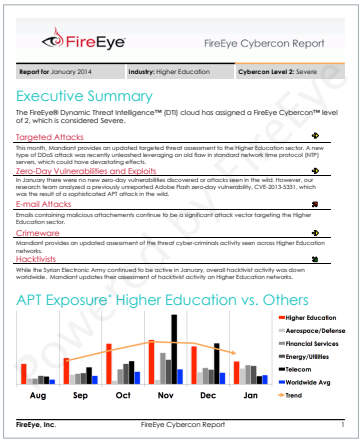
FireEye Managed Defense

Supervisión y protección de amenazas continuas a cargo de los expertos de FireEye

Aspectos destacados

- Mejora la protección contra amenazas y aumenta el valor de la plataforma FireEye con el acceso 24x7 a la experiencia de los analistas de FireEye.
- Identifica al atacante, sus intenciones y la forma en que se debería reaccionar.
- Evalúa el riesgo de cada ataque y contiene rápidamente los dispositivos amenazados.
- Ofrece tres niveles de servicio acordes con su tolerancia a riesgos y las habilidades de su personal.
- Proporciona Global Security Operations Centers para dar un servicio permanente.


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

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 combina vigilancia continua 24x7 con información, asesoramiento y contexto sobre las amenazas avanzadas de la actualidad. Averigüe quién le ataca, por qué y qué debe hacer para contener rápidamente el incidente y pasar a la respuesta cuando sea necesario. Managed Defense se ofrece con tres niveles de suscripción para que pueda complementar convenientemente su tolerancia a riesgos y las habilidades de su personal.

Continuous Monitoring

Para ayudarle a dimensionar su equipo humano de seguridad, FireEye supervisa constantemente los sistemas suscritos y le informa de las alertas que requieren seguimiento.

Continuous Protection

Acelere su respuesta con analistas expertos de FireEye que investiguen las alertas y elaboren informes detallados de los riesgos de cada amenaza confirmada.

Continuous Vigilance

Persiga activamente a los enemigos de su red gracias a analistas de primer nivel que se sirven de técnicas avanzadas para encontrar a los atacantes que se ocultan en rincones remotos de su red.

	Continuous Monitoring	Continuous Protection	Continuous Vigilance
Alertas proactivas de APT y de día cero	•	•	•
Informes con datos	•	•	•
Supervisión del estado del sistema	•	•	•
Investigación a cargo de analistas		•	•
"Respuesta en directo" a demanda		•	•
Respuesta y contención de incidentes		•	•
Búsqueda proactiva de adversarios			•
Técnicas avanzadas de investigación			•
Contexto de los ataques y evaluación de riesgos			•

FireEye

Descripción de los servicios

Continuous Monitoring

Alertas proactivas de APT y de día cero: cuando FireEye detecta una APT o un ataque de día cero (aún no conocido), nuestros analistas envían una notificación proactiva con información contextual para que sea posible llevar a cabo un seguimiento de este ataque a la mayor brevedad posible.

Informes con datos: cada mes los suscriptores reciben informes y alertas sobre las amenazas sectoriales que van apareciendo. El informe FireEye Cybercon™ comunica la gravedad de los riesgos y alerta a los suscriptores de las amenazas más claras sectoriales o regionales.

Supervisión del estado del sistema: para lograr una seguridad ininterrumpida, los clientes reciben notificaciones anticipadas de los posibles problemas que podrían poner en peligro la eficacia de la detección en todos los sistemas suscritos.

Continuous Protection

Investigación a cargo de analistas: el equipo de analistas expertos de FireEye evalúa los ataques detectados durante las 24 horas del día y los 7 días de la semana. Cuando se detecta un peligro, el equipo analiza a fondo los sistemas afectados para confirmar el ataque y elabora un informe detallado con las actuaciones recomendadas como protección frente a la amenaza.

"Respuesta en directo" a demanda: los analistas de FireEye hacen uso de técnicas forenses de redes en sistemas activos para investigar, clasificar y analizar el riesgo en tiempo real. De inmediato se distribuye información sobre lo que ha sucedido exactamente, con recomendaciones para contener la amenaza.

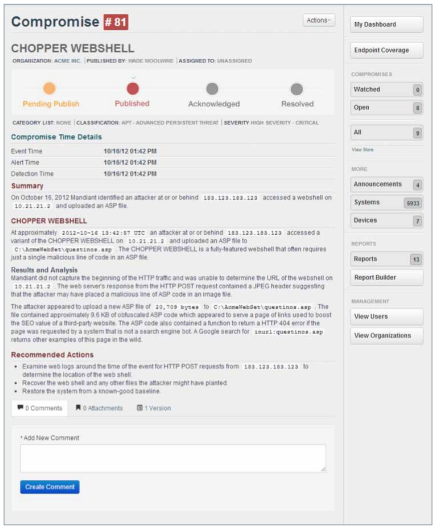
Respuesta y contención de incidentes: FireEye ofrece informes validados sobre riesgos con asesoramiento técnico, información contextual y la capacidad de impedir de forma automática el deterioro de los dispositivos afectados. Además, en la mayoría de los incidentes, el servicio pasará automáticamente a dar remediación y respuesta sin costo adicional.

Continuous Vigilance

Búsqueda proactiva de adversarios: en función de la información más reciente sobre los ataques y sus tácticas, técnicas y procedimientos (TTP), los analistas expertos y los especialistas forenses buscan proactivamente signos de riesgo e investigan la presencia de atacantes en la red.

Técnicas avanzadas de investigación: los analistas de FireEye usan tecnologías y metodologías propias para investigar alteraciones en el sistema, capturar paquetes completos, analizar el flujo de la red y aplicar ingeniería inversa al malware a fin de detectar indicadores de riesgo.

Contexto de los ataques y evaluación de riesgos: mejore sus conocimientos con la excepcional información de las tácticas, el modus operandi y el contexto geopolítico de los creadores de las amenazas, recopilado gracias al trabajo en primera línea de repuesta a incidentes, a la extensa investigación y a las más de 100 000 horas dedicadas cada año a la actividad de respuesta a incidentes.



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