Supply Chain Attacks

Abstract: The recent SolarWinds attacks leveraging the automatic Orion software updates sent ripples across the world on devastating effects of an APT (Advanced Persistent Threat) attack exploiting the supply chain based on trust factor of the vendor. This is one such example affecting the important and strategic institutions. 'The Great Suspender' Chrome extension was suspected to contain malware after the original author appeared to have sold it to unknown buyers. The classic example of such attack can be traced back to Stuxnet targeting the Natanz nuclear facility in Iran. Although the original authors for the same have never been officially found, the above 3 cases provide some insights on the trust factor and focus on zero trust factor in the production environment. This study provides some insights into high level description of 3 different supply chain attacks.

Keywords: supply chain, SolarWinds, Threats, Security, Trust

1. Introduction

A Supply Chain attack is a threat to any existing facility as compromise in any one link can have a downfall on immediate end users and the ripple can be felt across all other direct and indirect dependents. The usual attacks are at the place of produce / manufacture / development. The targets are usually the vendors whose trust factor are high and the end users hardly doubt on the content or security of the product. A supply chain attack can not necessarily mean a sabotage (Stuxnet), but also includes and not limited to espionage (SolarWinds). The immediate threats are faced by Multi-National Corporations who primarily have a large effect on the economy (Shamoon). The Threat actors are not always the APT as there are instances of espionage by MNC's over market competitors. The core focus in here is understanding the threats posed by the Supply Chain attacks.

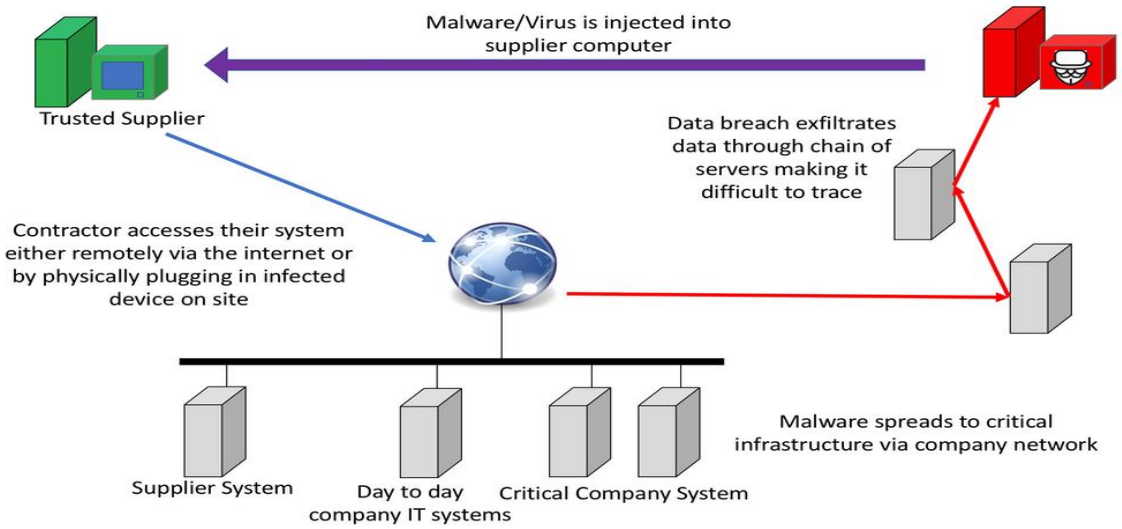

Figure 1: Typical supply chain attack

2. Stuxnet

Stuxnet was one of the most devastating malwares to have impacted physical damage on the target. The authors are allegedly US and Israel which targeted the Natanz Nuclear Facility of Iran to damage the centrifuges used to enrich high grade Uranium. Although it is reported that it was never meant to be leaked to the public but the aggressiveness showcased by the authors was stated as the main reason for the malware to be detected by threat intelligence agency/organizations like VirusBlokAda. Since this was a new sophisticated attack that was able to bypass the air-gap security measure, it was a matter of interest to explore the entry point of the malware. This was for the first time a malware that included a Programmable logic controller rootkit.

