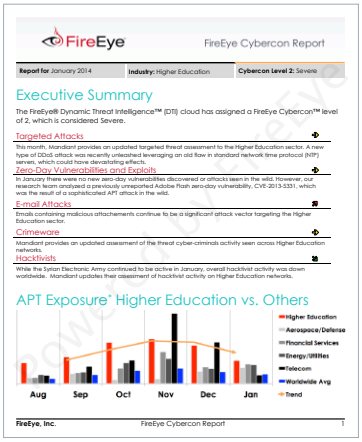
FireEye Managed Defense

FireEye 專家持續監控和防範威脅

重點

- 運用 FireEye 分析員全天候的專業，提升威脅防護措施及 FireEye 平台的價值。
- 找出攻擊者、攻擊意圖與回應方法。
- 分析各攻擊的風險，快速壓制被入侵的裝置
- 提供三大服務以因應貴團隊的技術和風險承受度。
- 提供 Global Security Operations Centers 全年無休的服務。


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 assesment 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 assesment of hacktivist activity on Higher Education networks.

APT Exposure* Higher Education vs. Others

Higher Education
Aerospace/Defense
Financial Services
Energy/Utilities
Telecom
Worldwide Avg
Trend

Aug Sep Oct Nov Dec Jan

FireEye, Inc. FireEye Cybercon Report 1

FireEye® Managed Defense 將全天候持續監控與今日先進威脅相關的情報、建議和內容加以整合。可找出攻擊者、攻擊原因與壓制事件所需採取的措施及必要事件回應錯失。Managed Defense 提供三大訂閱層級，讓您可補足團隊技術與風險承受度的不足。

Continuous Monitoring

爲了協助編制貴安全團隊，FireEye 持續監控訂閱系統，並在警告需要採取後續措施時通知您。

Continuous Protection

運用 FireEye 的分析專家加速回應能力，他們會調查警告並爲所有確鑿的威脅提供詳細的入侵報告。

Continuous Vigilance

運用分析專家主動找出網路內的罪犯，他們會使用進階分析技術來找出隱藏在網路遠端內的攻擊者。

	Continuous Monitoring	Continuous Protection	Continuous Vigilance
主動 APT 與零時差警告	●	●	●
情報報告	●	●	●
系統健全狀態監控	●	●	●
分析人員調查		●	●
隨選即用「即時回應」		●	●
事件回應與壓制		●	●
主動找到罪犯			●
先進調查技術			●
攻擊者檔案與風險分析			●

FireEye

服務一覽

Continuous Monitoring

主動 APT 與零時差警告—當 FireEye 偵測到 APT 和 (或) 零時差攻擊時，我們的分析人員即會提供附有情報內容的主動通知，讓您盡快回應攻擊。

情報報告—訂閱者每月會收到各業界最新威脅的報告和警告。FireEye Cybercon™ 報告會顯示風險嚴重度，並警告訂閱者特定業界或地區的重大風險。

系統健全狀態監控—爲了持續保障客戶，客戶將會收到主動通知，瞭解可能會影響各訂閱系統偵測效能的潛在問題。

Continuous Protection

分析員調查—FireEye 分析專家團隊將會全天候評估所偵測到的攻擊。偵測到潛在問題時，該團隊會對受影響的系統進行深入的分析、確認攻擊屬實，並提供詳細報告內有防範威脅的可行建議。

隨選即用「即時回應」—FireEye 分析員對運作中的系統採用系統和網路鑑識作業，即時調查、分類和分析風險。立即提供確實狀況的資訊及如何壓制威脅的建議。

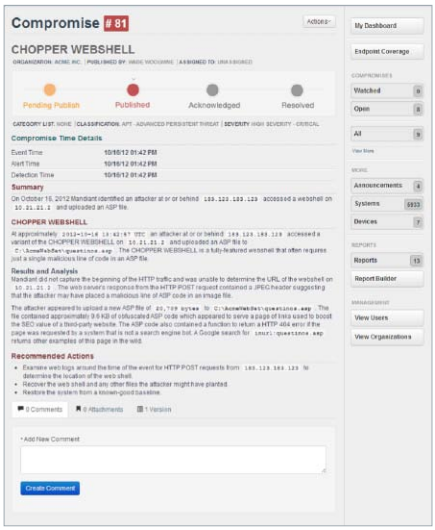
事件回應與壓制—FireEye 提供經驗證的入侵報告，內含技術建議、情報內容和自動壓制遭入侵裝置的功能。此外，針對多數事件，客服會自動將您免費轉至事件回應和修復支援部門。

Continuous Vigilance

主動找出嫌犯—分析專家和鑑識專家會依照攻擊者手法、技術和程序 (TTP) 的最新情報，主動找出入侵的跡象，並調查系統找出網路中的攻擊者。

先進調查技術—FireEye 分析員運用專屬技術和方法來調查系統元件、執行全面追捕、進行流量分析 (IOC)，及對惡意軟體執行逆向工程，加以偵測入侵指標 (IOC)。

攻擊者檔案與風險分析—利用從前線事件回應工作、大規模情報研究和每年超過 100,000 小時的事件回應行動所收集到的威脅發動者策略、作案手法和地理政治背景，更深入瞭解案情。



FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | APAC@FireEye.com | www.FireEye.com