# Malware, Zero Day and Advanced Attack Protection Analysis
# Zscaler Internet Security and FireEye Web MPS

**Detailed Lab Testing Report**

**DR141007C**

**14 November 2014**

Miercom
www.miercom.com

# Contents

## 1.0 Executive Summary

Miercom conducted a Security Efficacy Analysis of network-based breach detection and Zero Day and Advanced Persistent Threat (APT) protection solutions that utilize threat emulation. The assessment included products from vendors, Zscaler and FireEye.

Standard and advanced security tests were performed to verify the detection, blocking and operational capabilities on multiple areas of real-time malware threats, Zero Day attacks, modern malware, threat emulation (commonly referred to as sandboxing) and forensic reporting. The ability of the products to correctly identify block threats from a large sample of malware of an unknown nature emulated what the solutions need to provide in the real world when users click on web links.

Overall test results demonstrated that Zscaler outperformed FireEye Web MPS in all six categories of malware tested. The Zscaler platform proved to be more effective than FireEye in both performance and accuracy for the malware sample sets Miercom tested. The sample sets were independently created by Miercom..

For Zero Day threats, Zscaler's malware protection was extremely effective. ZScaler's security efficacy (commonly referred to as catch rate) was 30% better than FireEye Web MPS while testing Zero Day samples. The newly created samples are representative of dynamic threats that incorporated evasive measures that change the characteristics of the malicious file. The same samples that Zscaler detected and blocked were successfully able to bypass both anti-malware protection and file sandboxing within FireEye Web MPS.

Key Findings:

- Zscaler correctly classifies and identifies known threats with their first lines of defense; multiple layers of anti-malware protection.
- Zscaler is more efficient. By mitigating known threats immediately upon identification, it only sandboxes unknown objects, which allows for rapid incident response time.
- Zscaler blocks malware in the cloud, malicious objects never make it to the corporate network. The result is better performance, better security and less network congestion

During the assessment, we also tested and noted usability, forensic reporting, identification of false negatives and vendor specific limitations.

The identification and ability to decompose, emulate, and accurately determine whether or not newly created, Zero Day samples were in fact malicious was the main goal of this line of testing. Zscaler surpassed FireEye by 39% in accomplishing this goal.

We were pleased with the overall performance of Zscaler, particularly in its malware blocking and threat emulation effectiveness. Detailed test results follow and demonstrate how Zscaler and FireEye Web MPS compare in regard to malware detection, protection and Threat emulation.

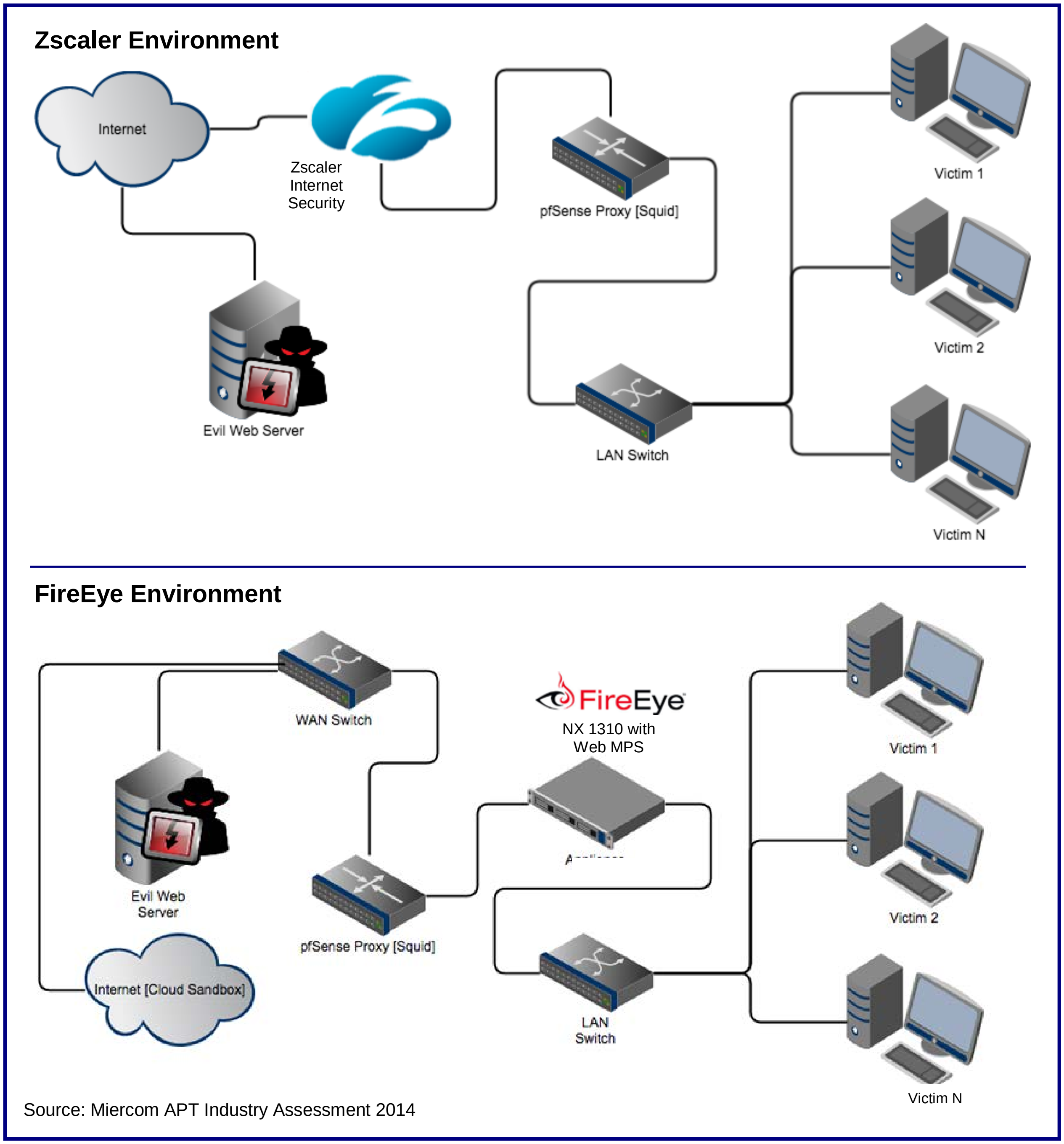
The Zscaler platform including sandboxing and malware protection performed well and demonstrated several advantages in advanced attack protection.

Robert Smithers

CEO

Miercom

## 2.0 Testing Environment



Source: Miercom APT Industry Assessment 2014

## 2.1 How We Did It

A test bed was created containing each product deployed in-line between a series of victim machines for each product, and a malicious web server that was used to serve up the malware samples. The end-nodes (victims and malicious web server) were all virtualized, but on different hardware to ensure that the machine state was the same throughout testing.

