MINERVA

Solution Brief

Minerva for Critical Infrastructure

Malicious attacks on industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA) environments are on the rise. The traditional defense — relying on critical infrastructure being isolated or air-gapped — is no longer feasible. Critical infrastructure facilities increasingly adopt the concept of Industrial IoT and interact with networks and equipment that allows mainstream and targeted threats to affect critical and vulnerable resources.

The feasibility of critical infrastructure information security incidents is far from theoretical, as the industry has learned from the attacks on the Ukrainian power grid, the IoT botnet (Mirai) and malware such as BlackEnergy and Energetic Bear/Dragonfly, which were specifically used to target ICS/SCADA networks. These campaigns clearly indicate that existing defenses are no longer sufficient to keep critical infrastructure secure.

Attacks That Evade Existing Defenses

In an effort to remain undetected, advanced threats targeting critical infrastructure are specifically engineered to use evasive techniques to bypass existing security controls, including traditional and next-generation AV/EDR tools. With hundreds to thousands of evasive techniques available to attackers, security tools that rely on known indicators, signatures, behavioral models or patterns will simply not catch such threats until it's too late. At best, the evasive malware will be detected after the ICS/SCADA network has been compromised. The risk of detection being too little, too late, can have a devastating impact on critical infrastructure operations, as well as public health and safety.

Minerva Anti-Evasion Platform

A key challenge in protecting SCADA and ICS systems is that many endpoint security solutions are resource intensive and support a limited number of operating system (OS) versions. The Anti-Evasion Platform protects ICS/SCADA environments by exploiting the very nature of evasive malware and can be deployed to Windows legacy systems as well as the latest operating systems with a single installation package. Minerva blocks attacks designed to evade existing defenses, by creating an environment the malware perceives as hostile and unsafe for execution. Minerva accomplishes this using patented techniques that don't overlap with the approaches employed by other security tools.

Addressing a variety of attack scenarios, Minerva Anti-Evasion Platform includes multiple modules that reinforce each other to block unknown threats that employ different evasive techniques, such as file-based and fileless malware, ransomware attacks, malware delivered in weaponized documents and environment-aware malware.

Highlights

- ***Prevent zero-day, advanced and evasive malware*** *such as memory injection, malicious document and environmentally aware attacks*
- ***Protection for legacy systems*** *with a single installation package for Windows operating systems*
- ***No need for any pre-requisites*** *or kernel level drivers allowing for a quick deployment, no interference with legitimate applications and low administrative overhead*
- ***Effective upon installation with low maintenance -*** *Protects endpoints with low ongoing OPEX cost model*
- ***Lightweight -*** *takes up less than 20 MB disk space and ready to be deployed on any mission-critical production system without impacting its run-time performance or storage requirements*

Finally, Endpoint Security That Doesn't Add Operational Burden

To ensure significantly low operational burden, Minerva Anti-Evasion Platform is a passive, ultra-lightweight "set-it-and-forget-it" security solution for embedded and traditional Windows systems. Deployed as a unified installer with minimal system memory (RAM) and CPU usage, Minerva's Anti-Evasion Platform requires no reboots and has no prerequisite requirements for installation or upgrade.

The Minerva agent does not require an internet or management server connection, and doesn't rely on definition files or signatures to be highly effective. This makes it ideal for use in air-gapped and otherwise isolated environments. The Minerva Management Console server provides centralized management, dashboards and reports that help meet compliance requirements while meaningfully improving the enviroment's security posture.

Operational Benefits:

- No installation prerequisites
  (for example - .NET, C++ Redist, etc...)
- No reboot required during installation, uninstallation or upgrade
- Lightweight and low footprint
  - Uses < 20MB RAM and < 1% CPU
- Fast and easy deployment of single MSI for both 32/64-bit Microsoft Windows Desktop and Server Operating Systems
- Supports all Microsoft Windows OS versions (including legacy systems such as Windows XP, Embedded Systems, POS, etc...)
- No signature updates, or internet connectivity required
- Endpoints are protected even when disconnected from organization's network

Minerva Management Console:

- Supports integration with SIEM/Syslog and SMTP
- Authentication via LDAP/AD
- One management server supports up to 20k endpoints
- Easily Scalable to support very large organizations

About Minerva

Minerva is an innovative endpoint security solution provider that protects enterprises from today's stealthiest attacks without the need to detect threats first, all before any damage has been done. Minerva Anti-Evasion Platform blocks unknown threats which evade existing defenses by deceiving the malware and controlling how it perceives its environment. Without relying on signatures, models or behavioral patterns, Minerva's solution deceives the malware and causes it to disarm itself, thwarting it before the need to engage costly security resources.