Behavioral Detection of Threats & Data Loss in a Network

DR160623C
August 2016

Miercom
www.miercom.com

Contents

Copyright © 2016 Miercom

Executive Summary

Miercom was engaged by iboss to conduct efficacy testing of the iboss Secure Cloud Web Gateway Platform for efficacy in behavioral data loss prevention. Testing, which employed industry-leading assessment tools, was conducted in two phases. The first phase, release in March 2016, was a comparison of iboss' malware detection efficacy against comparable products.

This second phase, tested the iboss Secure Web Gateway for its ability to detect polymorphic malware, identify and block data loss extraction and for its highest achievable data throughput rate. The focus of iboss Secure Web Gateway (SWG) testing revolved around the behavioral detection of threats and data loss in a network.

Given the nature of polymorphic attacks, security products require multiple methods of detection since the threat is ever-changing as it embeds itself within a network. By detecting threats based on anomalistic behavior, rather than an attack signature, the iboss SWG can identify more active and complex threats that would normally go undetected.

Key Findings

- Real-time detection and event logs gave visibility and granular control for strengthening configurations and outbound traffic management
- Threats were logged at a rate of 25 events per second, identifying suspicious, anomalistic behavior against baseline traffic
- A 97.5% detection rate for active, polymorphic attacks was 16% higher than the Industry Average
- Observed 96.7% prevention rate of successful extraction of sensitive data, such as credit card numbers and phone numbers
- Showed expected throughput for 1518 byte TCP and UDP traffic, reaching a maximum of 950 Mbps

Deployment of this SWG in a realistic test network proved excellent protection and data loss prevention measures using anomalistic detection methods and real-time event logs. The degree of security this product provides against attacks and extraction makes it an integral piece of any enterprise protection solution.

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

Robert Smithers
CEO
Miercom

Copyright © 2016 Miercom

Introduction

Product Tested

In March 2016, Miercom published the report *iboss Cloud Secure Web Gateway* (DR160203B) after product testing. For that report, the iboss SWG was tested and confirmed to detect unconventional malware, for protocols such as TOR, which bypass typical web browser security. And despite the severity of the attack, it posed no threat to the network or its endpoints if stopped at the source.

During June 2016, we deployed the same SWG in an identical test network. For this second phase, we looked at polymorphic malware and data extraction scenarios to see how the secure web gateway (SWG) handles the most lethal attacks and prevents loss of sensitive information.

The following firmware versions were used in testing:

- iboss Secure Web Gateway version 8.1.2.60
- iboss Threat Console version 8.1.2.96
- Current Signature version 4.0.7.5

Test Focus

The focus of testing was to demonstrate the ability of the iboss SWG to minimize data loss and maximize throughput performance. Included were:

Active Malware Detection. Active threat malware was used to determine detection efficacy and behavioral detection techniques. The active threat, or "zero-day", malware was from Miercom's proprietary Security Testing Suite. Efficacy results were recorded, compared to and later included in the 2016 Secure Web Gateway Industry Average.

Data Loss Prevention. Sensitive data such as credit card numbers, social security numbers, tax IDs, or other user defined patterns were delivered with generated traffic flow through the network. By attempting to extract this data from the network, the device was assessed for its data loss detection and prevention efficacy.