To ensure delivery, a lightweight web application was developed to organize the sample sets. Additionally, the application performed a user agent verification on the client browser to eliminate accidental propagation of the malware.

The web server would be called upon by the victim via an HTTP GET request and the product would act as an intermediary. Each product configuration was carefully reviewed to ensure that both vendors represented in the test bed were equally deployed with comparable features.

Prior to performing the analysis, each product was verified working by issuing a base test with a select number of samples, such as binary executables, botnets, worms, viruses, Zero Day and newly created samples and an array of different file types. This test ensured that each product was functioning and reporting on the malicious files being requested by the victim machines.

The baseline test consisted of a small legacy sample set of malware used to ensure that each appliance was working correctly. The base samples chosen were checked against VirusTotal. Each sample set contained a variety of malware classifications and each product was confirmed working before conducting tests for the record.

**Evil Web Server**

- Debian Linux using the LAMP Stack (Linux Apache MySQL PHP)
- The web application checked that the request originated from a custom browser agent to prevent accidental propagation of the samples
- Each sample set was organized and placed on a separate page

**Victim Browser Configuration**

- Windows 8.1
- Firefox v. 32.0.x
- Firefox DownThemAll plugin - To download the large sample sets automatically

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact Miercom Professional Services via reviews@miercom.com for assistance. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a product selection. Miercom engineers are available to assist customers for their own custom analysis and specific product deployments on a consulting basis.

## 2.1 Products Evaluated

Testing was performed on the following systems:

- Zscaler

  Internet Security Platform with Advanced Persistent Threat Protection

  2014 Edition

- FireEye

  NX 1310 Appliance with Web MPS appliance Sandbox

## 2.4 Malware Sample Sets

The sample sets created for testing are representative of the type of threats that these products will need to correctly identify and block in the real world when users click on malicious or compromised web links. They include a large sample of “unknown” malware that has never before been seen or analyzed. There are six types of malware in the sample sets:

- **Legacy Malware**

  Legacy samples included several hundred variants of known malware that have been in circulation for 30 days or more. The malware classifications primarily consisted of viruses and worms.

  The sample sets contained variants of:

  Sysbot - Spyware
  AutoRun - Virus
  Danger - Trojan
  Hooker - Trojan
  Injector - Trojan
  Homepage - Spyware
  ZeroAccess Rootkit
  Hijack - Trojan
  Infector - Virus

  Legacy malware samples should be mitigated without the need for threat emulation, so it was a test of the product to determine the efficacy of the AV protection alone prior to sending newly created and more specific samples (documents, RATS, botnets, etc.). If a sample got through, threat emulation should have identified it immediately due to the known heuristics of the malware.

- **Advanced Persistent Threats**

  Advanced Persistent Threats (APTs) are “back doors” or malware that consists of a staged payload that when propagated, allows an attacker to obtain a shell (command line access to the remote target) at the same privilege level as the vulnerable application or service. These payloads are often masked with randomization and evasion techniques to bypass AV protection.

  We used select samples from Mandiant’s Advanced Persistent Threat sample set.

  **Note:** Mandiant was acquired by FireEye in early 2014. However; these samples are legacy, but specific in that they account for advanced evasion techniques used by attackers and with covert penetration testing.

- **BotNets**

  Variants of Zeus and Citadel were collected from high-interaction honeypots. Botnets use a technique known as Command and Control, where an intermediary receives orders from an attacker and those commands are then forwarded to all infected hosts. Botnets are commonly used in spamming and DDoS operations.

- **RATS**

  RATS or Remote Access Trojans masquerade inside of other legitimate software. When propagated onto a victim host, they provide full remote control over that victim. Remote Access Trojans and malicious payloads containing backdoors were used for further exploitation.

The sample set was a mix of MS Office documents and PDF files. The Office documents contained macro viruses and the pdf files contained a variety of viruses, APTs and worms.

- **Malicious Documents**

  This sample set also contained a mix of Microsoft Office documents (Microsoft Word, PowerPoint and Excel files) that held known macro viruses and PDF files made up of a variety of viruses, APTs and worms.

- **Zero Day**

  Each Zero Day sample changed the hash value of the sample to have it purposefully evade signature-based detection. By evading signature-based detection, the samples bypassed AV and were emulated in the sandbox.

  These malware samples are the most challenging to detect by signature-based (legacy) scan engines.

## 3.0 Security Efficacy Analysis

To safeguard enterprise networks from ever-evolving computer attacks, threat protection solutions must be highly effective while also providing superior performance and high availability. A comparison of the Zscaler and FireEye products based in functional hands on testing and analysis follows.

### Zscaler Internet Security with Advanced Persistent Threat Protection

| | |
|---|---|
| **Solution** | The Zscaler Internet Security Platform is a cloud-based service with a built-in virtual sandbox. |
| **Capture Rate** | Detection rate was 100 percent for legacy, advanced persistent threats (APTs), and RATS samples. Detection rate was 77% for Zero Day threats and 70% for malicious documents. |
| **Sandbox Performance** | Zscaler had the fastest performance with threat emulation results in minutes. Zscaler's cloud-based approach ensures that virtual machine sandboxes can be created on demand, eliminating analysis bottlenecks. |
| **Reporting** | Although the threat emulation did not provide a timeline of malware propagation and execution, detailed information on this could be found by doing drill-downs from the web-based threat emulation dashboard. |
| **Deployment** | Zscaler was very easy to deploy – there is no hardware or software to install, we simply directed our Internet traffic through their cloud. |
| **System Scalability** | Zscaler has superior scalability - as a cloud-based system, Zscaler includes built-in high availability and contractually guarantees 99.999% uptime. |

