Malware Injection into Client Software

The attackers insert their malware to run alongside (or in) third-party software. Stuxnet and Bonadan did this.

DETECTION

User and Entity Behavior Analytics
Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Stuxnet
Bonadan

https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury

https://attack.mitre.org/techniques/T1554

EXPV1_0421

Backdoors™ & Breaches

PERSISTENCE

Created by: BLACK HILLS | Information Security