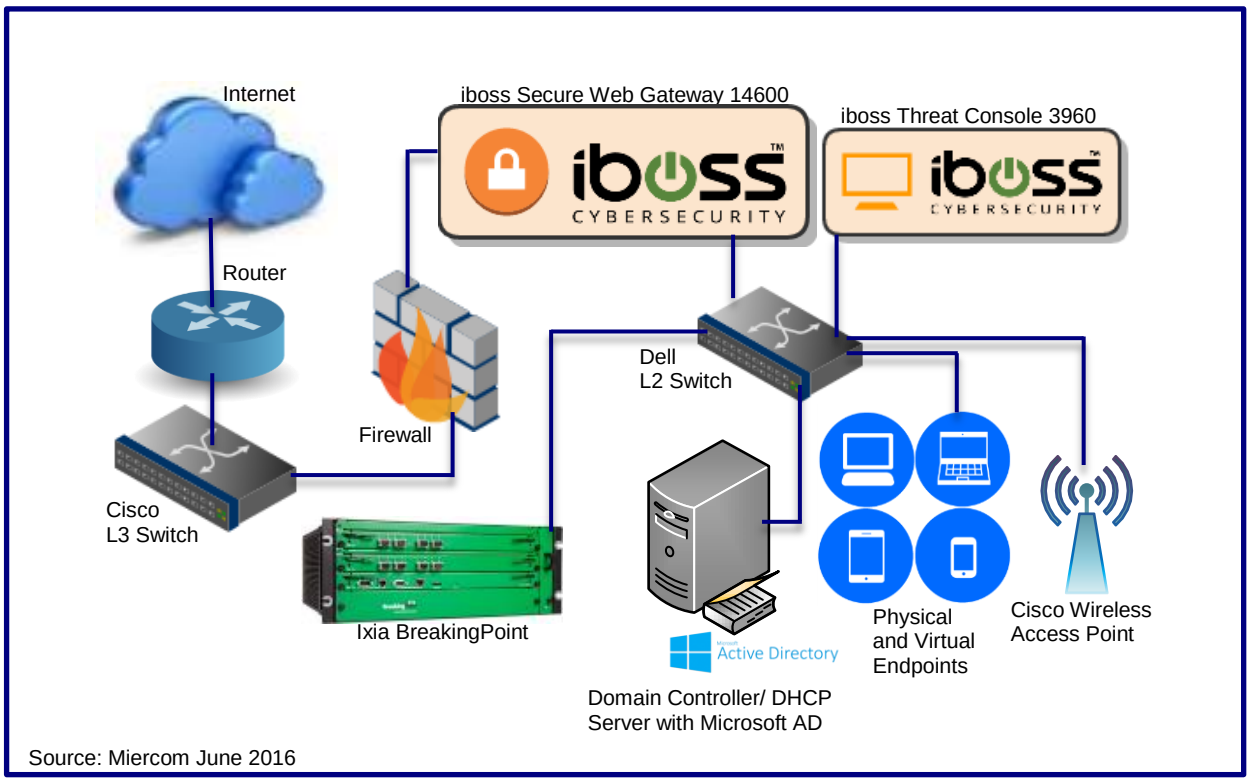
Performance Throughput. Simulated traffic was sent through the iboss SWG to determine the maximum throughput. The highest rate of traffic the device could process was recorded, reflecting its handling capacity before packet loss.

Copyright © 2016 Miercom

How We Did It

Our custom-built network was the same as the one used in the March 2016 *iboss Cloud Based Secure Web Gateway* report. The network reflected a real world environment, employing devices any enterprise network would – L2 and L3 switches, a firewall, domain controller, active directory and a wireless access point.

Test Bed Setup



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 Security Test Suite: This suite contains a malware server, a database of legacy and sophisticated threat samples, which range in technique and age. For testing, we focused on Active Threat samples which are custom-crafted and polymorphic. Detection percentage of this malware type reflected the strength of the iboss SWG for eliminating severe risks to a network.

Ixia BreakingPoint: This testing appliance provides a robust and realistic environment for security testing. It is capable of over 30,000 malware samples and is used to optimize next-generation firewalls, intrusion prevention systems and secure web gateways. Its database of personal and sensitive information allows it to test for data loss security of network protection devices.

Method

To simulate traffic, Ixia BreakingPoint generated TCP and UDP packets. Within traffic flow, malicious samples from our test suite were sent through the device under test (DUT) via FTP. The percent of samples detected was recorded, as well as how the console identified malware to the user.

Data Loss Prevention (DLP) testing was performed using the Ixia BreakingPoint, which has a database of over 300 application protocols and generates credit card numbers, tax payer IDs, phone numbers and keywords. Additionally, a third-party test tool was used to assess for DLP detection. DLP rules were set up in iboss to ensure an optimized configuration. HTTP/S POST requests were used to extract sensitive data from the secured LAN sides of the network.

iboss was evaluated for its ability to detect active threat malware and the extraction of the sensitive data by using behavioral detection. Any anomaly seen in the network was expected to trigger an event in the iboss SWG system and send a notification through the Threat Console.

