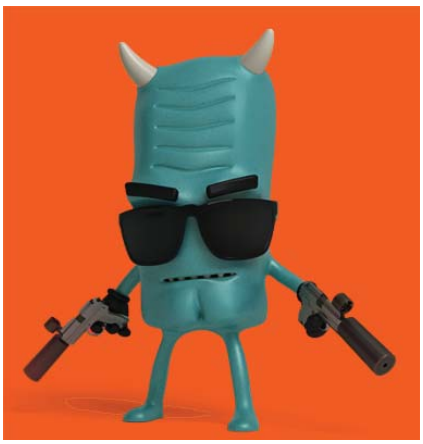
MINERVA

gruppo Daman
Passione e Innovazione

Minerva Anti-Evasive Platform

Prevenire gli attacchi Malware con l'inganno



La **criminalità Cyber** è sempre più sofisticata e in grado di sviluppare tecniche di attacco che superano le fragili barriere della sicurezza informatica.

Ogni giorno vengono prodotti e distribuiti "**codici malevoli**", ignorati dai software antivirus, mentre in altri casi questi codici vengono nascosti all'interno di "**contenitori**", facilmente reperibili nella darknet.

Sono "**tecniche evasive**" che consentono ai **malware** di superare le difese, infiltrarsi nella rete e attendere il momento giusto per colpire.

E' quindi necessario modificare il paradigma di Cyber Defence, quello classico dei Software AntiVirus, e attivare un modello di prevenzione della sicurezza della postazione utente **basato sull'inganno**. Il malware nascosto nel suo contenitore, prima di attivarsi e colpire, farà una serie di verifiche per accertarsi di essere nell'ambiente adatto al suo scopo e quindi di non trovarsi in un ambiente per lui ostile. L'inganno consiste proprio nel **simulare un ambiente ostile**, suggerendo al codice malevolo di restare nascosto, fino alla sua definitiva eliminazione.

Minerva

Per affrontare e risolvere questo problema il **Gruppo Daman** distribuisce in Italia **la piattaforma Minerva**, una soluzione innovativa che è in grado di neutralizzare il potenziale offensivo dei malware "evasivi" con una tecnica basata proprio sull'inganno. La **piattaforma anti-evasione** di Minerva sfrutta la natura stessa dei malware evasivi: utilizzando una tecnica basata sull'inganno, Minerva blocca gli attacchi progettati per eludere le difese esistenti, creando un ambiente che il malware percepisce come ostile e non sicuro per l'esecuzione.

I principali punti di forza di questo approccio innovativo sono:

- **Prevenzione da attacchi ancora sconosciuti** - riducendo drasticamente gli attacchi evasivi con un approccio radicalmente diverso dalla tipica sicurezza delle postazioni di lavoro.
- **Efficientamento nella gestione degli allarmi** - eliminando la dispendiosa attività di "inseguimento" degli allarmi, bloccando i malware già nella fase di preinstallazione.
- **Riduzione del carico di lavoro a livello amministrativo** - rendendo sicure le postazioni di lavoro con un processo di distribuzione rapido ed efficace e senza la necessità di introdurre onerose attività di manutenzione.
- **Valorizzazione degli investimenti già effettuati** - rafforzando la protezione di lavoro in una logica di integrazione rispetto all'architettura AntiVirus già esistente, ed evitando i rischi e i costi di un processo di "replacement".

Blocca il conto alla rovescia degli attacchi evasivi

Minerva fornisce la tranquillità che eventuali attacchi furtivi e sconosciuti saranno comunque bloccati prima dell'infezione e prima che questi possano generare danni.

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

gruppo Daman
Passione e Innovazione

info@daman.it
www.daman.it

Minerva Anti-Evasive Platform

MINERVA

L'approccio originale della Piattaforma Minerva

La maggior parte dei malware non ancora identificati usano 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

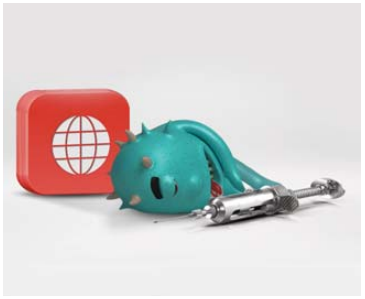
Principali funzionalità della piattaforma

- **Simulazione di un ambiente ostile** - Minerva fa apparire ogni postazione di lavoro come un ambiente ostile per i malware evasivi, simulando la presenza di prodotti di sicurezza avanzati e suggerendo implicitamente al malware di mantenersi nascosto nel suo contenitore senza rivelare la sua vera natura.

In questo modo Minerva:

- blocca ogni attacco di tipo "evasivo" senza la necessità di identificare la presenza e la tipologia del malware
- riduce le onerose attività di "indagine" innescate da falsi allarmi o da allarmi irrilevanti
- riduce il rischio di subire danni a causa di attacchi sconosciuti.