It can be argued that Stuxnet was not included as a code in the original product, but migration from the internet into the air-gapped systems at the nuclear facility through the contractor's systems or other physical means can be stated as a supply chain attack. The trust on the contractors about their job and software's used by them is the point of interest in here. If the malware was alleged to jump from the contractor's device into the air-gapped system, the pre-existing prevention systems like firewall, Anti-Virus, etc were unable to detect it as the use of zero days made it difficult to find something unknown at that time. The detection (March 2010) of Stuxnet using a signed driver with a valid Realtek Semiconductor Corps certificate establishes the supply-chain attack as the trust on the certificate allowed the Stuxnet to execute as a legitimate vendor product.

It is this security mechanism that was one of the reasons for the malware to be recognized as legitimate executable and allowed to carry on with its execution. After the detection of certificate of Realtek Semiconductor corps, the malware used another vendor's certificate (JMicron Technology Corp). Thus, the abuse of multiple vendors certificate was something that was incredibly complex to figure out in the supply chain as it would mean stopping entire systems and disinfecting the systems from the malware. The security mechanism that was introduced to manage trust factor was abused to let the malware work pointing out a problem which needed a very complex solution quickly as the same mechanism can be used to affect other organizations.

---

3. SolarWinds

December 12th 2020, A major disclosure of a brilliant and successful attack was brought into light by FireEye when they disclosed that their network was breached by a highly sophisticated threat actor. This was just the beginning of a horror show that would change the view of security and supply chain management. This is by far the most successful espionage attack that was undetected for almost a year, evading the most advanced IDS, firewalls and endpoint protection systems. One of the main reasons being the malware/dropper was signed by the certificates of SolarWinds and was introduced into the customers network by an automatic software update in their Orion Network Management Products. The ripple effect was on such a massive scale that the Acting Director of US CISA stated "The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks", and CISA issued a directive to disconnect or power down SolarWinds Orion Products immediately.

Focus on Supply Chain: Interesting point to be noticed in here is the affected consumers were some of the major US government institutions which possess some of the critical information about the country. Compromise of such data will have the worst possible effect with regards to stability and development of the country. FireEye was the first organization to disclose the breach as it was a small mistake from the threat actor whose action to register an unknown device into the FireEye network triggered an alarm that opened the pandoras box. The defence mechanism in place at every organization failed to detect the presence of malware. The targets breached were at no fault of their own except the trust assuming all their systems were using legitimate software and the updates by vendors are clean and malware free.

SolarWinds security mechanism failed to detect they have been breached. The failure to detect their products have been tampered with and the tampered products being sent to customers over the updates is the primary reason for the attack to grow into such a large scale. The threat actor was also able test a dummy code by injecting it into updates and the customers downloading it and integrating it into production environment, which also went unnoticed. Microsoft even went on to comment “skillful and methodic operators who follow operations security (OpSec) best practices” about the attackers.