### FireEye Web MPS 1310 Malware Detection System

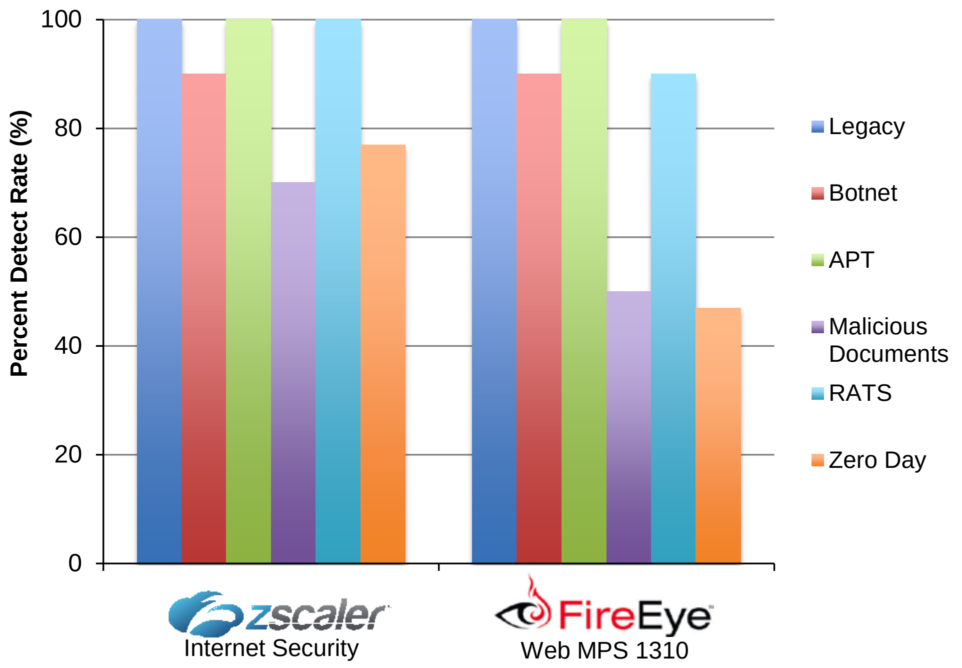
| | |
|---|---|
| **Solution** | FireEye Web MPS 1310 solution is made up of a physical appliance with a built-in virtual sandbox. |
| **Capture Rate** | The product caught 100 percent of legacy and APT samples and 90 percent of botnet and RATS threats. However, it scored 50 percent or lower in identifying malicious documents and Zero Day samples. |
| **Sandbox Performance** | Miercom engineers found FireEye to be extremely slow in that completing the tests and gathering the results took days. Each FireEye appliance supports a limited number of virtual machine sandboxes, and because FireEye is designed to analyze every file that comes through, severe analysis bottlenecks can occur, delaying security alerts. |
| **Reporting** | The dashboard for management was visually appealing and generally effective. However we found it difficult to navigate to analyze the malicious samples detected. |
| **Deployment** | Individual appliance deployments are required for each separate network. The FireEye appliance was fair to moderate in difficulty to install. There is added complexity when adding multiple appliances for geographically dispersed networks. |
| **System Scalability** | A single FireEye appliance does not provide high availability. Production deployments for which high availability is a concern will require multiple boxes and a load balancer. |

## 3.1 Table of Security Efficacy Percent Detection Rates

| | Zscaler | FireEye |
|---|---|---|
| **Legacy** | 100 | 100 |
| **APTs** | 100 | 100 |
| **Botnets** | 90 | 90 |
| **RATS** | 100 | 90 |
| **Malicious Documents** | 70 | 50 |
| **Zero Days** | 77 | 47 |

**Note:** Zero Day samples consisted of mutated or new strains of lethal modern malware, as well as custom crafted, newly developed malware.

## 3.2 Security Efficacy – Overall Detection Rate



Source: Miercom APT Industry Assessment 2014

$$\text{Security Efficacy} = \frac{\text{Number of Samples Detected}}{\text{(Total Number of Samples)}} * 100$$

## 3.3 Time for Detection Analysis

There can be large differences in the amount of time a threat protection solution needs to analyze a malware sample. The following table shows the average time a sample was analyzed in the specific product's sandbox:

| Vendor | Average Time per Sample |
|---|---|
| Zscaler | ~ 10 minutes |
| FireEye Web MPS 1310 | ~ 18 minutes |

It is important to note that Zscaler only sends samples to its sandbox that it cannot classify as malicious using its other layers of security analysis techniques. FireEye sends all samples to its sandbox. So for example, if 100 samples were sent to each product and only two samples were unknown malware, ZScaler would have its results within minutes, while FireEye would often require up to a full day to deliver its results.

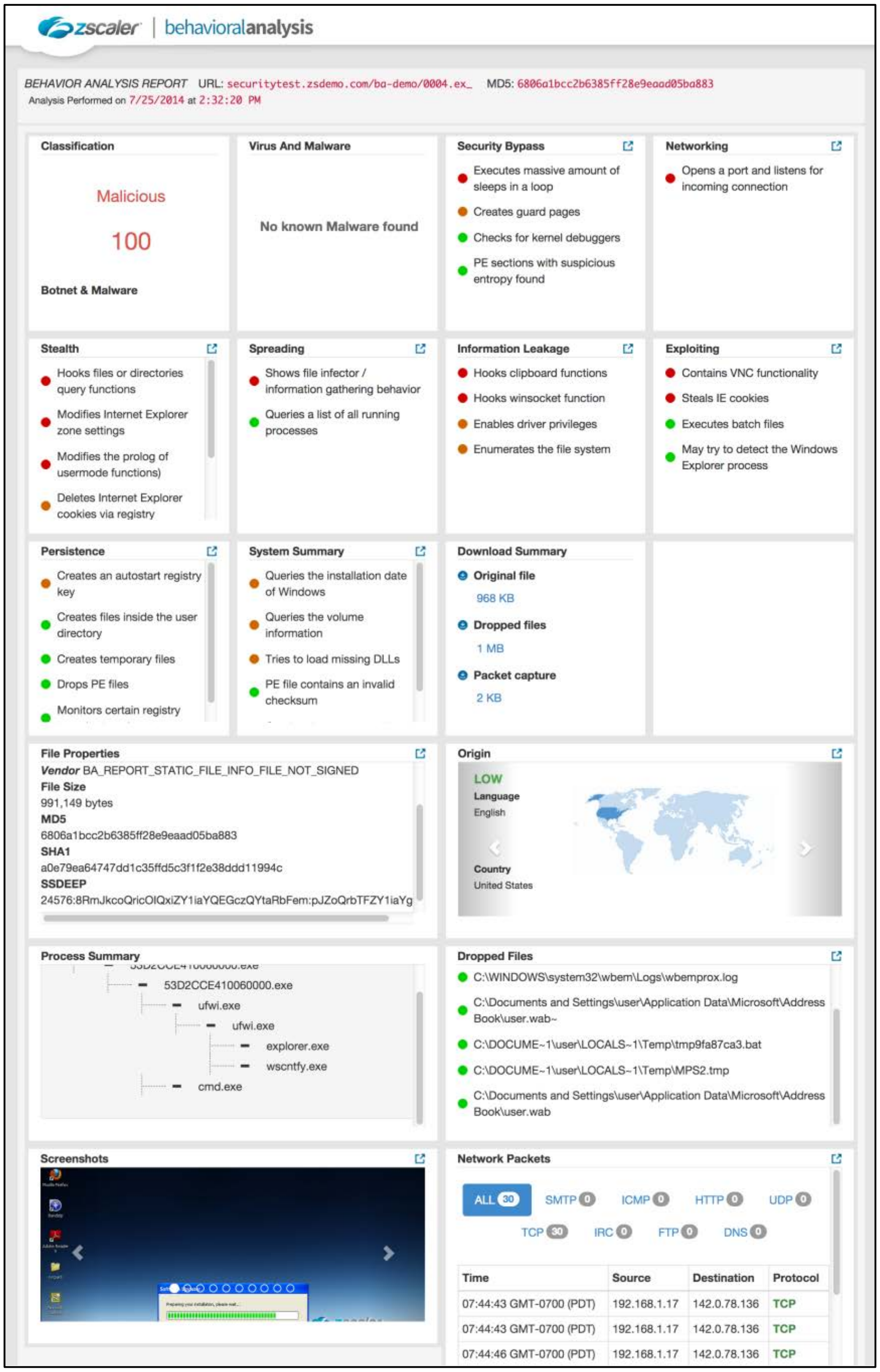
This time lag has security implications. Since FireEye is typically deployed in TAP mode and does not block unknown samples from reaching target devices, this long delay means that a significant amount of time may pass between the infection of the device and the time that malware is detected.

