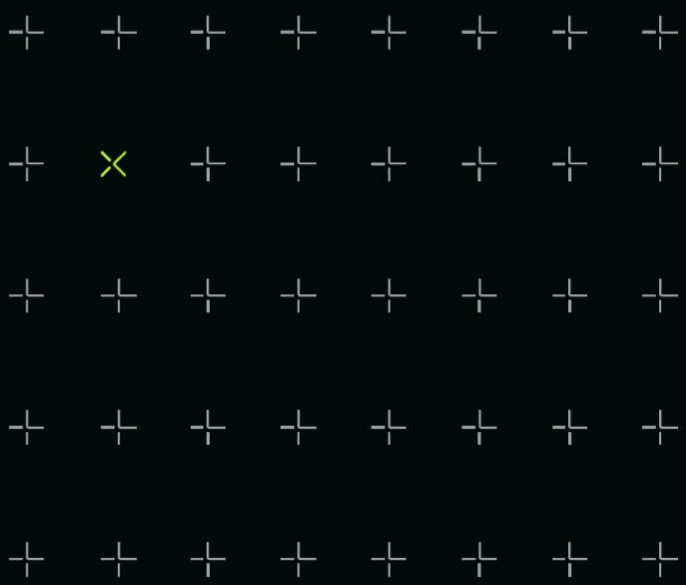
Cyber Cert Labs

Threat Intelligence Report:

XZ Opensource Supply Chain Threat Intelligence Brief April 2024



11.04.2024 TLP: Green

cybercertlabs.com

Executive Summary

On March the 29th a Microsoft engineer accidently discovered a backdoor that had been intentionally added to XZ utils software project, an open-source data compression utility that is used in almost all Linux distributions. The backdoor had been deliberately planted by a developer in the project. This developer had joined the project two years earlier and over the course of the two years earned the trust of the project maintainer by contributing bug fixes and code improvements to the project. Leveraging this trust and having been given the ability to directly approve code changes to the project the developer inserted the backdoor in February of this year.

The investigation is still in its early stages but already there are indications that the level of investment in terms of time and the sophisticated nature of the backdoor indicate that this may be a nation state effort. This is another software supply chain attack that is consistent with a recent pattern of planting backdoors into commonly used software with the aim of compromising organisations that use the tainted software.

Impact Assessment

The forensic analysis of the backdoor is ongoing, however initial analysis shows that the backdoor had specifically targeted a remote access capability in the Linux operating system called SSH. SSH provides a remote shell to a user allowing remote access to the operating system. The backdoor allows someone with knowledge of the backdoor to abuse this service to take complete control of any Linux system that the attacker can reach with the SSH service. The CVE rating for this vulnerability is a 10, the highest impact rating a vulnerability can have.

Had the backdoor not been discovered, the updated version of the xz utils code containing the backdoor would have made its way into almost all Linux distributions. This would have provided those with knowledge of the backdoor to silently compromise any Linux system with an exposed SSH service that could be reached by the attacker. The complex nature of the backdoor would have made it difficult to identify because significant technical skill had been used to hide the backdoor.

Operational Mitigation

As stated previously this software supply chain attack is another in a series that have affected organisations worldwide. While the attempted inclusion of this backdoor was deemed a near miss due to the accidental discovery of it, further software supply chain attacks are expected in the future.

In order to reduce the risks associated with such threats organisations can take a number of mitigating actions, these are:

- Indexed and searchable Software Bill of Materials (SBoMs)
- Threat Modelling and Analysis
- Assume breach capabilities
- Honeypots

Software Bill of Materials (SBoMs)

A Software Bill of Materials is a structured list of all the elements that make up an entire piece of software. It typically includes all the software packages that are contained in a

single piece of software. Standards have been developed to provide a consistent structure to these lists and therefore they can be indexed and made searchable. Having a searchable indexed data repository of SBoMs allows cyber security teams to rapidly assess the impact of any software supply chain attack. Being able to rapidly identify affected software and triangulating this with a software inventory will identify vulnerable targets. This means cyber security teams are not dependant on software vendors to provide this information and can take defence actions in hours not days. A good example is the recent vulnerability in the log4j software, a commonly used logging library. Many organisations had to wait days for individual software vendors to do this analysis.

Cyber security regulation is moving in the direction of mandating that software vendors provide customers with a SBoM for all versions of software that the release. In the USA CISA is leading the effort to develop this capability which is based on executive order that mandates a minimum level of information to be contained in an SBoM for all software products. In the EU the Cyber Resilience Act will also mandate that all software products provide an SBoM as part of the required documentation provided to organisations that purchase software. These efforts will make it possible to develop over time a detailed searchable indexed data repository of SBoMs.

Threat Modelling and Analysis

The nature of software supply chain attacks is that when they are discovered rapidly assessing an organisations exposure can be difficult. Organisations that include Threat Modelling and Analysis (TMA) as part of their cyber security operations have a capability to rapidly assess new threats as they have already built the foundational models to support this. Coupled with the SBoM analysis to identify vulnerable systems, TMA provides the additional layer on top to rapidly identify insertion points, propagation paths and key security controls to dial up. This enables a much more rapid response to these types of threats that require high levels of cyber security agility.

Assume Breach Capabilities

Often when supply chain attacks are discovered it can be the case that organisations have already been compromised. Having capabilities that assume a breach may have already occurred such as a Zero Trust and rapid network isolation or containment can help to reduce the overall impact of these types of threats.

Honeypots

Honeypots are fake services (such as SSH) which create a secured environment that looks and feels like a real environment to an attacker. Having SSH honeypots particularly in an internal environment could provide early indicators or malicious activity that could assist with any impact assessments of a potential software supply chain attack.

Conclusion

It seems that software supply chain attacks will continue as they are proving to be effective for threat actors. What is novel about this attack is the targeting of an open-source project by effectively taking it over. Also, the period of almost two years to set the stage for the attack is interesting. Whoever is behind the attack was willing to spend that time and effort and clearly felt that the return on investment would be worth it.