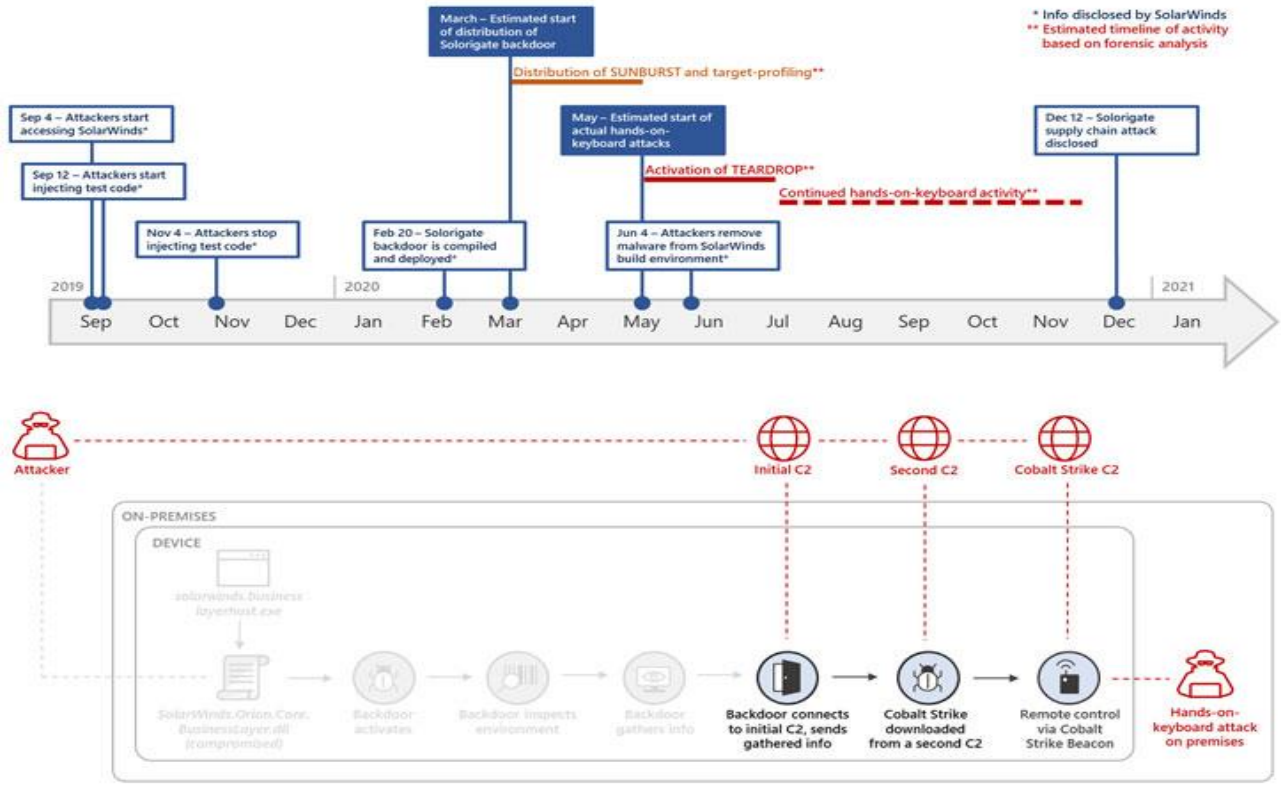

Figure 2: Microsoft Timeline of Attacks

Impact: SolarWinds hack has brought into focus about zero trust principles which states that an explicit audit has to be done and should not rely on only one mechanism for protection. It follows the approach of least privileged access and always assumes a breach and relies on real time implementation of policy. Organizations have started a manual audit of their infrastructure; Automatic updates have been disabled. Reducing the use of 3rd party services as much as possible

3. Great Suspender Malware

In November 2020, netizens warned about a chrome extension called The Great Suspender appearing malicious. Google took down the extension recently and opening the extension page redirects to 404 not found. According to issue #1263 in the extensions GitHub Repo, the new owners updated the extension to v7.18 without updating the code in GitHub which led to some users point about something fishy about the same. Although the new owners updated the extension twice the code was not pushed into GitHub except for some few manual commits. The issue was flagged due to use of Open Web analytics with remote scripts and CDN, prompting questions about user data being shared. Some users claimed it had some similarities to extensions with malware and crypto miners. This issue is similar to Nano Adblocker where new developers used the extension for malicious purpose.

