



Exploiting Trust Relationships: Attacking the Supply Chain.

Mr Earl Carter¹

¹*Cisco*

The threat landscape is constantly evolving and incorporating new attack vectors. Users have been a favorite target over the last few years, but now we have seen an increase in malware attacks utilizing the supply chain. During this talk I will explain how an attacker can use the supply chain to corrupt a third party piece of software and thus deliver malware into a network through a trusted avenue. To illustrate the effectiveness of supply chain attacks I will provide an in-depth analysis of two major supply chain attacks that our company analyzed in 2017: Nyetya and CCleaner. Nyetya caused major disruption in the Ukraine by targeting the me.doc tax software that was utilized by 80% of the companies in the Ukraine and CCleaner targeted high tech and telecommunications firms. Finally, I will explore possible ways to defend against this upcoming threat vector.