BluVector Targets Growing Memory-Based Malware Threat with Real-Time Detection

Abstract

In July 2017, advanced threat detection startup BluVector augmented its machine learning-based analytics engine to detect memory-based attacks in real time. This means the BluVector Network Security Monitoring and Analytics platform leverages a new network emulation technique to identify a broader spectrum of attacks coming from both malicious files and embedded file attacks executed in memory. The release is timely, considering memory-based attacks increased dramatically over the last 12 to 18 months.

Delivering a One-Two Punch to Zero-Day Malware

BluVector, a recent spinoff from defense contractor Northrop Grumman, managed to generate a healthy buzz around its ability to reduce the amount of time it takes to detect zero-day malware on enterprise networks, using patented supervised machine learning techniques. But that capability, which the company claims produces far fewer false positives was, until recently, focused on malware using malicious files to infect its hosts. It did little to address the use of file-less, memory-based attacks increasingly deployed by cyber criminals. Recognizing the gap, the company implemented a technique called speculative code execution. This approach attempts to determine what an input can do, rather than observe what it does when it executes offline in a sandbox. Running in parallel with their already patented file-based detection, speculative code execution enables BluVector to detect malicious shellcode and JavaScript embedded in files, while at the same time adding delay for analysis and avoiding triggering sandbox evasion techniques increasingly used by malware to avoid detection.

With the new capability, BluVector uses its emulation technology to allow the potentially malicious shellcode or JavaScript to play out at a high rate of speed to identify suspicious execution sequences. Any attempts at obfuscation, including delayed execution, would be observed in the high-speed emulator. The emulator enables deeper analysis on the suspected code and gathers more details on it. At the same time, conviction of malicious code can be done in milliseconds. Existing sandboxing techniques can take several minutes to reach similar conclusions.

Conviction of malicious code can be done in milliseconds.

While the initial implementation of speculative code execution will detect shellcode in any file type supported by BluVector, the scripting language emulation is limited to JavaScript embedded within PDF documents. Later this year, BluVector intends to release another version capable of applying the technique to web pages (some file-less malware will use parts of the file system for presence or activation, but the malware itself does not place executables on the file system).

The product is deployed in a 2RU appliance that connects to a SPAN port or network tap, and operates on networks as fast as 10 Gbps. Speculative code execution is a part of a new detection module in BluVector's monitoring and analytics platform. Although it's still too early to determine how many false positives the new technique generates in real customer networks, BluVector found very few false positives in its internal testing.

Context

Though BluVector itself is a relatively new startup formed in 2016, the development of its technology dates back to 2010 under the guidance of parent company Northrop Grumman. The spinoff was sold in January to investors LLR Partners for $50 million, although Northrop Grumman retained the ability to continue to sell the technology to its DoD and Intelligence Community customers. Prior to spinning out BluVector, Northrop Grumman had already begun pilot deployments with about a dozen high-profile customers, including IBM. There it drew the attention of former IBM CISO/general manager of the IBM Security Services Division Kris Lovejoy, who was so impressed by the technology that she opted to leave IBM in order to lead the startup and guide its efforts to bring the technology to the commercial market. Thanks in part to the extended incubation period it enjoyed under Northrop Grumman, the technology was already awarded two patents, including one awarded in July for System and Method for Automated Machine-Learning, Zero-Day Malware Detection.

Over the last 18 months, security researchers from Kaspersky Lab, Morphisec, SentinelOne, and Proofpoint documented a spike in the use of file-less malware. Such malware operates directly in-memory, thus avoiding detection generated when placing executables on the host file system. Attackers typically employ widely used system administration or pen-testing tools such as Metasploit and PowerShell to package and then place malicious code in the host's memory. Although the exploit is not new, it has seen a resurgence as attackers work harder to avoid detection. The use of speculative code execution is itself not brand new. In 2011, researchers at Columbia University published a paper on the use of speculative code execution to detect return-oriented programming payloads. Return-oriented programming is an exploit technique in which attackers take control of the call stack to commandeer program control flow and then execute existing machine instruction sequences in the endpoint's memory. BluVector's speculative code execution, however, does not focus on ROP detection.

Over the last 18 months, security researchers documented a spike in the use of file-less malware.

EMA Perspective

The speculative code execution capability in the new 2.4 release is the icing on the cake of BluVector's analytics platform. It builds on a solid base of supervised machine learning detection of file-based zero-day attacks that is orders of magnitude faster than many existing malware detonation sandboxes. Speculative code execution fills a gap with its ability to identify attacks that seek to hide in plain sight by using file-less malware and commonly used pen testing and administrative tools. Although speculative code execution was identified as early as 2011 as a way to spot malicious, return-oriented programming payloads, most vendors who were focused on stopping advanced attacks now use a combination of sandboxing, dynamic analysis, and heuristics to try to detect such attacks.

As a Network Security Monitoring and Analytics platform, it's important that BluVector integrates with other data sources and workflows, and within an existing security architecture. To its credit, the company provides integration with a range of third parties, including top SIEM providers such as Splunk and IBM's QRadar, and endpoint protection providers such as Carbon Black. It also uses threat intelligence feeds to allow customers to leverage their existing investments in automated response and reporting.

BluVector's biggest challenge now is to raise awareness of its unique approach and build out its go-to market program. Its biggest question at this point in its journey is whether the low false positive rate found in the internal testing of the speculative code execution exists in real-world proof of concepts. If such is the case, it could gain a leg up against much larger competitors in the race to deliver more accurate and less noisy solutions to discovering threats that get past existing defenses.

At a time when the industry is struggling with a dearth of experienced security practitioners, BluVector is smart in trying to convey the improved TCO it delivers over competitive network security solutions. The company claims it can save customers $1,392 per incident and, in some customer case studies, event triage shrunk from 20 hours down to four hours per incident. If such savings can be replicated by all customers, the company will gain the competitive edge it needs to compete with much larger and better-established rivals. Of course, if it can prevent a single breach from occurring thanks to its speedy detection, it could save an enterprise $3.62 million–the current average cost of a breach.