CYBER STASH

In The Wake Of Solarwinds Compromise

eclipse

Solarwinds Compromise

As the greatest hack in history continues to evolve, the compromise of 18,000+ organisations, from which most can be found on the Fortune 500 list, has shaken our industry to the core and will undoubtedly force many security practitioners to scrutinise aspects of cyber threats that were not previously identified, or were identified but rated with very low or neglectable likelihood of occurrence during risk assessments.

Either way, the question needs to be asked, can such unknown supply-chain exploits even be mitigated and if so, how exactly? This question conversely opens up Pandora's box, and demands further reflection of other possible supply-chain and technology-based risks. Presumably the companies on the Fortune 500 list, on average, would have the highest amount of security budget enabling them to operationalise the people, processes and technology to effectively manage cyber risks, and to then rigorously audit its controls periodically to ensure compliance with corporate security policies and best practice industry guidelines.

Unfortunately however, when designing attacks, cyber-criminals continue to outsmart and evade security controls by using their understanding of how defenders implement and operationalise security within corporate networks.

While every software has inherent risks, we can no longer afford to accept and leave low risks untreated in applications that are supposed to safeguard our organisations.

Cyber Risk Assessment

The sophistication, elegance and effectiveness of the Solarwinds Compromise perpetrated by what's attributed to Russian APT actors, has once again caught our cybersecurity industry by surprise and in light of the risks exposed, below are several questions to be re-assessing as a cybersecurity practitioner:

1. *What if our vulnerability scanning and penetration testing platforms is compromised?*
2. *What if our remote access platforms or software is compromised?*
3. *What if our patch management platform is comprised?*
4. *What if our backup management system is compromised?*
5. *What if our endpoint security agent is compromised or evaded?*
6. *What if our privileged access management platform is compromised?*
7. *What if our IoT, OT, ICS, SCADA management platform is compromised?*
8. *What if our "insert your favourite OS, asset, or application here" management software is compromised?*

Exacerbating the risk, many of the above IT management systems have access to all or a large number of sensitive systems within an organisation. Many even store service or privileged account credentials and use these to access the assets and applications they manage. Allowing any level of doubt that the integrity of such systems can be compromised, is simply leaving an organisation exposed to sophisticated attacks.

Software vendors must also implement mitigation strategies that protects the integrity of their code and its distribution to clients.

Limit Your Exposure

The hacking tools stolen from FireEye can be used to exploit over a dozen vulnerabilities in common applications used by many enterprises today.

FireEye has released a list of CVEs for the affected systems and applications on its Github repository.

The following is a prioritised list of CVEs that should be mitigated to limit the effectiveness of the leaked Red Team tools.

CVE	Description	CVSS
CVE-2019-11510	Pre-auth arbitrary file reading from Pulse Secure SSL VPNs	10
CVE-2020-1472	Microsoft Active Directory escalation of privileges	10
CVE-2018-13379	Pre-auth arbitrary file reading from Fortinet Fortigate SSL VPN	9.8
CVE-2018-15961	RCE via Adobe ColdFusion (arbitrary file upload that can be used to upload a JSP web shell)	9.8
CVE-2019-0604	RCE for Microsoft Sharepoint	9.8
CVE-2019-0708	RCE of Windows Remote Desktop Services (RDS)	9.8
CVE-2019-11580	Atlassian Crowd Remote Code Execution	9.8
CVE-2019-19781	RCE of Citrix Application Delivery Controller and Citrix Gateway	9.8
CVE-2020-10189	RCE for ZoHo ManageEngine Desktop Central	9.8
CVE-2014-1812	Windows Local Privilege Escalation	9
CVE-2019-3398	Confluence Authenticated Remote Code Execution	8.8
CVE-2020-0688	Remote Command Execution in Microsoft Exchange	8.8
CVE-2016-0167	Local privilege escalation on older versions of Microsoft Windows	7.8
CVE-2017-11774	RCE in Microsoft Outlook via crafted document execution (phishing)	7.8
CVE-2018-8581	Microsoft Exchange Server escalation of privileges	7.4
CVE-2019-8394	Arbitrary pre-auth file upload to ZoHo ManageEngine ServiceDesk Plus	6.5

Reference: https://github.com/fireeye/red_team_tool_countermeasures

Notwithstanding that these vulnerabilities are not new and could have been exploited through other exploitation frameworks and hacking tools, every organisation should ensure that its vulnerability mitigation program continues operating effectively regardless of whether there are high exposure advisories about active exploits operating in the public domain.

Sunburst

The Solarwinds Compromise was not easy to detect without having prior knowledge of the SunBurst trojan or without having previously identified and implemented controls to detect or mitigate the attack vector. We now know that the backdoor was created with the trojanised update and found embedded within the signed Orion code itself and distributed using official patching mechanisms available from the vendor.

