Cloud Based
Secure Web Gateway

DR160203
March 2016

Miercom
www.miercom.com

Contents

Executive Summary

Miercom was engaged by iboss to conduct efficacy testing of the iboss Secure Web Gateway Platform as a network security solution. Testing, which employed industry-leading assessment tools, was conducted in February 2016. Results were compared to the average security efficacy percentage for comparable products, derived from the malware detection portion of the Secure Web Gateway Industry Assessment of 2016.

The device was tested for its ability to detect our mixed, sophisticated sets of legacy and advanced malware for local, remote and mobile devices. This report is intended to highlight the defense capabilities of the device against the most threatening, complex threats to date.

Malware using techniques to evade protocol and port detection were of particular focus. This solution was evaluated for detecting complex data extraction, endpoint visibility, event correlation of high risk endpoints, real-time responses to minimize loss, and threat analysis.

Key Findings

- Real-time detection and options to prioritize events give robust control to the user in the dashboard
- Detected 100% of Advanced Evasive Technique attacks, as well as 100% of common malware such as botnets and remote access trojans
- Mobile malware were found and logged with 100% efficacy in an easy to view monitoring console to provide intelligence for immediate remediation steps
- Recorded and identified 97% of polymorphic attacks – complex, intelligent malware which is hard to identify for most security solutions

The iboss Secure Web Gateway Platform was tested for its ability to minimize time to detect threats and data loss associated with an infection. Its detection was accurate and comparatively more so than the Industry Average by more than 14%. Deployment and console navigation were simple to learn and use. The level of security this product provides makes it an excellent choice for adding an extra layer of security to an enterprise network.

Based on the results of our testing, the iboss Secure Web Gateway Platform has earned the Miercom Certified Secure certification in February 2016.

Robert Smithers

CEO

Miercom

Introduction

Product Tested

The iboss Secure Web Gateway Platform is different from traditional secure web gateways (SWGs) by placing its focus beyond the malware. The product is designed to analyze techniques of entry, no matter how unconventional. Despite threat severity, if it is prevented at the source, there is no danger to the network. This design provides direct protection for local, remote or mobile endpoints accessing the secured network.

Protocols, such as TOR, are exploited to bypass typical web browser security. The iboss SWG is designed to prevent these protocol vulnerabilities and any malware thereafter.

Test Focus

The purpose of this report is to demonstrate the ability of the iboss SWG to minimize the time between the event and awareness of an infection and subsequent data loss.

Discussion topics of this report include:

Detection. Miercom's proprietary set of malware samples are sent to the device via HTTP/S for local, remote and mobile endpoints. The percentage of samples detected are recorded and compared to the 2016 Secure Web Gateway Industry Average. Malware delivered via anonymous, peer-to-peer sharing will be delivered using a TOR browser to determine the device's efficacy for malware evading common protocols. Additionally, sophisticated sets of malware are delivered and observed, such as those using automatic download methods, threats targeting a specific operating system and polymorphic attacks.

Data Loss Prevention. Event logging is assessed in real-time and evaluated. The detection technique of the device will be assessed for its ability to prioritize risks and provide responses in the dashboard.

