Making Anti-Malware Solutions More Effective

An Interview With
Eddy Bobritsky
CEO, Minerva Labs

ANTI-VIRUS SOLUTIONS have always suffered from the challenge that attackers can evade detections, even when the AV approach incorporates advanced methods beyond signatures. As a result, most users of anti-virus express disappointment with the efficacy of the control. Minerva Labs is a start-up cyber security firm that has developed a novel means for dealing with this problem, and their approach focuses directly on this issue of malware evading the known protections.

What Minerva does specifically is introduce an anti-evasion control for malware protection on the endpoint. With the Minerva technology, anti-malware solutions are thus made better, because evasion is no longer a strategic offensive option. We recently connected with Eddy Bobritsky, CEO of Minerva to ask him about this unique approach to anti-malware and how his solution is changing the game in endpoint security.

EA: What is meant by evasion in the context of anti-malware?

EB: As anti-virus solutions evolve, the adversaries aren’t standing still or “retiring” simply because AV approaches now incorporate artificial intelligence and other advanced methods. These very advancements are causing attackers to implement measures for evading detection by anti-virus and other anti-malware controls. Defenders improve in response to the attackers, which causes the attackers to improve, and so on. Such cat-and-mouse dynamics are inherent to the cybersecurity industry. Minerva Labs’ mission is to disrupt this cycle by turning the very strength of the adversaries—their incentive and ability to evade—into an advantage for the defenders.

EA: How does the Minerva technology work?

EB: Minerva’s Anti-Evasion Platform interferes with attempts to evade other security measures. We do this by using elements of deception on the endpoint in a way that causes malware to self-convict, instead of attempting to distinguish between legitimate and malicious programs. For example, malicious software is often designed to terminate its execution or go to sleep if it’s being analyzed. This extends the time during which the threat can remain undetected. One of Minerva’s approaches involves lying to malware in a way that causes it to believe it’s always
being analyzed. By simulating the environment that such malware considers hostile, we cause the malicious program to choose not to run. This is just one illustration of how our way of protecting endpoints is effective against never-before-seen threats, defending enterprises even against malware that AV cannot detect.

**EA:** Does the Minerva solution complement or replace existing anti-virus products?  
**EB:** Our Anti-Evasion Platform does not replace AV, it augments the AV to cover the gap that any AV leaves on the endpoint, even those products that incorporate advanced techniques such as machine learning. To accomplish this, our solution resides on the endpoint together with anti-virus software. This approach allows us to focus on the problem we’re uniquely qualified to solve—causing evasion techniques to stop working—while allowing anti-virus vendors to stop threats that are not as evasive. Many customers used Minerva’s Anti-Evasion Platform to augment their existing AV products, forgoing the expense and risk of replacing these products with others.

**EA:** How advanced has malware become in recent years?  
**EB:** Adversaries increasingly incorporate some form of evasion throughout the attack process. For example, in the 99% of exploit kit attacks that Minerva examined, at least one evasion tactic appeared somewhere along the path. Given the reactive nature of detection-based approaches to protecting endpoints, attackers continue to succeed at compromising enterprise defenses. Unfortunately, evasion techniques and tools are now available even to novice adversaries and are often incorporated into even commodity threats. The more evasive the malware, the greater the chances that AV software will fail at stopping it. It’s the opposite with our solution: The more evasive the threat, the greater the likelihood that it will be subject to our interference.

**EA:** What are some new features you’re working on for your platform?  
**EB:** Just to name a few: We’ve seen an increasing demand for our Anti-Evasion Platform from not only end-user enterprises, but also from Managed Service Provider. In response, we’re releasing functionality that makes its especially convenient for our MSP partner to deploy and oversee our solution. In addition, we’re continuing to enhance our unique value proposition for incident responders who seek to contain malware outbreaks with incredible granularity. This includes the ability to “vaccinate” endpoints against malware families that avoid infecting the same system more than once—a capability we’re continuing to expand based on feedback from the field. Also, we’re expanding our Critical Asset Protection features that involve principles of deception to protect special-purpose devices such as ATMs and Industrial Control Systems.