As such, even if an endpoint security solution detected the malicious code and blocked it from downloading, or detected the DLL containing the malicious code at runtime, many administrators, checking that the file was signed and from a trusted source, would have assumed that the response from the endpoint software was a false trigger and created an exception to allow the download to complete, or DLL to run.

It took FireEye, a security company who specialises in breach detection to be breached to disclose SunBurst. All the same, Charles Carmakal, the senior VP and CTO at Mandiant-FireEye, said that they resulted to looking through 50,000 lines of source code to determine there was a backdoor within SolarWinds.

An enterprise who doesn't specialise in cybersecurity, even if they have a well funded security practice, would not have detected the breach and if they did, they would not have disclosed the root cause; a malicious code inserted within SolarWinds.Orion.Core.BusinessLayer.dll.

Mitigation Challenges

The Solarwinds Compromise was not easy to detect without having prior knowledge of the SunBurst trojan or without having previously identified and implemented controls to detect or mitigate the attack vector. We now know that the backdoor was created with the trojanised update and found embedded within the signed Orion code itself and distributed using official patching mechanisms available from the vendor.

As such, even if an endpoint security solution detected the malicious code and blocked it from downloading, or detected the DLL containing the malicious code at runtime, many administrators, checking that the file was signed and from a trusted source, would have assumed that the response from the endpoint software was a false trigger and created an exception to allow the download to complete, or DLL to run.

It took FireEye, a security company who specialises in breach detection to be breached to disclose SunBurst. All the same, Charles Carmakal, the senior VP and CTO at Mandiant-FireEye, said that they resulted to looking through 50,000 lines of source code to determine there was a backdoor within SolarWinds.

An enterprise who doesn't specialise in cybersecurity, even if they have a well funded security practice, would not have detected the breach and if they did, they would not have disclosed the root cause; a malicious code inserted within SolarWinds.Orion.Core.BusinessLayer.dll.

Motivation

Today, you can speak to any IT Executive and they will tell you that ransomware is their top-of-mind risk. What's however evident from the hacking tools breached from FireEye, is that the primary goal of the adversary was to steal intellectual property that would give them an upper hand – this is a strong characteristic of state-sponsored actors, as opposed to organised crime syndicates who are financially motivated and typically use ransomware to complete their mission.

What's Missing?

Given the unsophisticated nature of code used to develop simple fileless beacons, especially if these are operating as part of a signed trusted application, many backdoors can be left undetected and continue to operate hidden within the enterprise network.

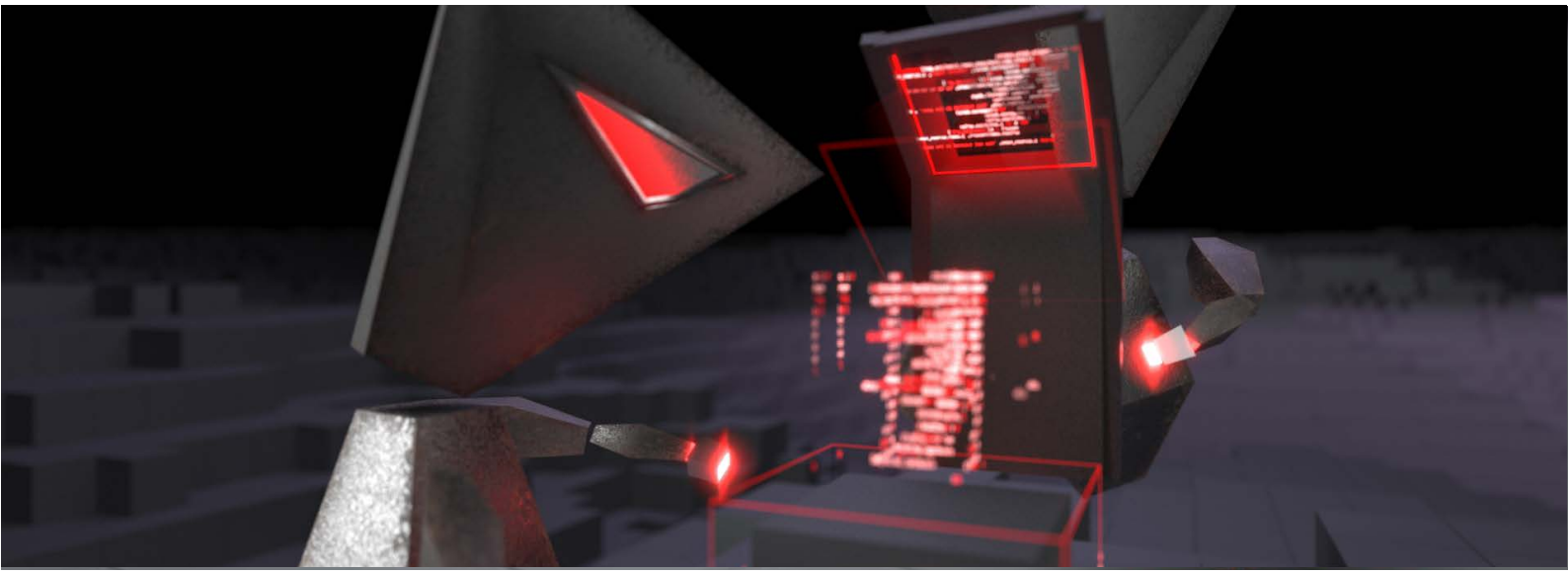
While effective endpoint protection platforms can stop and somewhat clean-up malware, many don't end of cleaning up the initial trojan that's acting as the beachhead and are particularly ineffective at cleaning up the attack if the beachhead is running on a different system to where the malware was discovered.
Moreover, if the malware is designed to evade and disable the endpoint agent, it's game over. Keep in mind that real-time endpoint security engines don't have the luxury of forensically validating every aspect of a system by going underneath higher-level operating system APIs and working directly with volatile memory structures. This forces them to sample events down the kill-chain at 30-to-130 samples per minute which exposes inherent detection gaps that can lead to compromise. These are some of the reason that allow adversaries to breach and continue to sustain their position inside enterprise networks.