Zscaler also has a quarantine feature which blocks unknown samples while they are being classified in the sandbox. This ensures that even the first device that attempts to download a new Zero Day threat does not get infected.

## 3.4 Other Considerations

### Reporting

The Zscaler threat emulation dashboard was easy to navigate and the level of detail excellent. Behavior and origin of a malware sample was shown. The screen was extremely easy to read and navigate, being very intuitive to Miercom engineers. As well as the screen being very well organized, there were many data filters present so that getting to exact data needed could be easily accomplished. The following screen displays a Zscaler Behavioral Analysis report.



*BEHAVIOR ANALYSIS REPORT* URL: securitytest.zsdemo.com/ba-demo/0004.ex_ MD5: 6806a1bcc2b6385ff28e9eaad05ba883
Analysis Performed on 7/25/2014 at 2:32:20 PM

**Classification**

Malicious

100

Botnet & Malware

**Virus And Malware**

No known Malware found

**Security Bypass**

- ● Executes massive amount of sleeps in a loop
- ● Creates guard pages
- ● Checks for kernel debuggers
- ● PE sections with suspicious entropy found

**Networking**

- ● Opens a port and listens for incoming connection

**Stealth**

- ● Hooks files or directories query functions
- ● Modifies Internet Explorer zone settings
- ● Modifies the prolog of usermode functions)
- ● Deletes Internet Explorer cookies via registry

**Spreading**

- ● Shows file infector / information gathering behavior
- ● Queries a list of all running processes

**Information Leakage**

- ● Hooks clipboard functions
- ● Hooks winsocket function
- ● Enables driver privileges
- ● Enumerates the file system

**Exploiting**

- ● Contains VNC functionality
- ● Steals IE cookies
- ● Executes batch files
- ● May try to detect the Windows Explorer process

**Persistence**

- ● Creates an autostart registry key
- ● Creates files inside the user directory
- ● Creates temporary files
- ● Drops PE files
- ● Monitors certain registry

**System Summary**

- ● Queries the installation date of Windows
- ● Queries the volume information
- ● Tries to load missing DLLs
- ● PE file contains an invalid checksum

**Download Summary**

- **Original file** 968 KB
- **Dropped files** 1 MB
- **Packet capture** 2 KB

**File Properties**

*Vendor* BA_REPORT_STATIC_FILE_INFO_FILE_NOT_SIGNED
**File Size**
991,149 bytes
**MD5**
6806a1bcc2b6385ff28e9eaad05ba883
**SHA1**
a0e79ea64747dd1c35ffd5c3f1f2e38ddd11994c
**SSDEEP**
24576:8RmJkcoQricOIQxiZY1iaYQEGczQYtaRbFem:pJZoQrbTFZY1iaYg

**Origin**

LOW
**Language**
English
**Country**
United States

**Process Summary**

```
   ─ 53D2CCE410060000.exe
      ─ 53D2CCE410060000.exe
         ─ ufwi.exe
            ─ ufwi.exe
               ─ explorer.exe
               ─ wscntfy.exe
         ─ cmd.exe
```

**Dropped Files**

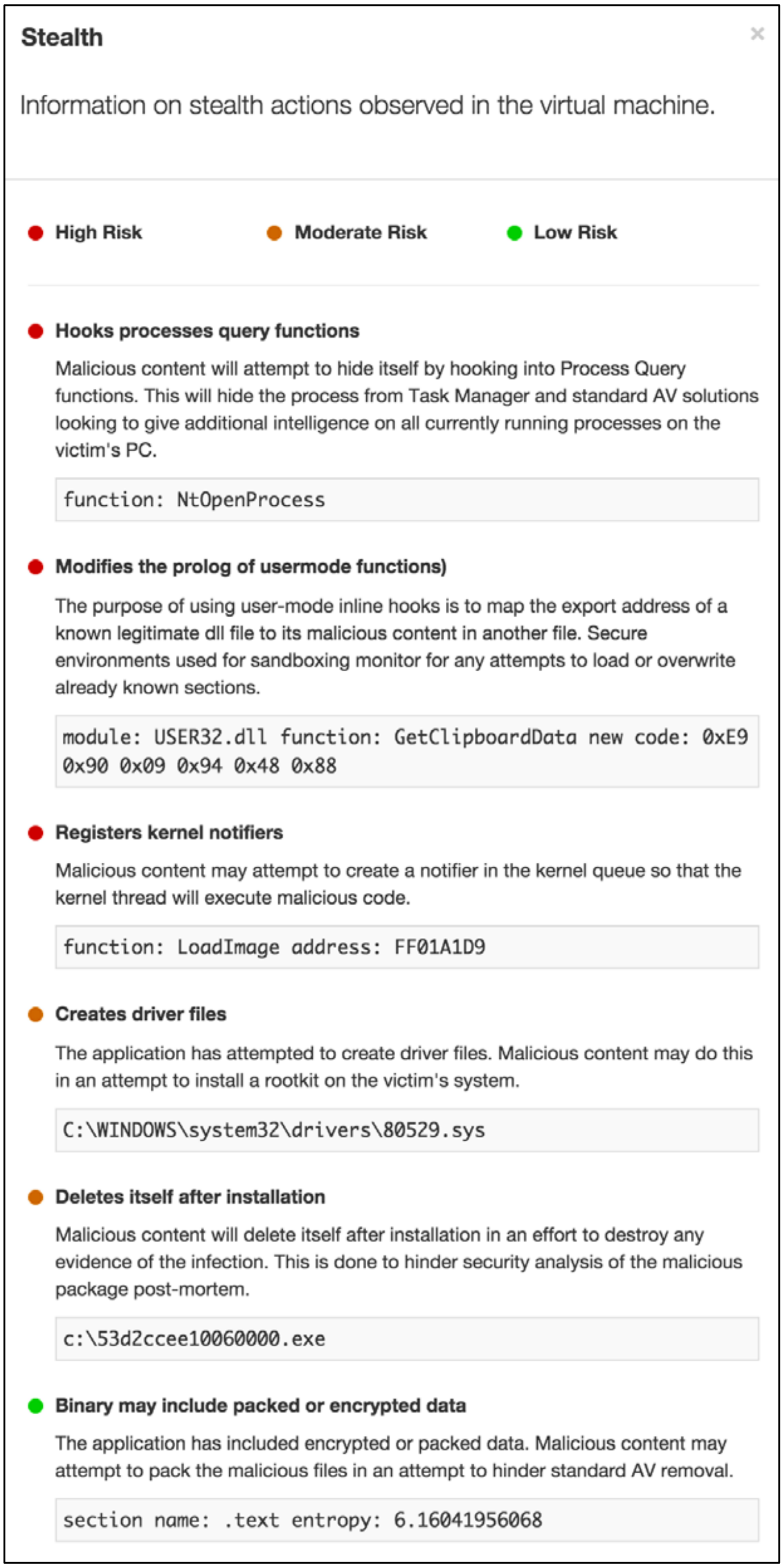
- ● C:\WINDOWS\system32\wbem\Logs\wbemprox.log
- ● C:\Documents and Settings\user\Application Data\Microsoft\Address Book\user.wab~
- ● C:\DOCUME~1\user\LOCALS~1\Temp\tmp9fa87ca3.bat
- ● C:\DOCUME~1\user\LOCALS~1\Temp\MPS2.tmp
- ● C:\Documents and Settings\user\Application Data\Microsoft\Address Book\user.wab

