Minerva Anti-Evasive Platform

MINERVA

L'approccio originale della Piattaforma Minerva

La maggior parte dei malware non ancora identificati usa diverse tecniche evasive per superare i controlli dei sistemi di sicurezza, tutte però basate sulla stessa premessa...

si nascondono in un contenitore per assumere le sembianze di un file legittimo...

e rimangono nascosti fino a che non identificano un ambiente ideale per uscire dal contenitore e cominciare ad agire.

Per capire se l'ambiente è quello giusto per uscire allo scoperto, inviano una serie di query...

Mentre il malware sta completando la sua "analisi ambientale", il codice maligno viene mantenuto compresso e crittografato, così da rendere impossibile la sua identificazione. L'estrazione e l'esecuzione del codice maligno viene messa in atto quando il malware si è assicurato di trovarsi in un ambiente idoneo, dove non sono attivi gli strumenti di sicurezza che abbiamo citato prima.

Ed è proprio in questo caso che entra in gioco la Piattaforma Minerva VR™

PATENTED

Minerva VR™ è costruito su una semplice premessa: poiché il malware non estrae e non esegue il codice maligno in un ambiente ostile, Minerva simula un tale ambiente e impedisce in questo modo l'esecuzione del malware...

...così il malware rimane "addormentato" nel suo contenitore per un tempo indefinito.

Minerva valorizza inoltre l'intero sistema di sicurezza, perché notifica agli altri strumenti la presenza di un malware sconosciuto.

Gruppo Daman S.r.l
T. +39 06 5159281

gruppo Daman
Passione e Innovazione

info@daman.it
www.daman.it