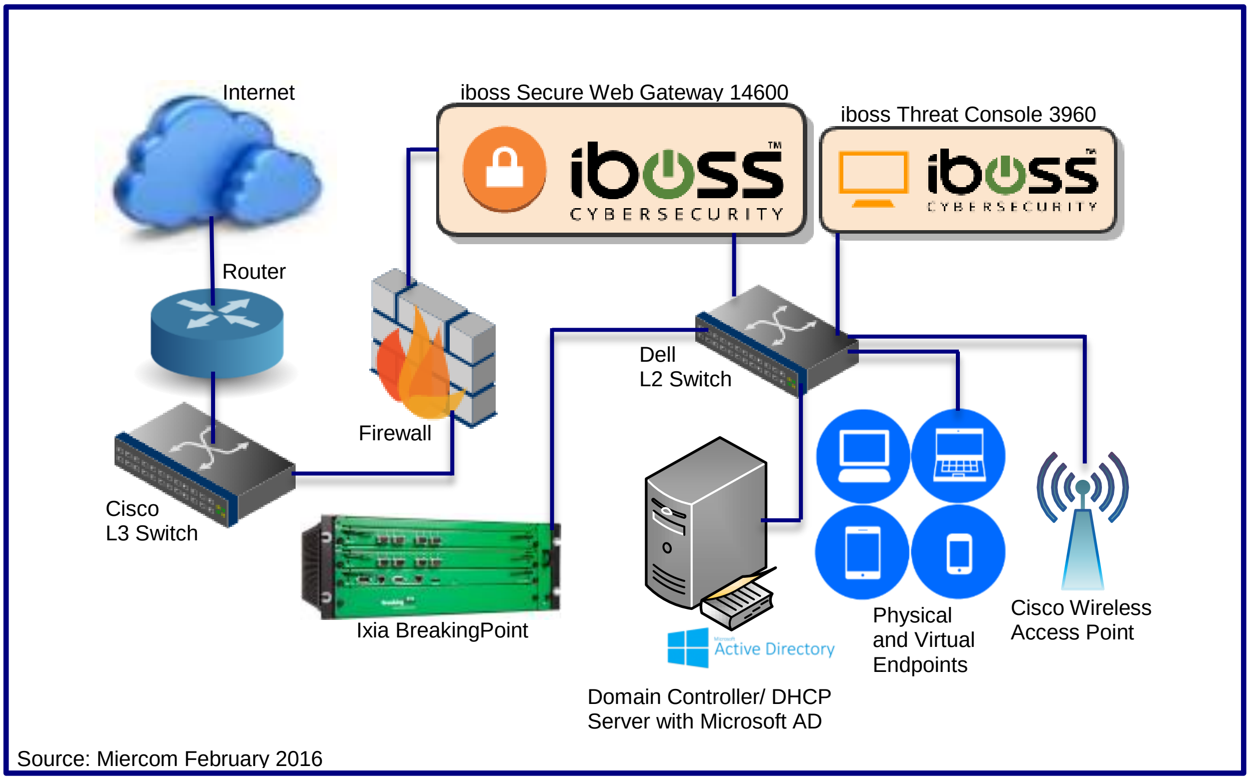
Reporting. The reporting console is evaluated for its clarity of endpoints within the network and associated activity. Threat visibility and containment is analyzed for usefulness to IT management.

How We Did It

Traffic is generated and delivered to a custom built network to simulate a real world environment. Polymorphic malware samples and malware evasive protocols are sent to the network from multiple sources to evaluate the DUT's ability to detect, prevent and respond to these threats.

Results of detection efficacy, data loss monitoring, threat intelligence and reporting visibility were observed and recorded. These were analyzed to determine the approach, capability and usefulness of the security product.

Test Bed Setup



Source: Miercom February 2016

The iboss Secure Web Gateway was deployed in-line between a firewall and layer-2 switch, connected from WAN to LAN. The iboss Threat Console was also connected to the layer-2 switch via LAN port.

Endpoints consisted of physical and virtual laptops and mobile devices. These devices simulated local, remote and mobile endpoints accessing the network, susceptible to malware.

