Event Triggered Malware

The attackers' malware triggers only when specific events occur. For example, when a specific DLL or service is started.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
SIEM Log Analysis

TOOLS

Tsunami
WMI Malware

https://attack.mitre.org/techniques/T1546/014

https://youtu.be/XFk-b0aT6cs

EXPV1_0421

Backdoors™ & Breaches

PERSISTENCE

Created by: BLACK HILLS | Information Security