MINERVA

Solution Brief

Using Minerva's Anti-Evasion Platform for Incident Response

Minerva's Anti-Evasion Platform automatically stops threats that are designed to evade other security tools, such as malware sandboxes as well as traditional and "next-gen" anti-malware products. While the solution is often deployed as a proactive measure to strengthen endpoint security across the enterprise, it is also a powerful tool in the hands of an incident response team reacting to an intrusion. In this scenario, Minerva not only disables malware that bypassed security controls, but also contains it to give responders time to contain and eradicate the threat.

Prevention Without Detection

102 infections PREVENTED

The patented technology behind Minerva's Anti-Evasion Platform interferes with attempts to evade security software, compensating for weaknesses inherent to any detection-based anti-malware approaches, such as those employed by antivirus products. Instead, Minerva's solution deceives evasive threats in a way that causes them to self-convict, disarming themselves if they engage in steps to get around other security tools. In other words, it can prevent infections by evasive malware without attempting to detect malicious software by scanning files or processes for patterns associated with previously-seen malware.

Minerva's approach augments existing enterprise security controls without overlapping with their functionality. It's especially effective against threats programmed to avoid forensics environments to stay under the radar of security vendors, as well "fileless" attacks that employ memory injection techniques and malicious document files. Enterprises that have deployed Minerva's Anti-Evasion Platform proactively have seen a significant decrease in the amount of infections. Moreover, incident response teams that have deployed Minerva's solution during an active malware outbreak were able to quickly neutralize the threat and rapidly return the organization to steady state.

Neutralizing Malware During Incident Response

When malware finds its way into the enterprise, incident responders need to react quickly to locate and contain the malicious software on its path towards eradicating the adversary's presence from the environment. Armed solely with investigative Endpoint Detection and Response (EDR) and forensics tools, IR teams often engage in manual steps to terminate the offensive processes or otherwise disable the attacker's tools and prevent malware from spreading. This is a time-consuming, error-prone effort that requires deep expertise and can quickly drain the individuals involved in the efforts that often feel like the game of Whac-A-Mole. Since the malware involved in the incident somehow found its way past the organization's security controls, deploying Minerva's Anti-Evasion Platform as part of the IR process often helps contain the threat automatically and quickly. The solution can automatically neutralize such evasive malware in several ways, including:

Key Benefits:

- *Effective prevention against malware designed to avoid forensics environments*
- *Quickly neutralize active malware outbreaks and rapidly return to steady state*
- *Contain outbreaks immediately through endpoint vaccination that can be deployed enterprise-wide*

- Make all endpoints in the enterprise appear to malware like forensic environments that evasive threats are often programmed to avoid, deceiving such malicious programs into terminating their own processes or putting themselves to sleep.
- Prevent "fileless" or packed malware from placing its malicious code in memory space of another process, causing such malicious programs to break, terminate themselves, and cutting off their ability to reinfect systems using memory injection techniques.
- Disarm malicious document files, which often get past other anti-malware tools and are used by adversaries for both initial infections as well as to propagate within the organization as innocuous-looking email attachments.

By deploying Minerva's Anti-Evasion Platform during incident response, even if the environment is infested with malware, the organization can neutralize the threat automatically, so it has the opportunity to eradicate the infection and return the enterprise to a normal state of operations.

Containing Malware Though Vaccination

Another powerful capability of Minerva's Anti-Evasion Platform allows incident response teams to "vaccinate" endpoints against certain malware families to contain the attack. Malicious programs often leave infection markers on the endpoint to avoid infecting it twice and risk operational issues and detection. Responders can use this behavior to their advantage by mimicking the presence of the markers to vaccinate endpoints from the associated threats.

Minerva gives customers the ability to centrally simulate the presence of mutex-based injection markers across all enterprise endpoints with a few clicks. The ability to simulate (rather than actually create) the infection markers allows the solution to be highly selective regarding how and when it reveals the presence of the vaccine. This approach avoids cluttering the system with unnecessary artifacts, doesn't interfere with legitimate applications and doesn't confuse end-users.

Containment Without Business Disruption

Minerva's Anti-Evasion Platform restrains active malware even if the solution wasn't preemptively deployed in the enterprise. Such actions, automatically performed on the endpoints, allow responders to contain the threat in a manner that's more precise and less disruptive to business than the traditional steps of taking full systems or even networks offline.

Minerva's lightweight agents are designed for rapid deployment across all enterprise endpoints. They are easy to rollout without manual steps, don't consume system resources in any noticeable way, avoid interfering with malicious applications and require no reboots. As the result, Minerva's solution is a powerful and unique addition to the incident responder's toolkit.

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.

Headquartered in Petach Tikva, Israel, and with offices in New York and Atlanta, Minerva boost customers' existing defenses without the need to embark upon a costly and risky overhaul of their entire endpoint security architecture. To learn more about Minerva, visit **www.minerva-labs.com.**