Name: AVIVORE *(Context)*
Country : China
Motivation :Information theft and espionage
First seen : 2015
Description : (Context) Until now, most prominent supply chain intrusions have been 'vertical'; initial victims are typically Managed Services Providers or software vendors leveraged by attackers to move up or down the supply chain. However, since summer 2018, Context Information Security has been investigating a series of incidents targeting UK and European Aerospace and Defence that are best described as 'horizontal'. Advanced attackers have been leveraging direct connectivity between suppliers and partners who are integrated into each other's value chains. We have been tracking this activity under the codename AVIVORE. Affected victims include large multinational firms (Primes) and smaller engineering or consultancy firms within their supply chain (Secondaries). Context has worked closely with victims, the National Cyber Security Centre (NCSC), security organisations, and law enforcement agencies across Europe to reduce impact and prevent further compromise.
Observed : Sectors: Aerospace, Automotive, Energy, Satellites.
Countries: UK and Europe.
Tools used :Mimikatz, PlugX, Living off the Land.
Information: <https://www.contextis.com/en/blog/avivore>