Test Tools

Miercom Malware Server: This server contains proprietary samples of legacy and sophisticated threats. These types of threats are diverse and detection percentages for each reveal the strengths and weaknesses of the device's protection. The following categorizes of threats were used:

Miercom Malware Set
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
BotNet Communicating programs that delivers spam and 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
Remote Access Trojans (RATs) Trojans disguised as legitimate software which remotely control victim once activated
Malware Evasive Protocols
TOR/P2P/I2P Malware contained in downloads via torrent sites on P2P or I2P networks
Advanced Threats
Polymorphic Malware Constantly changing, making it difficult to detect
Zero Day Malware Exploits a known vulnerability before the vulnerability is fixed
Mobile Malware Targets mobile devices and shuts them down or accesses them remotely

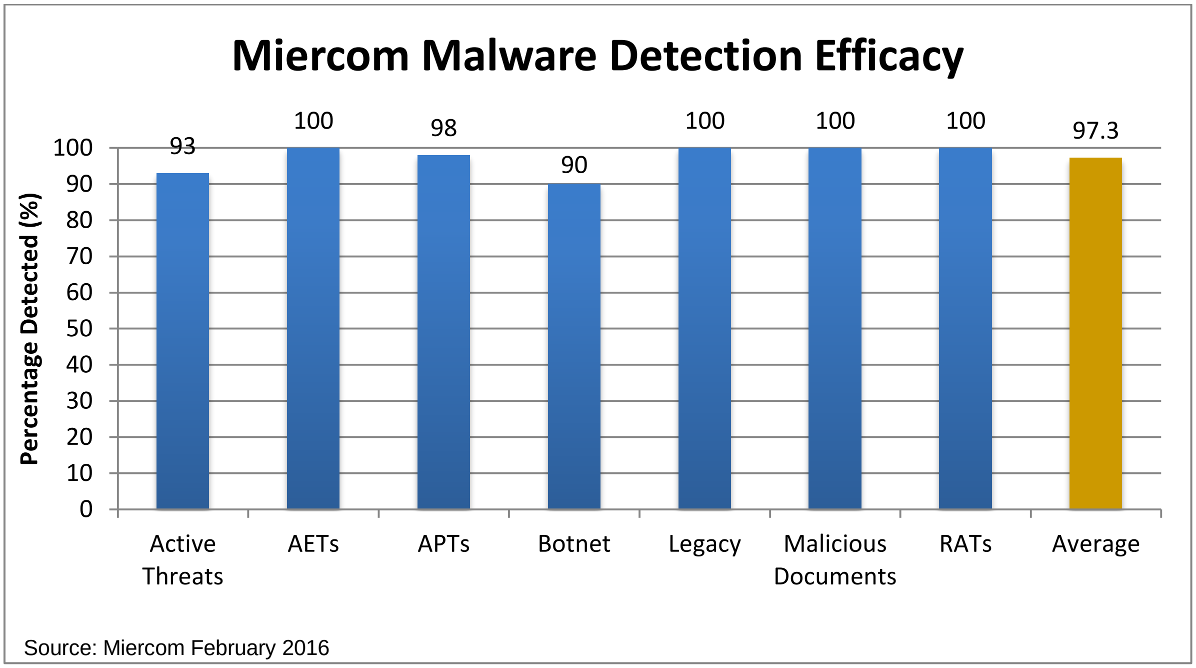
Ixia BreakingPoint: This industry testing appliance provides a robust and realistic environment for security testing. It is capable of over 30,000 malware samples and used to optimize next-generation firewalls, intrusion prevention systems and secure web gateways.

Detection

Miercom Malware Samples

These malware sets are used in the industry-wide study of malware detection for network security devices. Common malware are botnets, legacy, malicious documents and RATs. An emphasis is placed on active threats, AETs and APTs which are more complex and challenging for security solutions to identify. Detection results will inform the individual approaches to different malware types, as well as its granularity among market competitors.