**Screenshots**

**Network Packets**

| Time | Source | Destination | Protocol |
|---|---|---|---|
| 07:44:43 GMT-0700 (PDT) | 192.168.1.17 | 142.0.78.136 | TCP |
| 07:44:43 GMT-0700 (PDT) | 192.168.1.17 | 142.0.78.136 | TCP |
| 07:44:46 GMT-0700 (PDT) | 192.168.1.17 | 142.0.78.136 | TCP |

It was easy to click on the expansion icon in the top right corner of any section to see more detailed information on the specific section.  The following screen displays the detail shown when expanding the Stealth section.



### Stealth

Information on stealth actions observed in the virtual machine.

● High Risk ● Moderate Risk ● Low Risk

● **Hooks processes query functions**

Malicious content will attempt to hide itself by hooking into Process Query functions. This will hide the process from Task Manager and standard AV solutions looking to give additional intelligence on all currently running processes on the victim's PC.

```
function: NtOpenProcess
```

● **Modifies the prolog of usermode functions)**

The purpose of using user-mode inline hooks is to map the export address of a known legitimate dll file to its malicious content in another file. Secure environments used for sandboxing monitor for any attempts to load or overwrite already known sections.

```
module: USER32.dll function: GetClipboardData new code: 0xE9
0x90 0x09 0x94 0x48 0x88
```

● **Registers kernel notifiers**

Malicious content may attempt to create a notifier in the kernel queue so that the kernel thread will execute malicious code.

```
function: LoadImage address: FF01A1D9
```

● **Creates driver files**

The application has attempted to create driver files. Malicious content may do this in an attempt to install a rootkit on the victim's system.

```
C:\WINDOWS\system32\drivers\80529.sys
```

● **Deletes itself after installation**

Malicious content will delete itself after installation in an effort to destroy any evidence of the infection. This is done to hinder security analysis of the malicious package post-mortem.

```
c:\53d2ccee10060000.exe
```

● **Binary may include packed or encrypted data**

The application has included encrypted or packed data. Malicious content may attempt to pack the malicious files in an attempt to hinder standard AV removal.

```
section name: .text entropy: 6.16041956068
```

The main FireEye dashboard screen was appealing, but the screens past that were not well organized and very difficult to navigate.  It seemed as if too much information was present on the screen, making searching on the screen for specific data more of a time-consuming process. FireEye also did not have similar data filters; it was harder to search for specific data on a malware sample.

## Ease of Use

Zscaler has graphical SIEM characteristics with data visualization that allowed for rapid threat identification, which then equaled better incident response.

Configuration was easy on Zscaler. It took literally five minutes to get the Internet security platform up and running. Zscaler worked well and it was easier to navigate from screen to screen.

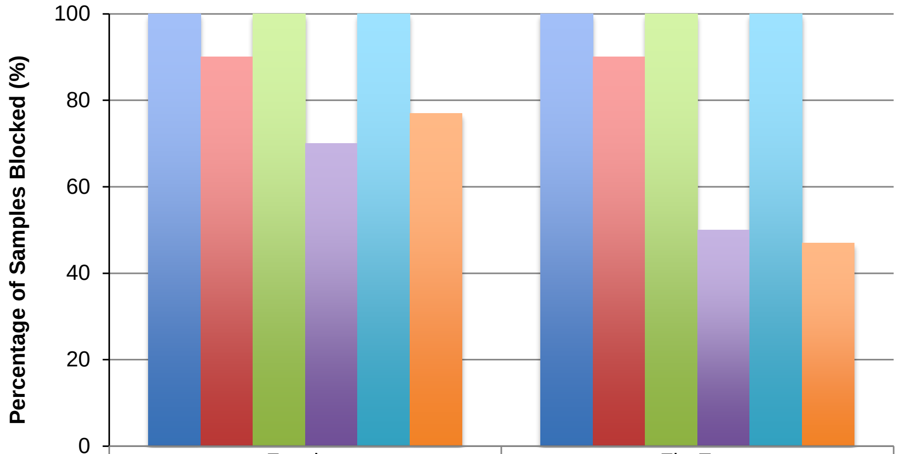
FireEye took more planning to deploy because network placement had to be determined. Configuration and testing to make sure the product was working also took three to four times longer minimally 4 hours.

## 4.0 Anti-Malware Protection

Each product has signature-based malware detection. For the purposes of testing, this protection was enabled on both products as a preliminary defense. In most cases, if the signature was identified, the threat was immediately mitigated. However and by design, FireEye required that each sample be forwarded to the sandbox for further analysis.

Proved in anti-malware protection testing, Zscaler had some clear advantages over FireEye Web MPS. It was more accurate by correctly classifying and identifying known threats and that allowed for immediate incident response time. Zscaler's cloud architecture also prevented network congestion and delivered better performance.