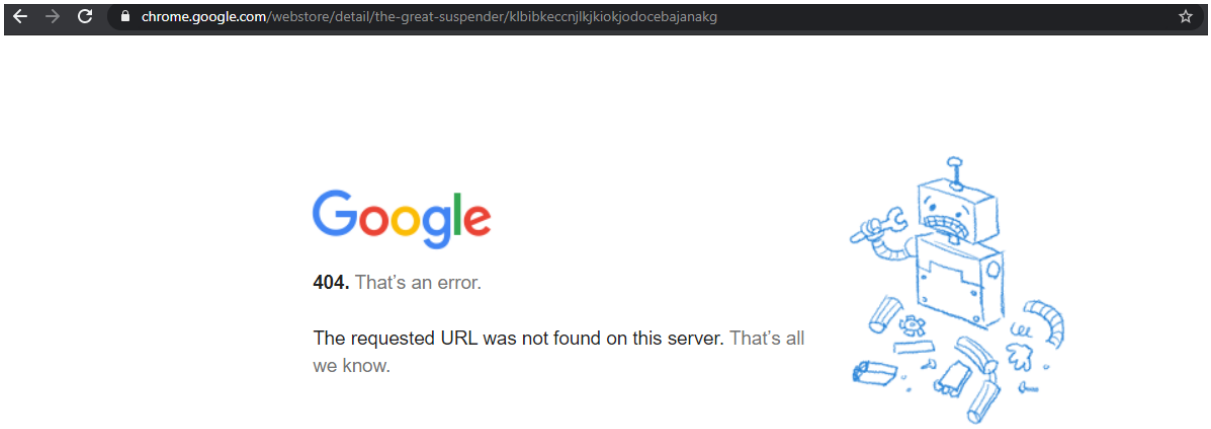

Figure 3: The Great Suspender

This Acquire and subvert model is a very dangerous threat as not every user is tech savvy and understands what happens in an update or who the author is for a product being used by them. Only a selected few user will be able to notice it which is what happened with the great suspender extension and was detected early. This is not the case every time specially for a product with millions of users, the impact area is widespread and over different demography. Solo Developers who code for passion develop a product which becomes popular, ultimately leading the original authors to sell their code to buyers who would like to work on the project. Sometimes the transactions are legitimate but like the above case, it can be leveraged into supply chain attack by malicious threat actors. Unknowing users will receive the malware in updates and fall victim to the threat actors. Millions of affected users now have the potential to infect other users in their network or contacts via the malware. With pirated software and absence of anti-virus it becomes easy for the malware droppers to go undetected and execute its payload without any obstruction. Usually, such attacks are for credential stealing and crypto-mining, but a targeted attack against organization users can lead to installation of several backdoors for later operations. A user granting privileges to such extensions can lead to abuse easily.

4. Conclusion

Supply chain attacks have existed in different forms over the years, but the sophistication increases every year and once in a while attacks like SolarWinds leave a lasting impact which prompts policy changes and change in perception about security. Implementation of zero trust policy is not completely practical as it involves manual labour and also usage of AI – ML is still in developing stages. The ever-increasing attack surface and TTP's always make defending more difficult than planning the attacks. Education of end users about supply chain attacks is a difficult task as not everyone has the capacity to understand the pros and cons of a policy. The original authors might also go rogue at any given point of time, making it really difficult task for the IT team to monitor the threats. Weaponizing 0 days with supply-chain attacks is the worst nightmare for and security team and such attacks will become more common in the future with the rise in number of malicious actors and the availability of tools in the model of services make the task much harder.

References:

1. https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach
2. https://thehackernews.com/2021/02/warning-hugely-popular-great-suspender.html
3. https://en.wikipedia.org/wiki/Stuxnet
4. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
5. https://images.theconversation.com/files/225047/original/file-20180627-112611-qdcpak.png?ixlib=rb-1.1.0&q=45&auto=format&w=1000&fit=clip
6. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
7. https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/
8. https://en.wikipedia.org/wiki/VirusBlokAda
9. https://thehackernews.com/2021/01/heres-how-solarwinds-hackers-stayed.html
10. https://thehackernews.com/2020/12/us-agencies-and-fireeye-were-hacked.html
11. https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network
12. https://www.microsoft.com/security/blog/2021/01/19/using-zero-trust-principles-to-protect-against-sophisticated-attacks-like-solorigate/
13. https://www.theregister.com/2021/01/07/great_suspender_malware/
14. https://github.com/greatsuspender/thegreatsuspender/issues/1263
15. https://github.com/greatsuspender/thegreatsuspender/issues/1304
16. https://www.reddit.com/r/chrome/comments/gg2nii/auto_refresh_extension_now_malware/fqd64jx/
17. https://github.com/NanoAdblocker/NanoCore/issues/362