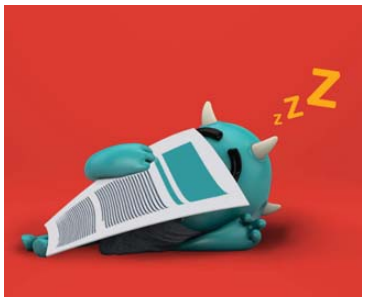
- **Prevenzione da attacchi Memory Injection** - Minerva previene attacchi che usano tecniche di Memory Injection, tra queste le tecniche fileless, con cui i malware tentano di nascondersi all'interno di processi legittimi, evitando il rilevamento.



In questo modo Minerva:

- blocca l'attacco prima che possa infettare il sistema ed evita ogni accesso a dati sensibili
- elimina i rischi di un errore umano
- identifica in modo automatico i processi non autorizzati.

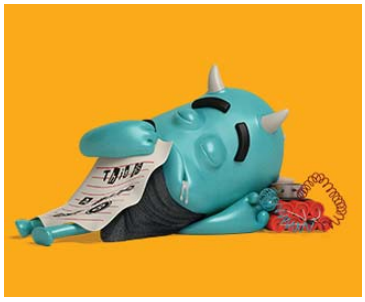
- **Prevenzione da Documenti infetti** - Minerva previene attacchi sofisticati basati su codice maligno che si nasconde all'interno di file legittimi.



In questo modo Minerva:

- blocca malware che usano tecniche evasive nascondendosi all'interno di normali documenti
- consente di trarre vantaggio dall'uso delle macro al fine di ottimizzare le operazioni di business, evitando al contempo i rischi di sicurezza che questo modo di operare comporta.

- **Protezione dai Ransomware** - Minerva previene attacchi Ransomware, usando le funzionalità sopra esposte: Simulazione di un ambiente ostile, Prevenzione da attacchi Memory Injection, Prevenzione da Documenti infetti.



In questo modo Minerva:

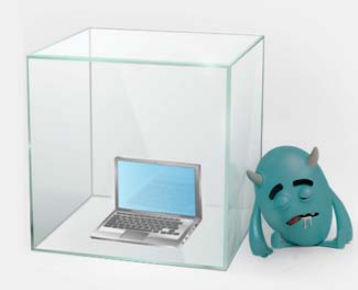
- consente di salvaguardare i dati di un'organizzazione
- evita la condizione di dover cedere a un ricatto.

Minerva Anti-Evasive Platform

MINERVA

- **Vaccinazione della postazione di lavoro** - Minerva è in grado di usare gli "infection marker" generati dal malware per procedere a una rapida ed efficace "vaccinazione" delle postazioni di lavoro dell'organizzazione.

  La vaccinazione preventiva può essere eseguita anche quando un attacco globale è in corso, evitando così di esporre al rischio infezione le postazioni di lavoro.



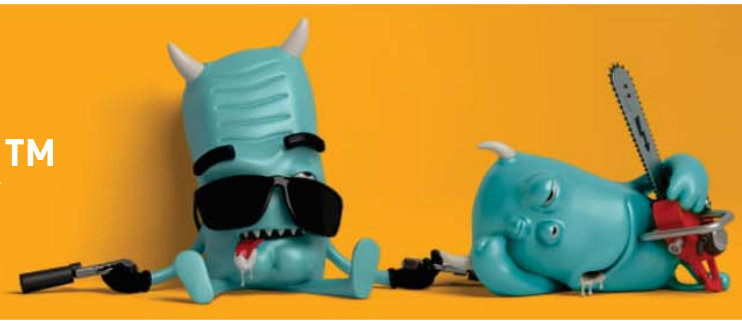
- **Integrazione** - Minerva è una piattaforma sviluppata con l'obiettivo di integrarsi con le soluzioni e le procedure di sicurezza già implementate, andando quindi ad aggiungere valore, grazie alle sue funzionalità esclusive, al sistema di Cyber Defence dell'organizzazione.

- **Rapidità di implementazione** - Minerva è una soluzione studiata per garantire un processo di implementazione rapido e indolore, con un impatto molto minore rispetto a progetti di ammodernamento di architetture AntiVirus già presenti all'interno dell'organizzazione.

  In questo modo Minerva consente di ottenere i seguenti vantaggi:

  - il più elevato tasso di prevenzione della categoria, che scaturisce dalla combinazione della piattaforma Minerva con l'architettura di sicurezza corrente
  - una consistente riduzione dei costi operazionali di manutenzione, senza la necessità di passare attraverso tediosi proessi di replacement
  - rapidità di distribuzione e velocità di upgrade, con la capacità di rilasciare Minerva in produzione a una media di 10.000 postazioni di lavoro a settimana
  - il più basso impatto e consumo di risorse nella categoria delle soluzioni di sicurezza.

Minerva VR™



La fine dei Malware evasivi

Daman

Il **Gruppo Daman** seleziona prodotti innovativi e sofisticati mirati al mercato dell'Information and Communication Technology, per la successiva distribuzione sul territorio italiano.

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

gruppo Daman Passione e Innovazione

info@daman.it
www.daman.it