### 4.1 Samples Blocked / Detected by Anti-Malware Protection



| | Zscaler | FireEye |
|---|---|---|
| 🟦 Legacy | 100 | 100 |
| 🟥 Botnet | 90 | 90 |
| 🟩 APT | 100 | 100 |
| 🟪 Malicious Documents | 70 | 50 |
| 🟦 RATS | 100 | 100 |
| 🟧 Modified/ Zero Day | 77 | 47 |

Source: Miercom APT Industry Assessment 2014

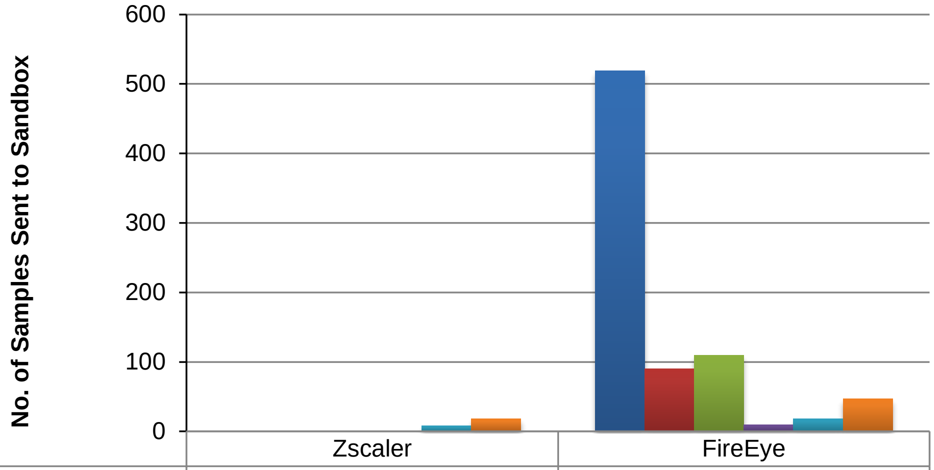
This graph depicts the percentage of samples that were effectively mitigated by anti-malware protection. Zscaler and FireEye identified all legacy, APT and RATS samples that were sent to them. Zscaler was better at identifying newly created and Zero Day samples at 77 percent with FireEye at 47 percent. Zscaler also caught 70 percent of malicious documents with FireEye detecting 50 percent.

FireEye sent all samples to the sandbox for analysis, which could considerably increase operating costs as more appliances would be needed for efficient performance on a larger network infrastructure.

## 5.0 Threat Emulation Comparison

Zscaler provided the strongest protection of the network by accurately blocking the most malware samples, preventing 100 percent of legacy, APT and RATS threats. The Zscaler also blocked 90 percent of botnets, 77 percent of Zero Day threats and 70 percent of malicious documents.

### 5.1 Malware Samples Rendered to Threat Emulation



| | Zscaler | FireEye |
|---|---|---|
| 🟦 Legacy | 0 | 519 |
| 🟥 BotNet | 0 | 90 |
| 🟩 APT | 0 | 110 |
| 🟪 Malicious Documents | 0 | 10 |
| 🟦 RATS | 8 | 18 |
| 🟧 Zero Day | 18 | 47 |

Source: Miercom APT Industry Assessment 2014

In this chart, the closer to a zero count for any malware type sent for threat emulation, the better. Miercom engineers observed that Zscaler would immediately recognize malware that it had analyzed previously, so would then just automatically block it.  It would only send to threat emulation malware that had not been previously analyzed, therefore results were reported quickly.

Sandbox implementation in FireEye is very different.  Even if FireEye identified malware that it had previously analyzed as bad, it would not just block it but would send it for threat emulation to be analyzed again.  That is why the numbers are larger for FireEye in this chart.

It is important to note that this choice by the vendor of what to send for threat emulation means that our testing took minutes to complete with Zscaler up to a day to complete with FireEye. In real world deployments, this may cause organizations to need to purchase additional or larger FireEye boxes than otherwise necessary to ensure timely classification of malware.

## 5.2 Accuracy of Threat Emulation

| Vendor | Findings |
|---|---|
| FireEye | Implementation is slow. Physical appliance and local sandbox.<br>Results took days to process.<br>FireEye detected 39% fewer Zero Day threats than Zscaler.<br>Report data is detailed but very difficult to navigate, which makes it hard to determine malware characteristics. |
| Zscaler | Implementation is fast.  Cloud-based platform and sandbox.<br>Accurate and consistent. Samples sent to the sandbox were properly classified and mitigated.<br>Most efficient sandbox. Results were quick and dashboard provided detailed forensic reporting.<br>By design, block detect rate is better because only unknown samples are sent to the sandbox.<br>Classification of malware is more than 50% more accurate compared to FireEye. |

