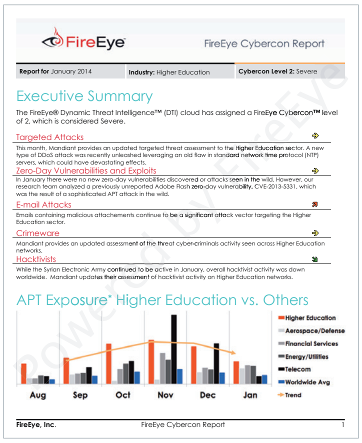
Service Overview

FireEye Managed Defense

Continuous Threat Monitoring and Protection by FireEye Experts

Highlights

- Improves threat protection and enhances the value of the FireEye Platform with 24x7 expertise from FireEye analysts
- Identifies who is attacking you, what their intention is, and how you should respond
- Assesses the risk of each attack and rapidly contains compromised devices
- Offers three service levels to align with your team's skills and risk tolerance
- Provides Global Security Operations Centers for follow-the-sun service


FireEye Cybercon Report

Report for January 2014	Industry: Higher Education	Cybercon Level 2: Severe

Executive Summary

The FireEye® Dynamic Threat Intelligence™ (DTI) cloud has assigned a FireEye Cybercon™ level of 2, which is considered Severe.

Targeted Attacks

This month, Mandiant provides an updated targeted threat assessment to the Higher Education sector. A new type of DDoS attack was recently unleashed leveraging an old flaw in standard network time protocol (NTP) servers, which could have devastating effects.

Zero-Day Vulnerabilities and Exploits

In January there were no new zero-day vulnerabilities discovered or attacks seen in the wild. However, our research team analyzed a previously unreported Adobe Flash zero-day vulnerability, CVE-2013-5331, which was the result of a sophisticated APT attack in the wild.

E-mail Attacks

Emails containing malicious attachements continue to be a significant attack vector targeting the Higher Education sector.

Crimeware

Mandiant provides an updated assessment of the threat cyber-criminals activity seen across Higher Education networks.

Hacktivists

While the Syrian Electronic Army continued to be active in January, overall hacktivist activity was down worldwide. Mandiant updates their assessment of hacktivist activity on Higher Education networks.

APT Exposure* Higher Education vs. Others

FireEye, Inc. FireEye Cybercon Report 1

FireEye® Managed Defense combines 24x7 continuous monitoring with intelligence, advice, and context about today's advanced threats. Find out who is attacking you, why, and what you need to do to quickly contain the incident and pivot to incident response when necessary. Managed Defense provides three subscription levels so you can appropriately supplement your team's skills and risk tolerance.

Continuous Monitoring

To help scale your security team, FireEye constantly monitors subscribed systems and informs you when alerts require follow up.

Continuous Protection

Accelerate your response with expert analysts from FireEye that investigate alerts and provide detailed compromise reports for each confirmed threat.

Continuous Vigilance

Actively pursue adversaries in your network with expert analysts that use advanced analytical techniques to find attackers hiding in remote corners of your network.

	Continuous Monitoring	Continuous Protection	Continuous Vigilance
Proactive APT and Zero-Day Alerts	•	•	•
Intelligence Reporting	•	•	•
System Health Monitoring	•	•	•
Analyst Investigation		•	•
On-Demand "Live Response"		•	•
Incident Response and Containment		•	•
Proactive Hunting for Adversaries			•
Advanced Investigative Techniques			•
Attacker Context and Risk Assessment			•

Service Overview

Continuous Monitoring

Proactive APT and Zero-Day Alerts—when FireEye detects an APT and/or a zero-day attack, our analysts provide a proactive notification with intelligence context so you can follow up on this attack as soon as possible.

Intelligence Reporting—subscribers receive monthly reports and alerts about emerging industry-specific threats. The FireEye Cybercon™ report communicates the risk severity and alerts subscribers to heightened industry- or region-specific risks.

System Health Monitoring—for continuous assurance, customers receive proactive notifications of potential issues that could compromise detection efficacy for all subscribed systems.

Continuous Protection

Analyst Investigation—the FireEye team of expert analysts evaluate detected attacks 24x7. When a potential compromise is detected, the team performs an in-depth analysis on affected systems to confirm the attack and delivers detailed reporting with actionable recommendations for threat protection.

On-Demand "Live Response"—FireEye analysts leverage system and network forensics on live systems to investigate, classify, and analyze the risk in real time. Information on what exactly happened and recommendations on how to contain the threat is immediately provided.

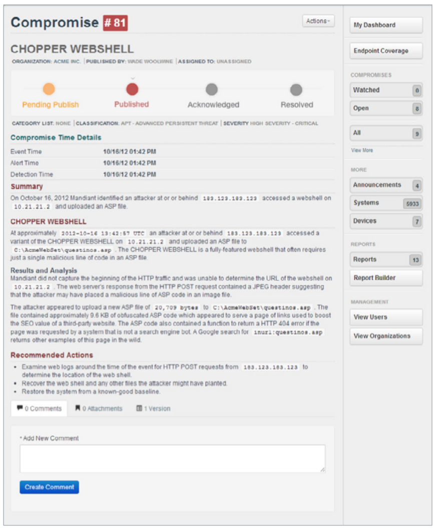
Incident Response and Containment—FireEye provides validated compromise reports with technical advice, contextual intelligence, and the ability to automatically contain compromised devices. In addition, the service will automatically pivot to incident response and remediation support at no additional cost for most incidents.

Continuous Vigilance

Proactive Hunting for Adversaries—based on the latest intelligence about attacker tactics, techniques, and procedures (TTPs), expert analysts and forensics specialists proactively hunt for signs of compromise and investigate your systems for attackers on your network.

Advanced Investigative Techniques—FireEye analysts use proprietary technologies and methodologies to investigate system artifacts, perform full-packet capture, conduct netflow analysis, and reverse-engineer malware to detect indicators of compromise (IOC).

Attacker Context and Risk Assessment—gain deeper insights by leveraging exceptional insight into threat actor tactics, modus operandi, and geo-political context gleaned from front-line incident response work, extensive intelligence research, and 100,000+ hours of incident response activity every year.



FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@FireEye.com | www.FireEye.com