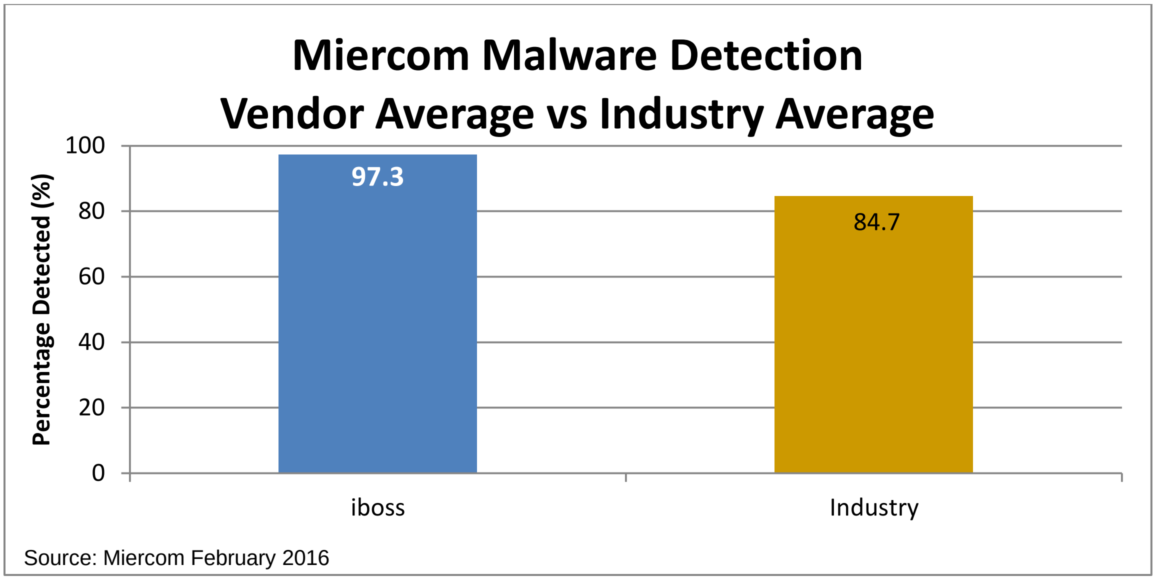
Results



Source: Miercom February 2016

iboss detected 100% of common malware: legacy, malicious documents and RATs, making it a valuable addition to any security infrastructure of an enterprise. Additionally it detected 100% of the AETs – a complex form of malware with techniques to evade detection. APTs were detected with a 95% efficacy and 90% of all Botnet samples were found. Active threats, polymorphic in nature and the most complicated type of malware, was detected at an 88% efficacy. Average detection was 97.3% of the comprehensive set of malware samples.

Miercom uses its proprietary sample set to assess security solutions for detection of malware. The average of the iboss device's individual results were compared that of competing devices to provide context to its efficacy score.



Source: Miercom February 2016

The iboss product detected 14.9% more malware samples than the Industry Average of similar security products.

Malware Evasive Protocol Samples

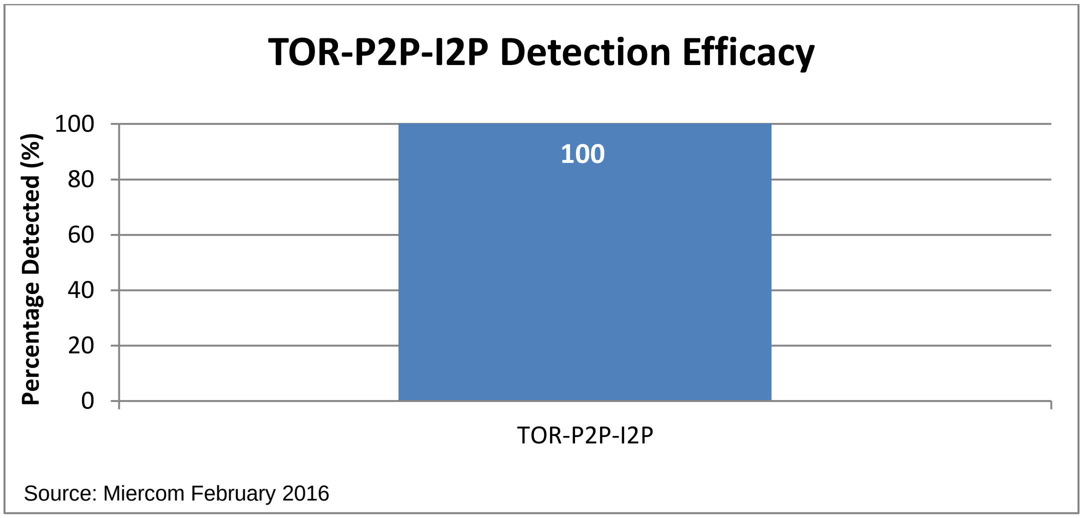
TOR and the Dark Web are associated with a convoluted system of servers and hosts, making communication practically anonymous and can be used for criminal activity.

