BLUVECTOR®

Feature Review

FILELESS MALWARE DETECTION

Fileless malware, also called the invisible threat, is particularly hard to detect because it resides in system RAM and exploits authorized system and administrative tools in ways that elude whitelisting and other common mitigation strategies.

Version 3.0 of BluVector introduced the capability to detect fileless threats, within milliseconds, before they infect end-user systems or begin moving laterally throughout the enterprise network. Through an analytic, called the "Speculative Code Execution" (SCE) engine, BluVector is the ONLY solution capable of detecting fileless malware at the perimeter.

Q: *What is fileless malware?*

A malicious attack that is specifically created to start or complete an action that is untraceable by today's security tools. Rather than downloading a file to a host's computing device, the attack occurs in the host's memory (RAM), leaving no artifact on disk. Powering down or rebooting an infected system removes all artifacts of the attack; only logs of legitimate processes running remain, thereby defeating forensic analysis.

Q: *How does fileless malware get on a system?*

An attacker injects the malware code into a host's memory by exploiting vulnerabilities in unpached operating systems, browsers and associated programs(like Java, JavaScript, Flash and PDF readers). Often this is triggered by a Phishing attack that entices a victim to click on an attachment or can be a simple link to a malware-infected website or a compromised advertisement in a reputable site.

Q: *What happens once fileless malware infects?*

Once the malware is in memory, attackers can steal administrative credentials, attack network assets, establish backdoor connections to remote command and control (C2) servers. Fileless attacks can also turn into more traditional file-based attacks by downloading and installing malicious programs directly to computer memory or to hidden directories on the host machine. The threat actor can also employ a variety of tactics to remain in control of the system after a shut-down or reboot.

Q: *Why do signature-based defenses fail to detect fileless malware?*

Attackers utilizing fileless attacks are aware that the speed of corporate networks and the bandwidth they consume is increasing at a significant rate. This makes the detection of zero-day fileless malware at the network perimeter through traditional mechanisms an expensive proposition due to the high-end hardware required to operate at required speeds. Even amped up, traditional defenses have the issue of efficacy due to the complexities of detecting fileless attacks in an avalanche of traffic.

Q: *Why is BluVector so effective in detecting fileless exploits?*

BluVector focuses on the very early stages of a fileless attack, the initial compromise. The Speculative Code Execution engine operates on any network stream and emulates how malware will behave when it is executed. Operating at line speeds, SCE determines what an input can do if executed and to what extent these behaviors might initiate a security breach. By covering all potential execution chains and focusing on malicious capacity rather than malicious behavior, the analytic technology vastly reduces the number of execution environments and the quantity of analytic results -- often to just two or three -- that must be investigated.

SCE runs in parallel to BluVector's patented machine learning engine which is designed to detect file-based attacks so BluVector customers gain two different ways to detect full fileless or fileless attacks that turn file-based.

Q: *Why has detection of fileless malware become important?*

Fileless malware was first seen broadly in 2014, when a fileless version of the Wowliks malware -- Trojan.Poweliks – was found lurking in the Windows registry of a compromised system.

In 2016 new attacks emerged with PowerSniff, PowerWare and August. These attackes used techniques like malicious macros, PowerShell and shellcode to execute and remain hidden from traditional detection.

In 2017 the number of attacks and breach notifications identified as being caused by fileless attacks has taken a sharp uptick. There has been a sea change in the threat landscape, with cybercriminals adopting anti-forensic techniques originally developed by nation-states engaged in cyberwarfare and attacks on critical infrastructure networks.

PRODUCT CAPABILITIES

- Operates at line speeds on network stream and performs Speculative Execution
- Uses multiple heuristics to detect malicious or obfuscated JavaScript embedded in Webpage HTML targeting network services and endpoint services
- Shows suspicious execution sequences, de-obfuscates self-modifying malicious JavaScript and shellcode to reveal operational details
- Near zero false positive rate
- Correlating metadata about the detected malware to help an analyst evaluate the potential risk
- OS agnostic, detecting threats at the network level