromised code.

As part of the third phase, attackers leveraged service or admin accounts present on the target server, as well as Windows admin tools that supported remote code execution to move laterally from the SolarWinds system deeper into the various targeted networks.

Once they acquired Domain Admin, the hackers were free to move to the ADFS server, where they acquired the SAML signing certificate, modified certificate authorities and then were able to use attacker-owned Certificates to validate their masqueraded credentials.

Using the stolen certificate to forge new SAML tokens, attackers were able to access Azure Active Directory with admin permissions. The group was also able to gain access to applications (including email archiving), which provided further access to email directories. At this point, the attackers had direct access to email in specific user accounts where they could further leverage native Office 365 tools like eDiscovery and Power Automate to harvest specific data.

This new breed of sophisticated nation-state attacks is becoming frequently combined with state-of-the-art AI technologies and tools, thereby pushing further, the gap between system activity and human limitations to stop them.

Experts agree that this is, once again, an example of a critical choke point at the intersection of "Privilege" and "Authentication."

Moreover, the very reason this incident was even discovered was because of stolen credentials being used to attempt to register a new device for MFA.

This new breed of sophisticated **nation-state attacks** is becoming frequently combined with state-of-the-art **AI technologies** and tools, thereby pushing further, the gap between system activity and human limitations to stop them.

Guidacent®

The SolarWinds cyber-attack serves as a sobering reminder to be constantly mindful of the threats that lurk deep within third-party vendor supply chains, And that starts with basic cybersecurity hygiene.

What Every Organization can do Now

- Security Awareness Training
- Adopt a Mandatory Security Framework
- Review Supply Chain SLAs
- How is Your MSP Managing Your Data?
- Perform a Security Assessment
- Adopt Principles of Least Privilege
- Insist on a "Zero-trust" Security Posture!

Regardless of business size or scope of operations, every organization can and should ensure it is taking certain measures to protect those assets that comprise the core of its business.

From a Security Operations perspective, organizations need to know where core assets and related data reside within their infrastructure.

Organizations should also ensure the appropriate classification of data and assets. These classifications help assess whether the right system controls are in place, including effective and comprehensive tools for auditing and event detection and notification.

Perhaps chief among all the security contingencies, businesses can take are those actions tied to "Principles of Least Privilege."

Want to learn more about best practices to protect your environment, including understanding what control framework makes sense for you?

Contact Guidacent today for a consultation. Our team of experienced, certified Information Security Professionals can help any size organization, regardless of where you might find yourself on the "Cybersecurity Maturity" scale.

Ready to learn how Guidacent can help your business improve its security posture?

Email us at cybersecurity@guidacent to schedule a free consultation.