Information transferred in this realm take advantage of protocols and ports. There are hundreds of thousands of ports, while only a little over a thousand have typical, or loose-standard, protocols. Dark communications travel encrypted with custom, atypical protocols on common ports such as 80, expecting something more common like HTTP.

Malware can evade detection if TOR protocol packets mask their payload with an HTTPS header. To the average network gateway, this request looks normal and malware instantly gains network access and control.

Results

Malware using TOR and other file sharing methods, such as Peer-to-Peer (P2P) and Invisible Internet Project (I2P), were analyzed in this test.



The iboss device detected 100% of all Dark Web and peer-sharing protocol malware. This category of stealth malware requires a high level of discernment by an SWG that many security products are not capable of.

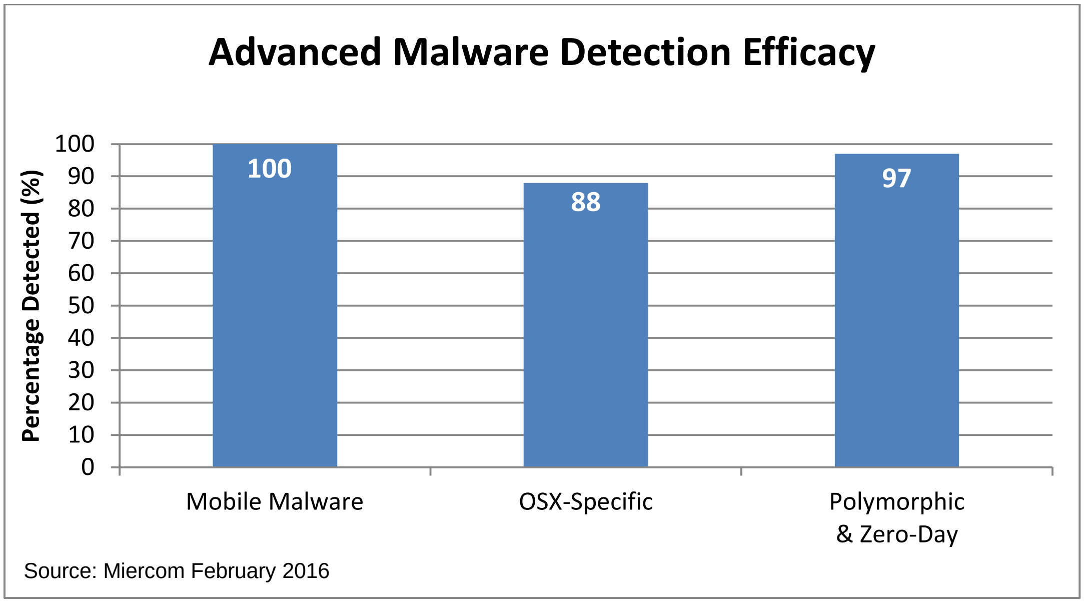
Advanced Malware Samples

Mobile devices are in the hands of almost all who need to stay connected on an enterprise or consumer level. This smart phone use has been exploited by hackers as another attack surface for gathering personal or financial information. The device was tested for its ability to detect malicious application package files such as .APK (Android), .DEB (Linux) and .IPA (Apple).