Performance was tested by generating increasing amounts of TCP with 64, 512 and 1518 byte packets; UDP using 1518 byte and UDP Cisco IMIX traffic. TCP throughput was tested by sending HTTP GET requests. Once packets were dropped, the DUT was recorded as reaching its maximum data throughput.

Results of detection efficacy, data loss prevention and performance were analyzed to determine the approach, capability and usefulness of the SWG.

Copyright © 2016 Miercom

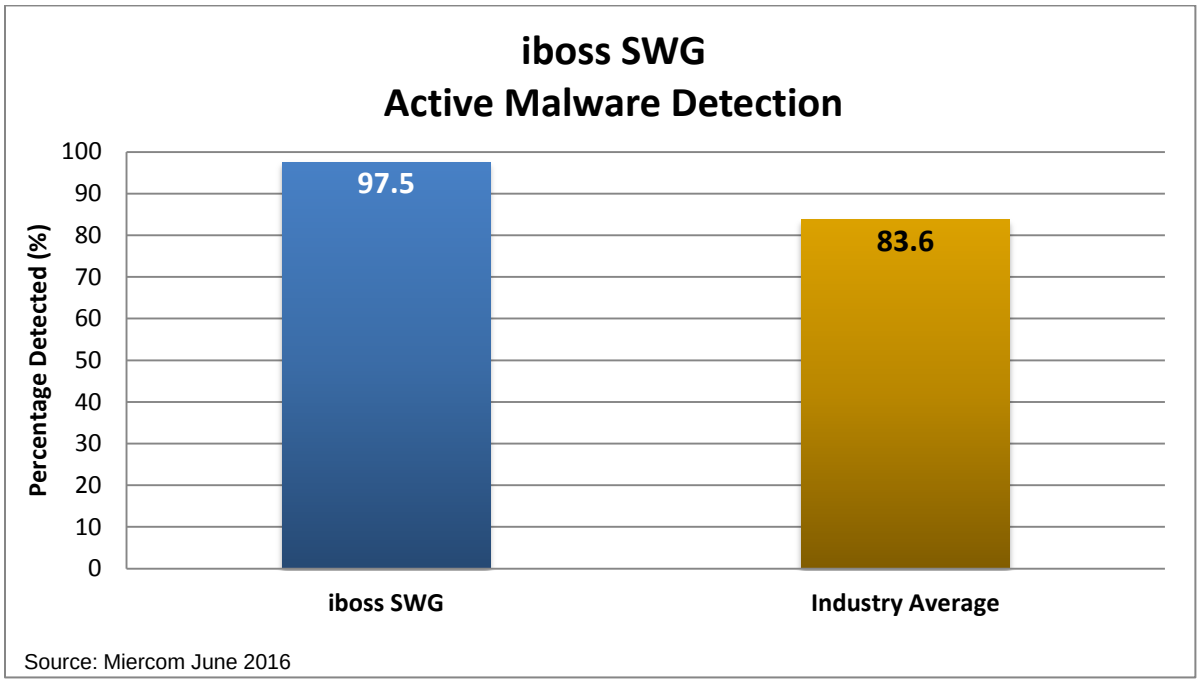
Detection

Miercom Malware Samples

Miercom's Security Test Suite contains a wide range of malicious samples. Common malware includes botnets, legacy attacks, malicious documents and RATs. More advanced samples consist of Advanced Evasive Techniques (AETs) and Advanced Persistent Threats (APTs).

The most threatening of all attacks are active, or "zero-day", samples which are polymorphic in nature. Not only do these samples consistently dodge reputation-based detection systems, but they are constantly changing their appearance to avoid security countermeasures.

Detection of these samples requires a diverse and layered approach. The results from the iboss SWG is shown as compared to the Industry Average.



The iboss SWG detected 97.5% of active, polymorphic threats. This was 16% higher than the Industry Average. These threats are the most complicated type of malware to detect due to their "moving target" characteristic.

