MINERVA

gruppo Daman
Passione e Innovazione

Solution Brief

Minerva per le Infrastrutture critiche

Gli attacchi informatici ai sistemi di controllo industriale - ICS - e ai sistemi di controllo e acquisizione dati - SCADA - sono in continuo aumento. Il tradizionale sistema di difesa delle infrastrutture critiche, basato essenzialmente sul loro totale isolamento dalla rete internet, oggi non è più ipotizzabile. Le infrastrutture critiche hanno ormai adottato la filosofia industriale dei sistemi IoT e interagiscono con la rete, diventando un target per attacchi dannosi che hanno lo scopo di "colpire" risorse che sono critiche e vulnerabili per definizione.

L'attacco alla rete elettrica ucraina o la diffusione di malware come BlakEnergy e Energetic Bear/Dragonfly, i quali erano stati disegnati proprio per attaccare la rete ICS/SCADA, stanno a dimostrare che il rischio di subire attacchi sulle infrastrutture critiche è molto concreto.

Queste campagne hanno infatti evidenziato come le difese esistenti non siano più in grado di mantenere le infrastrutture critiche al sicuro.

Attacchi che superano le difese esistenti

Con lo scopo di mantenersi "nascoste" e di non essere rilevate dai sistemi di sicurezza esistenti, le minacce che hanno come obiettivo le infrastrutture critiche vengono ingegnerizzate utilizzando nuove tecniche "evasive", in grado di superare i controlli degli strumenti di sicurezza, tra i quali citiamo i classici AV/EDR (Anti Virus/Endpoint Detection & Response), anche se di nuova generazione.

Migliaia di nuove "tecniche evasive" sono a disposizione dei criminali informatici, e sono tecniche che eludono la sorveglianza degli strumenti di sicurezza e che generano una reazione così tardiva da non essere in grado di neutralizzare il potenziale dannoso dei codici malevoli.

Spesso, la minaccia viene scoperta quando il sistema ICS/SCADA risulta già compromesso, cosa che può avere un impatto devastante sulle infrastrutture critiche.

Minerva Anti-Evasion Platform

La Piattaforma Minerva protegge gli ambienti ICS/SCADA, sfruttando a suo vantaggio la particolare natura dei malware "evasivi" utilizzando una tecnica basata sull'inganno. Minerva simula la presenza di un ambiente ostile, non adatto ad essere l'obiettivo di un attacco, suggerendo al malware "evasivo" di restarsene inattivo all'interno del contenitore nel quale si nasconde.

Questa particolare tecnica di difesa non interferisce e non si sovrappone alle tecniche già adottate dagli altri strumenti di sicurezza implementati, diventando complementare ad esse.

Indirizzando una varietà di potenziali scenari di attacco, la piattaforma Minerva ha un'architettura modulare, dove ogni modulo va a contrastare una specifica tecnica evasiva e quindi a neutralizzare una potenziale minaccia.

Tra queste tecniche possiamo citare:

- ransomware attack;
- malware file-based e fileless;
- weaponized documents malware;
- environment-aware malware.

Highlights

- ***Previene malware zero-day, avanzati ed evasivi*** *come nel caso degli attacchi memory injection, malicious document, environmental-aware.*
- ***Protezione per i sistemi legacy*** *usa un unico pacchetto di installazione per tutti i sistemi operativi Windows, di qualsiasi generazione.*
- ***Nessun prerequisito necessario*** *consente una rapida implementazione del prodotto, evitando qualsiasi interferenza con le applicazioni "legittime" e riducendo al minino l'impatto sul lavoro di amministrazione.*
- ***Installazione efficace e minima manutenzione*** *garantisce la massima protezione della postazione di lavoro a un costo minimo.*
- ***Leggero*** *occupa meno di 20 Mb di spazio disco e non ha impatti significativi sulle performance della postazione di lavoro, rendendo così possibile la sua distribuzione anche su sistemi mission-critical.*

Finalmente, una soluzione di sicurezza della postazione di lavoro che non aggiunge overhead

Per evitare di aggiungere overhead e peggiorare le prestazioni della postazione di lavoro, la piattaforma Minerva è passiva e molto leggera, una soluzione per sistemi Windows che segue l'approccio "installa-e-dimentica". Distribuita con un unico "installer" il quale utilizza solo una minima quantità di memoria (RAM) e di risorse elaborative (CPU), la piattaforma Minerva non richiede prerequisiti per essere installata o per essere aggiornata, e non richiede un "reboot" dei sistemi dopo la sua installazione.

Gli agenti non richiedono una connessione di rete e non fanno affidamento su file di definizione o su "firme" per essere efficaci e svolgere la loro funzione. Queste caratteristiche gli permettono di agire anche su ambienti isolati, come possono appunto essere gli ambienti ICS/SCADA.

La console di management della piattaforma Minerva, consente una gestione centralizzata con cruscotti e report che aiutano a rispettare i requisiti di compliance mentre la piattaforma migliora significativamente il proprio livello di sicurezza.

Benefici:

- Nessun prerequisito di installazione (es. .NET, C++, Redist ...)
- Nessun reboot richiesto durante l'installazione, la disinstallazione o l'aggiornamento
- Agente particolarmente leggero che usa meno di 20 Mb di Ram e meno dell'1% di CPU
- Rapidità e facilità di distribuzione per ogni singola MSI per 32/64-bit Microsoft Windows Desktop e Serving Operating Systems
- Supporta tutte le versioni di sistema operativo Microsoft (incluse le versioni legacy)
- Nessuna esigenza di aggiornare le "signatures" o di attivare connessioni di rete
- Le postazioni di lavoro sono protette anche quando non sono connesse alla rete

Minerva Management Console:

- Supporta l'integrazione con SIEM/Syslog e SMTP
- Autenticazione via LDAP/AD
- Un server di management supporta fino a 20.000 postazioni di lavoro
- Un livello di scalabilità che consente di indirizzare le esigenze delle grandi organizzazioni

Minerva Labs

Minerva Labs è una società che fornisce soluzioni innovative per la protezione delle postazioni di lavoro, in grado di proteggere le gradi organizzazioni dai moderni attacchi a cui sono sottoposte, con un approccio che gli consente di intervenire efficacemente ancora prima di identificare la minaccia e soprattutto prima che l'attacco produca danni all'organizzazione.

La Piattaforma Minerva labs Anti-Evasion blocca le minacce sconosciute le quali sono in grado di superare le attuali difese garantite dai tradizionali sistemi di sicurezza della postazione di lavoro. La Piattaforma Minerva Labs blocca queste minacce attraverso una tecnica basata sull'inganno e quindi sulla percezione che il malware ha dell'ambiente in cui si trova. Questa tecnica consiste nel simulare un ambiente ostile per un attacco, suggerendo in questo modo al malware di restare inattivo, vanificando il suo potenziale offensivo prima che questo possa provocare dei danni all'organizzazione.