# 6.0 Defense In Depth

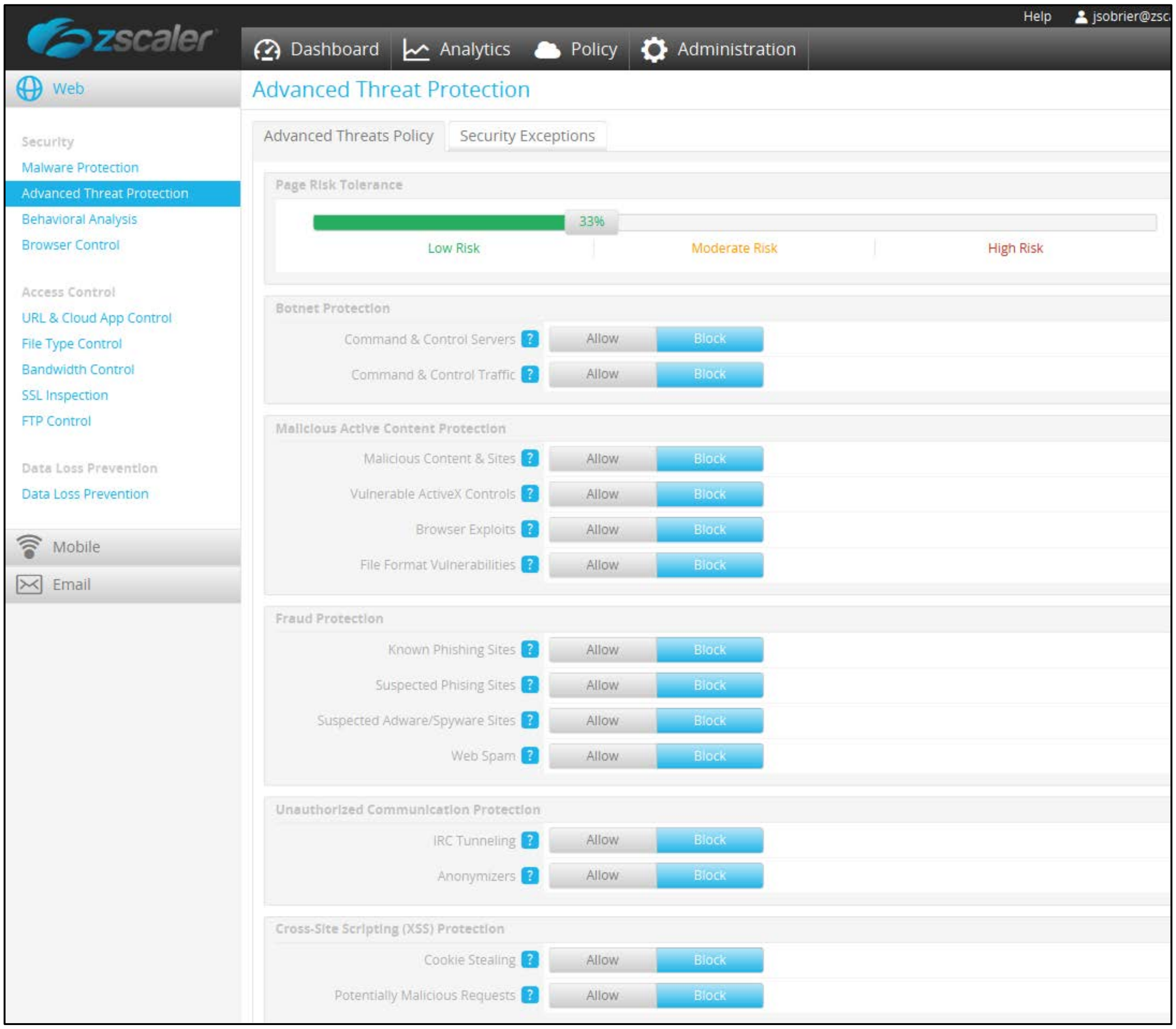
## 6.1 Protection

Zscaler deploys in-line and is able to block malware before it reaches any device in the network. Zscaler features multiple layers of security defenses in depth, including signatures, six different AV engines, static and dynamic analysis and behavioral analysis for unknown and Zero Day files. As a cloud-based system, it protects the network by being able to mine traffic and stop new threats immediately, before they reach the customer's network or the target device. Zscaler can also quarantine unknown zero-day objects. Comparing the security coverage provided by Zscaler and FireEye:

- FireEye appliances are typically deployed at a couple of key locations. Traffic from remote offices, road warriors (employees outside of company) and mobile devices must be backhauled to these devices in order to be scanned.
- SSL decryption is included with Zscaler, but not included with FireEye.
- Traffic visibility: Zscaler sees all the traffic from millions of locations all the time, but each FireEye device sees traffic from one location only.
- Network effects: When Zscaler identifies a new Zero Day threat in its sandbox, it automatically deploys blocks for that object, in real time, across its entire network
- Defense in Depth is included with Zscaler; FireEye only has behavioral analysis
- Zscaler is always deployed in-line and can always block. Most FireEye deployments are done in tap mode.

| Comparison of Protection | Zscaler | FireEye |
|---|---|---|
| Pro-Active detection | Vulnerability shielding: detect and report vulnerable browser plugins and browsers block older browsers | None |
| Block common malware inline | Six inline antivirus engines + Zscaler AV signatures | Limited |
| Malicious URL | Block malicious URLs through blacklist and content inspection | Limited Blacklist |
| Phishing – Block phishing sites | Detect known and unknown phishing sites | Does not block phishing sites detected by most browsers |
| Block XSS attempts and cookie stealing | Block cross site scripting attempts and cookie stealing | None |
| Block Adware sites | Block adware sites through blacklist and content inspection | Limited blacklist |
| Control archives – Embed malware in password-protected archive or zip | Handles RAR, ZIP, GZIP, BZ2, etc. | |
| Block potentially dangerous websites | URL filtering: block anonymizers, questionable websites, P2P website | |
| SSL – Block malware over SSL & HTTPS | SSL decryption available with "granular controls" | Additional hardware required |
| Notify users | Customizable End User Notification: web page displayed to the user with the reason for the blocked content | Connection reset or dropped, no notification to the user |
| Block traffic | Inline proxy | Mostly deployed in tap mode |

## Zscaler: Advanced Threat Protection Diagnostic Screen



Advanced Threat Protection

Advanced Threats Policy | Security Exceptions

Page Risk Tolerance: 33% (Low Risk | Moderate Risk | High Risk)

Botnet Protection
- Command & Control Servers: Allow [✓ Block]
- Command & Control Traffic: Allow [✓ Block]

Malicious Active Content Protection
- Malicious Content & Sites: Allow [✓ Block]
- Vulnerable ActiveX Controls: Allow [✓ Block]
- Browser Exploits: Allow [✓ Block]
- File Format Vulnerabilities: Allow [✓ Block]

Fraud Protection
- Known Phishing Sites: Allow [✓ Block]
- Suspected Phising Sites: Allow [✓ Block]
- Suspected Adware/Spyware Sites: Allow [✓ Block]
- Web Spam: Allow [✓ Block]

Unauthorized Communication Protection
- IRC Tunneling: Allow [✓ Block]
- Anonymizers: Allow [✓ Block]

Cross-Site Scripting (XSS) Protection
- Cookie Stealing: Allow [✓ Block]
- Potentially Malicious Requests: Allow [✓ Block]

The Advanced Threat Protection configuration screen in Zscaler provides the ability to set Allow or Block commands on the Advanced Threats Policy tab. Protection can be activated for botnet, malicious active content, fraud, unauthorized communication and cross-site scripting (XSS).

## 6.2 Detection

Zscaler finds infected devices by inspecting all outbound Internet traffic. The Zscaler platform intercepts botnet call-homes and attempts at exfiltrating data, including over encrypted channels and also identifies compromised devices. Zscaler also supports the ability to detect and block botnets, malware and other advanced threats on all ports and protocols.

New threats that are not detected by signature, AV and heuristic security can be detected by Zscaler Behavioral Analysis. Behavioral analysis is the only focus of FireEye, which is one dimensional so it does not provide defense in depth.

The main drawback of file sandboxing is that it takes a few minutes. This means that the first download of a “new” Zero Day file cannot be instantly blocked as malicious. Only subsequent downloads of the same file, after the file has been fully analyzed, can be blocked. Uniquely, Zscaler can actually quarantine the first download of a new file until the file is fully scanned, protecting against even the first download of a new malicious file.

Zscaler blocks newly identified malicious objects across its global system in real time. We verified that the list of malicious IPs and URLs found during our testing were blocked throughout the entire Zscaler network under 30 minutes.