Malware specific to the Apple operating system, OSX, was delivered to the DUT to evaluate its ability to detect threats attacking the Unix-based architecture. With increasing sales of Apple products over the decade, the landscape for exploiting this platform for mass attacks has become more prevalent.

Polymorphic, zero-day threats are very sophisticated forms of malware. They are constantly changing, evolving and disappearing – making them hard to predict and identify by reputation alone. Being able to detect these samples provides insight to the granular, machine-learning approach of the security solution under test.

Results



Source: Miercom February 2016

The 100% efficacy of mobile malware detection is beneficial to an enterprise using smartphones and tablets. Any compromise to communication could result in data loss and down time. Despite Apple architecture being somewhat harder to infiltrate than an Android device or Windows computer, malware is becoming more common for this platform. iboss was able to detect 88% of this malware category. Polymorphic, zero-day threats are the most agile and active malware to enter an enterprise. iboss was capable of detecting 97% of polymorphic threats – a huge advantage as a comparative product in the network security market.

Data Loss Prevention

Monitoring

Constant monitoring increases a product's awareness of malware entering the network. The idea is to use intelligence gathered by the SWG to minimize malware entry and consequently network data loss. This test determines how and how well the device monitors all malware samples.

Results

The iboss device had an event monitor which picked up every event created by the victim computer clients, including background applications. Initially, seeing all events simultaneously is a bit tedious but the device was able to pick up every minute instance of a threat.

The device was a passive monitoring system. In our testing, alerts were not used. Instead, for each malware sample sent to the network, an event was created in the monitoring log for up to 20 events at a time until refreshed. No data loss was observed during the monitoring process.

Actionable Intelligence

After monitoring, threat intelligence is gathered to create a map for remediation. Correlation of threat events yields a prioritized approach to dealing with the most threatening situations first. By prioritizing events, an IT admin can take action immediately.

This test evaluates the amount and granularity of intelligence useful for threat remediation.

Results

The option to prioritize certain threats, such as malware, was available with the iboss device. During testing of malware samples, other threat events were created in regards to theft and gambling. These event creations were done automatically by iboss and were prioritized based what was identified.

The iboss SWG immediately produced an alert after an event was created and categorized as malicious. All threats were quarantined and then either allowed or blocked.

Intelligence was accurate and provided enough information to create immediate and useful remediation.

Reporting

Visibility

Having detection efficacy defines a useful security device, but 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 iboss product was evaluated for its visibility of threats and its ease of deployment for a technical user.

Results

Threat visibility was granular but did not show the type of malware next to the threat. Instead, the event log is organized by tabular categories. The learning curve to deployment and gaining familiarity with the system only took a couple days. It was simple to identify where an IT admin would be able to make configuration changes. The dashboard was very simple to navigate.

Conclusion

The iboss Secure Web Gateway Platform was tested to show its ability to minimize the time to detect threats and record the data loss associated with an infection. The product was evaluated for its detection of Miercom's proprietary malware set, malware evasive protocols and a sophisticated set of malware types used in mobile devices, Apple products and polymorphic attacks. From these results, we were able to determine the way in which the product logs events in real-time for alerting of network attacks and minimize data loss. The entire reporting console was assessed for its clarity and usefulness to a real-world IT administrator.

The product had 97.4% efficacy against Miercom malware, outperforming the Industry Average Average of similar devices' efficacy by over 14%. Its detection of evasive protocols was 50%, showing the severity of these types of attacks on a network. For sophisticated threats, it performed at an average of 95%. These threats were very different and specific. We observed 100% detection against mobile threats and 97% detection of polymorphic attacks.

Intelligence gathered during testing was accurate and logged in real-time with options to prioritize attacks for easier remediation. Deployment was moderately simple and the console had clear navigation.

The iboss Secure Web Gateway Platform performed well for detecting common and some very sophisticated samples. This product would be a great addition to any network security infrastructure.

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.