MINERVA

*Solution Brief*

# Combating Modern Exploit Kits with Minerva's Anti-Evasion Platform

Exploit kits take advantage of vulnerabilities in end-user systems to infect endpoints with malicious code. These attack tools usually target web browsers or applications that could be invoked through a browser. Common targets of exploit kits have included Adobe Acrobat Reader, Java Runtime Environment and Adobe Flash Player. Successful exploitation allows the adversary to set the payload on the victim's system, which can be a trojan, ransomware, or any other form of malware. Modern exploit kits incorporate evasion tactics to avoid analysis, which makes Minerva's Anti-Evasion Platform especially effective at protecting enterprises from such threats.

## *Key Benefits*

- *99% of all exploit kit infections employ evasion tactics during the attack chain.*
- *Add a layer of defense until all patch management processes and updates are implemented.*
- *Easy to deploy and manage, without the need for pre-configurations or reboots.*

## *The Role of Exploit Mitigation*

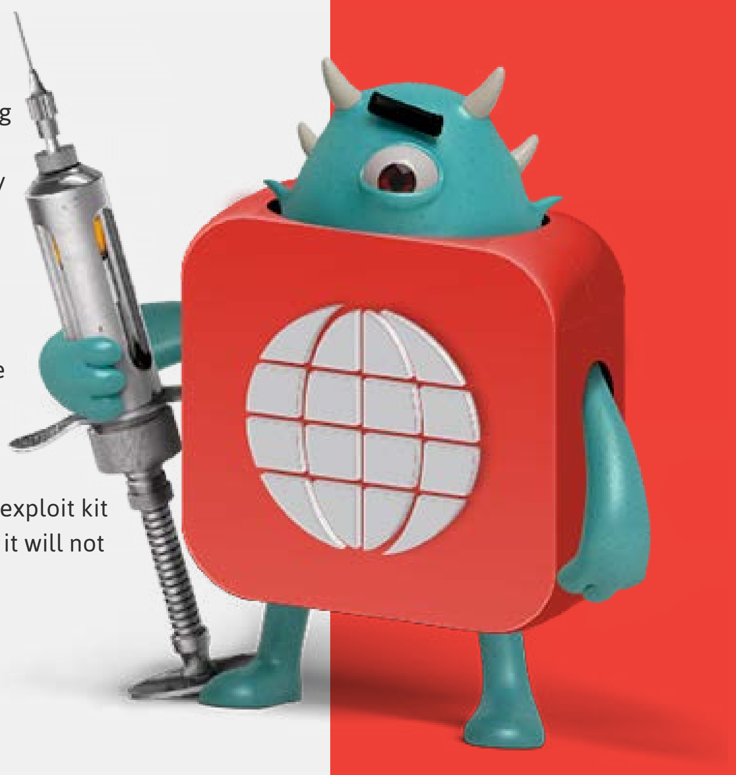
Many exploit kits target known vulnerabilities for which there are patches. Unfortunately, even enterprises with vulnerability management programs are unable to keep up with security update distribution at all times. As the result, operating systems include built-in technologies for decreasing the likelihood that an exploit will find a way to execute malicious code, even if the endpoint has the underlying vulnerability.

Windows now includes exploit protection as a free, built-in component of Windows Defender Exploit Guard. Endpoint Protection Platform (EPP) solutions offer additional exploit mitigation capabilities to help withstand exploit-driven attacks. In addition, compilers now allow developers to create applications that are resistant to some classes of vulnerabilities; one example of this functionality is Control Flow Guard (CFG) built into Microsoft Visual Studio. These are powerful approaches that mitigate exploit risks, **but they cannot stop all exploits.**

## *The Need for Evasion in Exploit Kits*

Exploit mitigation technologies increase the difficulty of compromising systems by exploiting software vulnerabilities. However, such countermeasures aren't able to defend against all attacks. In fact, they increase the value that a working exploit presents to the adversary, creating incentives for the attackers to be highly protective of their exploits and the associated malicious infrastructure.