Other observations noted for the Zscaler product:

- Secondary static analysis on all files newly created or created, including temporary files
- Additional analysis of network traffic leveraging Zscaler’s vast base of Internet traffic (13 billion transactions processed per day)
- Cloud Intelligence: Zscaler’s Behavioral Analysis is already deployed in more than 5,000 companies (13+ million users)
- Reports are available for all files (benign or malicious) scanned
- High-level report does not require deep security skills to make sense of it

| Comparison of detection | Zscaler | FireEye |
|---|---|---|
| 32-bit Windows executables | Yes | Yes |
| 64-bit Windows executables | Yes | Yes |
| PDF | Yes | Yes |
| Flash | Yes | Yes |
| Office documents | Yes | Yes |
| SSL | Yes, can inspect objects encrypted with SSL | No SSL decryption, requires additional hardware |
| Network effects and protection against first download | File fingerprints shared across entire system in real time, quarantine for patient zero | File fingerprint not always shared (depends on subscription), not real time, no quarantine |
| False positive: Spotify, Winrar, Windows updates, etc. | | |
| Presentation | 2-tier report: summary + technical details, information on each behavior and its meaning | Technical details for security researchers |
| Secondary static analysis | Details on files created or newly created | Technical details for security researchers |
| Metadata | Original samples, dropped files, PCAP, screenshots | Original sample, PCAP |

## 6.3 Remediation

When infections happen, administrators need to quickly determine who is infected, what was the impact of the infection, and have security measures in place to limit the loss of data and infection to other devices.

- Zscaler offers a large array of post-infection detection methods and also blocks exfiltration of data attempts, botnet calls, etc.
- FireEye's focus is on alerting. Company deploys other resources, such as end point agents or a Security Team, to respond to alerts.
- Zscaler's focus is on blocking threats and blocking data exfiltration No further action from the company should be needed other than to repair infected devices.
- Zscaler supports user authentication. Zscaler can report exactly who attempted to download a malicious object.
- Visibility: Zscaler shows all data in one place; FireEye shows malicious events only.
- Search: powerful in Zscaler; cannot look for a specific MD5 or URL with FireEye.
- Both products provide granular reports, but Zscaler is more organized and intuitive in providing the information.
- Data Leakage Protection is included with Zscaler, but not included with FireEye.

| Comparison of Remediation | Zscaler | FireEye |
|---|---|---|
| Botnet C&C detection | Block botnet call homes through blacklist and content inspection | Limited |
| Block traffic to suspicious destinations | Zscaler can block traffic to specific countries (ex: North Korea, China, Russia, etc.) | None |
| Block exfiltration of data, even if encrypted | Can block the exfiltration of credit card numbers, confidential documents, etc including over SSL channels | None |
| Logging | All traffic. Zscaler shows all transactions logs to give the administrator complete visibility of where a particular user went | Malicious transactions detected by FireEye only |
| Dashboard: view | All security events in one place | Few alerts |
| Dashboard: customization | All widgets can be edited and replaced. Time interval 1 day, 3 days, 7 days,1 month | Time interval: day, week, month |
| Report drill down | Analyze reports: per location, per user, per server, etc. | |
| Transaction logs | 30+ fields available | |
| Search | Search on a combination of any of the 30+ fields, MD5, URL, user, threat category, etc. | |
| User visibility | User aware: individual username per transaction, reports per user | IP and internal hostnames only |
| SIEM | Logs can be sent to a SIEM. Integrated with Splunk, ArcSight, | Use syslog to integrate with SIEM |

## 7.0 Deployment

Ease of deployment of FireEye and Zscaler was compared for a company with 5,000 employees in ten offices. Zscaler includes sandboxing of Windows executables for all of its customers at no change; advanced sandboxing and other operating systems are available for a monthly subscription fee.

- Zscaler: Cost increases only with number of users that are protected.
- FireEye: Cost increases with the number of boxes that are deployed and number of locations that are protected. Cost increases as bandwidth usage or volume of attacks grow.
- FireEye: Most deployment done in tap mode. Does not provide performance or high availability to be deployed inline in 95% plus of implementations.

| Comparison of Deployment | Zscaler | FireEye |
|---|---|---|
| Deployment | Turn on policy in Web UI | Add appliance to the network, route all web traffic through appliances, etc. |
| High availability | Built-in | Multiple appliances + additional hardware (F5 load balancer) |
| Deployment road-warrior<br>Deployment remote offices | Turn on policy in Web UI | Force remote users to VPN through HQ Remote offices: buy additional appliances or backhaul traffic |
| TCO | Cloud based approach is easier to deploy, more cost effective | IT staff must deploy, manage, maintain and upgrade the appliances. |

## 8.0 Common Limitations

While working with FireEye and Zscaler some common behaviors were identified that have an impact on the effectiveness of the products.

- Blocking archived files, such as ZIP, 7z and RAR, varied greatly between vendors. If a signature existed, the sample was often captured, but the sample could not be emulated in some sandboxes.
- Zscaler and FireEye had good detailed reports, but Zscaler excelled in that information was well organized, easy to navigate and effortless in drilling down to find specific information. It took more time to find specific information using FireEye.
- It was extremely difficult to figure out how to access the forensic reports for Zscaler's sandbox, but it was even harder to determine the source URL and filename on FireEye Web MPS.
- FireEye supports Mac OS X emulation today. Zscaler will not support Mac OS X emulation until 2015.

## 9.0 Bottom Line

We were more impressed with the Zscaler Internet Security Platform than we were with FireEye in how well the two systems blocked and detected threats, the accuracy of the sandbox for classifying malware types, the detailed information displayed on the reports, and the ease of use. The following lists more detail for each category.

- **Detecting and Blocking Multiple Type of Malware Threats**

  Zscaler is HIGHLY effective at blocking and detecting threats immediately with their first line of defense; anti-malware protection. Zscaler also outperformed FireEye in regard to the variation of samples that it was able to identify, which allows the product to offer better protection.

- **Sandbox Effectiveness and Accuracy**

  Zscaler is more accurate than FireEye Web MPS, in that it was able to catch both known and unknown samples that were completely missed by FireEye.

- **Forensic Reporting**

  Data visualization in Zscaler is clear and concise, which allows for better incident response time. FireEye reports were detailed but difficult to navigate.

- **Manageability and Effectiveness**

  Zscaler deployment is straightforward. The implementation is in line with industry standards. User interface is easy to use, which minimized deployment time, made it easier to administer, and much simpler to navigate.

  FireEye had a steeper learning curve and proper deployment takes much longer than the one hour suggested by FireEye.

## 10.0 About Miercom

Miercom has published hundreds of network-product-comparison 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.

## 11.0 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.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom. 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.

## 12.0 Fair Test Notification

FireEye was notified of this testing but has not yet provided comments or feedback to Miercom on this report..