MINERVA

Case Study

Worldwide Shipping Leader Guards Thousands of Endpoints Against Global Ransomware Attacks with Minerva Labs Innovative Malware Prevention Solution

The client is a leading worldwide shipping company with annual sales of $2-3 billion and over 4000 employees. The company provides global and regional services and has been pursuing route expansion to support supply chains in the world's emerging markets. With approximately 100 offices in different countries, they have made massive investments to modernize and centralize IT in recent years.

At client headquarters, the global CISO and his team are responsible for all things security related: implementing new information security solutions, regulations, methodology, and security awareness. The CISO also runs a SOC team that monitors their global network and systems 24/7 and gathers information on events and remediation.

The Challenge

The major concern for this client was ransomware infections. Because they have offices all over the world, they were vulnerable to the worldwide, worm-like attacks that have become increasingly prevalent and insidious in recent years. They were dealing with an average of two ransomware events per week across various offices, and were finding the attacks very hard to block and prevent.

They found that signature-based antivirus (AV) solutions were not sufficient, and estimate that AV was only blocking half of the attacks. Signature based solutions are on the most part, not able to find the malicious, sophisticated exploits, including the most virulent ransomware families. The client needed an effective complement to their existing solutions that wouldn't eat up memory or processing power.

The CISO recognized that once cybercriminals find a good attack surface that is also lucrative, more attackers using the same method will make attempts. The client saw within a year that the relatively small amount of attacks was increasing rapidly in number, variety, and sophistication. The CISO knew they had to find a powerful solution because the attacks would not slow down or stop. He recognizes that every organization needs a solution in addition to AV in order to detect unknown (not yet identified) attacks. When he originally sought a malware solution three years ago, most options were signature-dependent. Looking for a different, more effective approach, the CISO identified Minerva Labs.

The Solution

Minerva Labs award-winning Anti-Evasion Platform delivers prevention before detection by keeping malware in a constant sleep state. The solution neutralizes the malware before it can be installed, and before any damage is done. By simulating a hostile environment on every endpoint, Minerva Labs' technology tricks the malware so it will never activate.

The Minerva Labs Anti-Evasion Platform also works with an organization's existing security infrastructure by sharing with these solutions, threat intelligence on evasive malware that Minerva Labs prevented. This further integrates a company's defense-in-depth measures and increases the value and effectiveness of each component. Minerva Labs endpoint agent is lightweight, doesn't have pre-requisites, and doesn't necessitate rebooting endpoints.

Minerva Labs analytics for this client show that at least six high-risk Trojan and ransomware attacks were blocked (including Locky, Bandarchor, and Dropper). Additionally, 585 BEDEP fileless malware attacks were blocked, 3,800 exploit kit attacks were prevented, and tens of thousands of PUPs were eradicated (adware, spyware, and other "low-risk" programs that can lead to data leakage and should be kept off networks and endpoints).

The Result

Most importantly, the CISO reports that ransomware attacks stopped once Minerva Labs was installed. The Minerva Labs Platform blocked more than 95% of attempted attacks. Because fewer infections were able to take hold, the CISO's team didn't need to investigate endpoints or reinstall them, saving significant time and resources. They are able to see that many events are being blocked but they don't have to do anything about them. They know they are better protected from sophisticated malware, ransomware attacks, and new models of exploit kits — threats that their AV solution was unable to detect. The CISO is more aware of vulnerabilities and able to develop a deeper understanding of the environment they are dealing with.

The client reported that the small footprint of the agent on the endpoint is one of biggest benefits of Minerva Labs Anti-Evasion Platform. Minerva Labs requires less than 10 percent of the memory and processing power that a regular AV solution uses. With 15 years of infosec experience (20 years in IT), the CISO had led a lot of implementations. He was surprised by how easy the Minerva Labs solution was to install — he claimed it was one of the easiest he could remember doing. The client implemented Minerva Labs in 100 offices worldwide in a very short time. It was installed on approximately 4000 endpoints, and there were fewer than 20 PCs to troubleshoot, each taking about 10 minutes to resolve. The client sees this as remarkable in comparison to other security solutions, which are normally quite intrusive and disruptive.

The client is currently upgrading to Windows 10 and the Minerva Labs solution is still working smoothly with the agents previously installed. In contrast, each new Microsoft build creates numerous problems with their third party AV solution. The client reports that Minerva Labs seems to be agnostic, as he has had no OS-related issues so far (unusual for security solutions). He reports that end-users don't realize something new is running on their systems, and system administrators have no complaints. This satisfies his CEO's desire for balanced, sustainable results: a clean environment achieved without interference to the end user and business productivity.

The CISO took advantage of the Minerva Labs team's deep expertise in information security. Minerva Labs advisors were able to expertly answer all product questions (and more) and were receptive to input about enhancements to the product that would address additional issues for the client.

> “
>
> *Minerva's latest release significantly improves our endpoint defense strategy. We were able to deploy the solution within less than a week and saw immediate results. The number of ransomware attacks on us reduced dramatically and relieved the SOC team from having to investigate and remediate numerous alerts that resulted in days wasted on incident handling.*

About Minerva Labs

Minerva Labs 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 Labs 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.