Looking to protect themselves from security researchers, modern exploit kits increasingly employ evasion tactics. The objective of these methods is to distinguish between an endpoint that's worth attacking and an analysis system. For example, the following excerpt from an exploit kit probes the potential victim's system for files associated with virtualization software. Presence of these artifacts signals to the exploit kit that the endpoint might belong to a security researcher, in which case it will not attack as a way of concealing its true nature.



www.minerva-labs.com | contact@minerva-labs.com | +1-404-805-1510

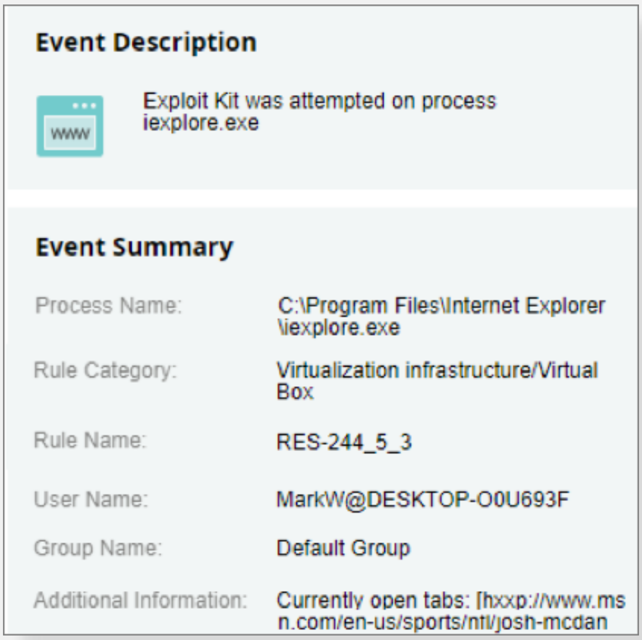
```
var n = {
    "C:\\windows\\win.ini": "yes",
    "C:\\Program Files\\fwebnc90ewnc9832n894cn": "no",
    "C:\\Program Files\\Oracle\\VirtualBox Guest Additions\\VBoxMouse.inf": "vbx",
    "C:\\Windows\\system32\\VBoxMRXNP.dll": "vbxn",
    "C:\\Program Files\\VMware\\VMware Tools\\vmtools.dll": "vmw",
    "C:\\windows\\system32\\drivers\\vmnet.sys": "vmn",
    "C:\\windows\\system32\\drivers\\vmxnet.sys": "vmxn",
    "C:\\Program Files\\Common Files\\VMware\\Drivers\\vss\\VCBSnapshotProvider.dll": "vmxc"
};
for (var o in n) re.fileExists(o, t)
```

Such exploit kits are designed to abort the attack at an early stage, even before attempting to exploit a vulnerability if they get “spooked” by possible malware analysis tools.

## Interfering with Exploit Kits

Minerva’s research into exploit kit campaigns examined the steps of successful attacks, starting from the earliest steps of exploit kit execution until infection of the victim’s system. The team examined the points in the attack paths that involved some form of evasion, such as the avoidance of malware analysis tools. 99% of the examined attacks involved at least one evasion tactic somewhere along the path. 86% of the attack paths employed evasion at the exploit kit phase.

These findings confirm the prevalence of evasion tactics very early in exploit kit attacks, even before the endpoint is subjected to any attempt to exploit a vulnerability. While such tactics typically give adversaries the advantage of staying undetected for a long time, they offer Minerva’s Anti-Evasion Platform an opportunity to protect enterprises from such attacks without relying on enterprise vulnerability management practices or exploit mitigation technologies. Instead, Minerva’s solution fools malware into “believing” it’s in a hostile environment that it’s programed to avoid, foiling attacks that might have bypassed other security controls.




Consider the example of Minerva preventing an exploit kit attack by simulating the presence of VirtualBox on the endpoint, as captured in the screenshot on the right. In this case, not only did the solution protect the system very early in the attack, it notified the enterprise about this event. Minerva supplied key details about the foiled attack, which that the company could use to further investigate the occurrence. Interfering with exploit kits in this manner is just one of the capabilities of Minerva’s solution, which offers a unique and practical layer for blocking threats designed to get past other solutions in the enterprise security architecture.

## 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’s Anti-Evasion Platform blocks unknown threats that evade defenses by deceiving the malware and controlling how it perceives its environment. Without relying on signatures, models or behavioral patterns, Minerva’s solution causes malware 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 boosts 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