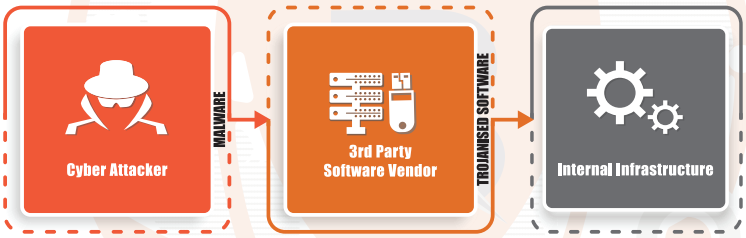
Software

Supply Chain Attack...

Backdooring Your Networks!!!

A supply chain attack, also referred to as a "third-party" attack occurs when someone gains access into your systems through an outside partner or support provider, who already has access into your infrastructure and IT environment. In recent years, this type of attacks have increased significantly as more and more suppliers and support providers have access into their client's sensitive data than ever before.

In today's digital economy, traditional software has shifted from being a driver of efficiency gains to an enabler of new customer experiences and markets. As organizations convert their business processes, the software delivery chain is fast becoming an increasingly attractive target for those looking to reach end-user customers.



In recent years, companies such as Target, Equifax and many others have faced massive data breaches and have had millions of their customer's personal identifiable information, credit card information and even bank account details exposed in the underground markets.

Supply chain attacks are increasing because of simple economies of scale, they enable "hacking at scale". The attackers can build up a 'hacking operation' against one organization and through it, are able to gain access and further compromise hundreds and thousands of other organizations and users. This is in favor of the attacker, obviously, which makes investing time and effort behind a successful supply chain attack a very lucrative proposition for the attacker. Once an attacker establishes foothold in a vendor system, they have access to new targets without having to invest in building up new 'hacking operations.' The impact of a software supply chain attack is continuous and widespread.

The path of least resistance.

Software supply chain attacks are gaining popularity on an exponential basis as they are a relatively easy way into soft targets, which in turn, gives the attackers access into their customer base. This line of attack is easier as the attacks are carried out using trusted applications. Third party contractors and suppliers provide stealthy gateway to hard-to-reach targets.

The complexity of detection.

Software supply chain attacks are hard to detect as most attackers install backdoors into legitimate software/firmware, they are rarely detected by IDS/IPS deployed onto the organizations. Moreover, vendors can connect to internal networks without proper checking for possible threats.

BEETLES
THE HACKER'S APPROACH

+8802-9513744
query@beetles.io
www.beetles.io

Aziz Bhaban
93 Motijheel C/A (3rd Fl.)
Dhaka-1000, Bangladesh