Copyright © 2016 Miercom

Data Loss Prevention

This test assessed the DUT for its data loss prevention (DLP) efficacy. Sensitive data was simulated and sent through the DUT to determine how many interceptions had occurred.

Using Ixia BreakingPoint, Personally Identifiable Information (PII) was simulated. Phone numbers, tax IDs, credit card numbers and random strings to represent user patterns and file entries were sent along with normal, baseline traffic through the DUT. By filtering content, the DUT was expected to prevent data exfiltration.

The iboss SWG prevented the loss of 96.7% sensitive data samples attempting to be extracted from the network. This test was repeated three times and the best result observed was recorded.

Behavioral Detection

Instead of analyzing traffic for signature-based red flags to find threats, the DUT utilized behavioral detection. This method compares events to a baseline of normal activity. Events that stand out are considered anomalies, which may or may not pose a threat to the network. By analyzing these events, the DUT can detect threats that would normally evade signature-based detection since they are polymorphic or operate using a disguised payload to extract data.

The iboss Threat Console was able to display events in real-time and at a rate of about 20 to 30 events per second. We used HTTP, FTP and email to attempt to transfer sensitive data out of the test network, and iboss detected these files being moved.

Events were created instantly in the dashboard. Event logs show how the file was downloaded, identify malware placed in sandboxing and the destination URLs of outbound traffic. This would help a system administrator investigate where activity took place, how to better configure the iboss SWG to meet their needs and which potentially unsafe websites to block.

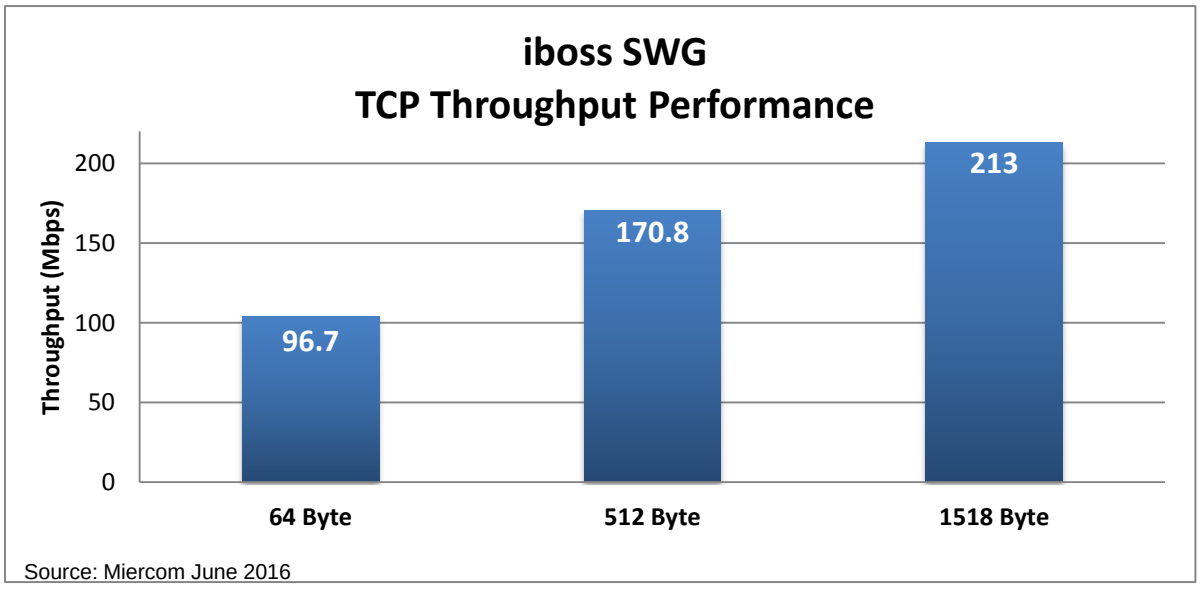
Copyright © 2016 Miercom

Performance

Throughput tests measured the maximum rate of traffic handled in megabits per second (Mbps). Ixia BreakingPoint generated increasing loads of traffic through the network and DUT. Once packets were dropped, the load was considered as the achievable maximum data rate.