What About Zero Trust?

What the Solarwinds Compromise has evidently disclosed is a failure of many originations to implement best practice access control measures. To be effective, the backdoor in the Solarwinds Compromise selects its C2 server using a Domain Generation Algorithm (DGA) to construct and resolve subdomains which it then connects to using HTTP calls.

The fact that such communication is successfully established, reveals that the organisations affected allow unrestricted outbound HTTP access to all or unclassified public URLs and IP addresses from corporate servers.
By simply limiting outbound access from corporate servers to only required URLs, Domains and IP addresses, the backdoor would be stopped in its path and not succeed.

Furthermore, to prevent or limit a backdoor probe from DNS tunneling its way to C2 servers, corporate servers where possible, should be restricted to resolving required domains only. Organisations should configure DNS policies to only approve queries from specific domains using Allow Lists, such that the DNS server only processes queries from allowed domains, while blocking all other queries from other domains.



Mitigation

Regardless of whether the implementation of protective controls are possible and feasible, timely detection and response is still a must. Even when malware is blocked by an endpoint security control, forensically triaging and investigating the incident is paramount to post-breach containment and clean-up activity.

However, this isn't achievable by conducting Forensic Detection Incident Response (FDIR) because this manual-driven approach is simply not feasible in large environments, especially considering the number of malware dealt by enterprises today. What is achievable though, is periodic and automated forensic state-based assessments which are preceded by further investigations for all leads. At CyberStash, this methodology is one where proactive and periodic static forensic surveys are taken of all endpoints across the entire IT fleet followed by dynamic and human analysis to investigate all suspicious leads with the purpose of exposing the true nature of a file.

As threats evolve to evade preventive controls, organisations must conduct periodic compromise assessments with the intention of maintaining a higher level of trust in its IT environment. Today, organisations continue to only carry out traditional assessments that evaluate vulnerabilities and risks of future compromise, but if they wish to stay ahead of threats before business impact occurs, they must equally focus on conducting periodic compromise threat assessments that are aimed at hunting down systems which are already compromised.

It's important to appreciate that while cybercriminals can outsmart defences, this doesn't necessarily mean they have sufficient time to outpace breach detection systems to cause irreversible damage to the business. Organisations must first accept that they can be breached and then begin designing defences that control breach detection time. This must become a critical KPI when measuring the cybersecurity capability and maturity for organisations who want to uplift their security posture .

The Forensic-Depth Post-Breach Compromise Assessment Company

CyberStash
Forensic-Depth Compromise Assessments

CyberStash delivers a Forensic-Depth Compromise Assessment Service which is a platform and service offering that detects systems that have already been compromised by an attack that's more sophisticated than what current security controls can catch. CyberStash establishes trust in the IT environment for the board and executives by conducting Forensic Depth Analysis across the entire IT fleet at a frequency that's defined by the organisation's risk appetite.

A higher degree of resilience and assurance is obtained because CyberStash effectively reduces dwell-time to 1 day by forensically detecting and responding to compromised systems before these lead to business impact.

info@cyberstash.com
1300 893 802
cyberstash.com
Sydney, Australia

Want to run a trial?

Reach Out To Cyberstash
For More information.

Explore
eclipse.xdr