This test was performed for different packet sizes and with two protocols: TCP and UDP. The product was configured with DLP, advanced threat protection (ATP), advanced evasion techniques (AET) and SWG protection mode.

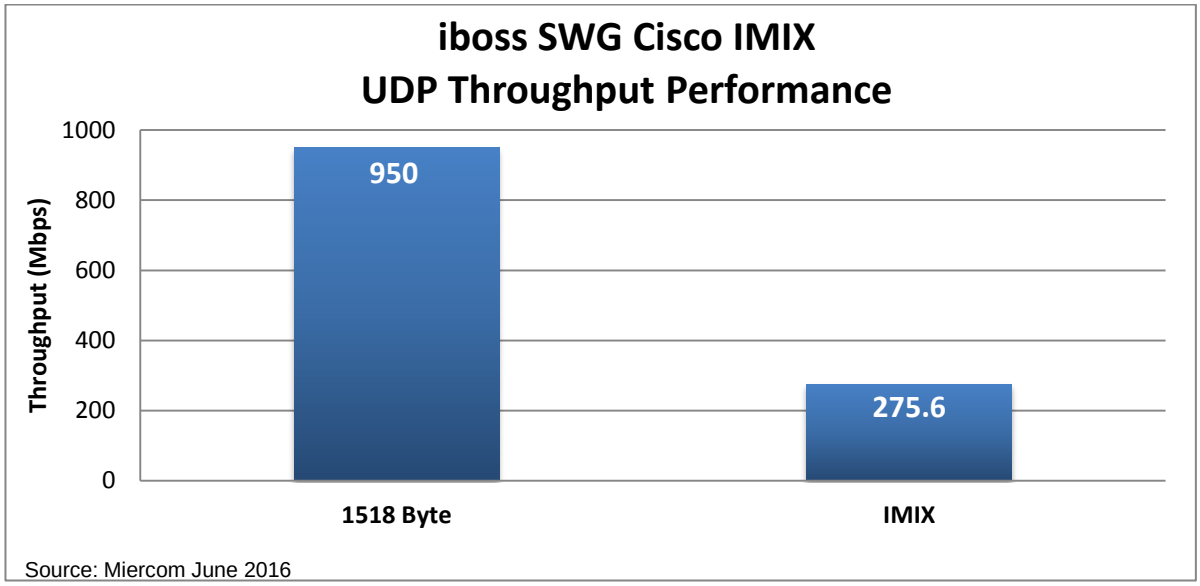
1518 byte	This is the largest frame size to hold the most data packets. With more bandwidth, the DUT has to work less to retrieve data and scan for malicious activity. This frame size is expected to yield the highest throughput rate. This is the baseline for the UTM test.
512 byte	With a moderate frame size and less data, it maintains sufficient bandwidth. The DUT works harder to sift through more frames to scan for abnormalities and is expected to have a lower throughput rate than 1518 byte traffic.
64 byte	This is the smallest frame size, and by using less bandwidth, it takes more frames to transmit data packets. This forces the DUT to work the hardest to scan and is expected to have the lowest throughput.



As expected, increased frame sizes resulted in increased throughput. This correctly reflects that the DUT had to work harder to scan more segmented data when the packet size is smaller, for 64 byte traffic, but showed its highest throughput for 1518 byte traffic at 213 Mbps.

Copyright © 2016 Miercom

Cisco IMIX	A mixture of frame sizes contains percentages of each of the preceding frame sizes. The UDP Cisco IMIX traffic used in testing had 7 streams of 64 byte, 4 streams of 512 byte and 1 stream of 1518 byte traffic. It was expected to have very low throughput but at a higher rate than the pure 64 byte traffic.



UDP performance was higher for the largest frame size than for Cisco IMIX, which consisted of a mixture of 64, 512 and 1518 byte traffic. Both 1518 byte and Cisco IMIX rates were higher for UDP than for TCP.UDP does not require acknowledgment of received packets. UDP traffic was a continuous packet stream and proved higher data rates, as expected.

Copyright © 2016 Miercom

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.

© 2016 Miercom. All Rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors. Please email reviews@miercom.com for additional information.