Presentación a Cliente

PREPARADO PARA

vialynk

GLOBAL SERVICE COVERAGE

Offices in: Melbourne, San Francisco, London & Dubai

FraudWatch International

Sobre Nosotros

Somos Comprobados y Confiados Globalmente

- Una empresa privada de seguridad de Internet
- Fundada en 2003
- Líderes en el Anti-Phishing y la industria de protección de marca en línea
- Con sede en Melbourne, Australia
- Oficinas en:
  - San Francisco
  - Dubai
  - Londres
- Centro de Operaciones de Seguridad abierto 24x7x365
- 2018 tiempo de takedown medio - 1 hora 51 minutos
- 2018 Promedio de tiempo de takedown - 7 horas 14 minutos

GLOBAL CLIENT BASE

4 OFFICE LOCATIONS

MULTI LINGUAL STAFF

THOUSANDS OF BRANDS PROTECTED

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

Productos Ofrecidos

FraudWatch International ofrece un servicio exhaustivo y completo de protección de marca en línea para combatir el fraude en línea, el abuso de marca y la suplantación de identidad.

GLOBAL SERVICE COVERAGE

Offices in: Melbourne, San Francisco, London & Dubai

FraudWatch International

Nuestros Servicios

Protección de Marca en Línea

FraudWatch International

Suite de Protección de Marca Empresarial

PHISHING

- Abuso de marca
- Vishing
- Smshing
- Pharming
- Mensajería
- Monitoreo de Dark Web
- * Interceptor
- * DMARC

MALWARE

- Command and Control
- Drop Zones

SOCIAL MEDIA

- Suplantación de marca
- * Suplantación de Ejecutivos

MOBILE APPS

- Listados de aplicaciones móviles no autorizadas
- Aplicaciones maliciosas para Android y iPhone

**El asterisco indica servicios adicionales (opcional)*

COMBINADO CON LA RESPUESTA DE INCIDENTES DE FRAUDWATCH INTERNATIONAL

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

Anti-Phishing

Soluciones de FraudWatch International

MONITOREO EN TIEMPO REAL

Pre-ataque:
- Protección del código fuente
- Supervisión de registro de dominios

FraudWatch Interceptor

Detección de ataque:
- Miles de millones de correos electrónicos de spam escaneados diariamente
- Monitoreo de servidores y sitios web maliciosos
- Seguimiento de DNS
- Supervisión de las fuentes de datos del cliente
- Análisis de cuentas de correo para abuso
- Análisis de rebote de correo electrónico

EL ANÁLISIS FORENSE

FraudWatch International SOC realiza análisis humanos en todos y cada uno de los sitios de phishing.
- Las URL / carpetas de phishing adicionales se capturan y se eliminan
- Los redireccionamientos de phishing se dan de baja, haciendo que un correo electrónico de phishing sea nulo

Información forense agregada al portal orientado al cliente, PhishPortal:
- Suplantación de identidad del código fuente del sitio web,
- sitio web de Phishing capturas de pantalla,
- Phish Kits
- Credenciales Robadas, si están disponibles,
- Dirección de IP / la información de Host

MITIGACIÓN DE AMENAZAS Y TAKEDOWN DE INCIDENTES

Mitigación
- Dilución de phishing
- Cebo de credenciales de sitio de phishing
- Cierre de redirección de phishing

Incident Takedown
- El tiempo de inactividad más rápido posible, cada vez
- Relaciones directas con:
- Método de codificación de datos:
  - Web Hosts / ISP's
  - Registradores de dominio
  - Equipos locales CERT
- Contacto simultáneo de múltiples canales
- Correo electrónico y contacto telefónico
- Nunca nos damos por vencidos!

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

Abuso de Marca

Evaluación | Monitoreo | Derribar

FraudWatch International evalúa posibles problemas de abuso de marca presentados por nuestros clientes, para determinar el potencial de takedown o eliminación del contenido de la marca infractora. Cabe señalar que no todas las menciones de una marca se pueden eliminar, y no censuramos Internet, sin embargo, si se infringe una marca o registro de marca comercial, FraudWatch International trabajará para que esto sea removido de Internet.

- Infracción de marcas Comerciales
- Contenido de derechos de autor (Copyright)
- Suplantación de marca

Métodos comunes de abuso de marca

www.phishportal.com
www.fraudwatchinternational.com

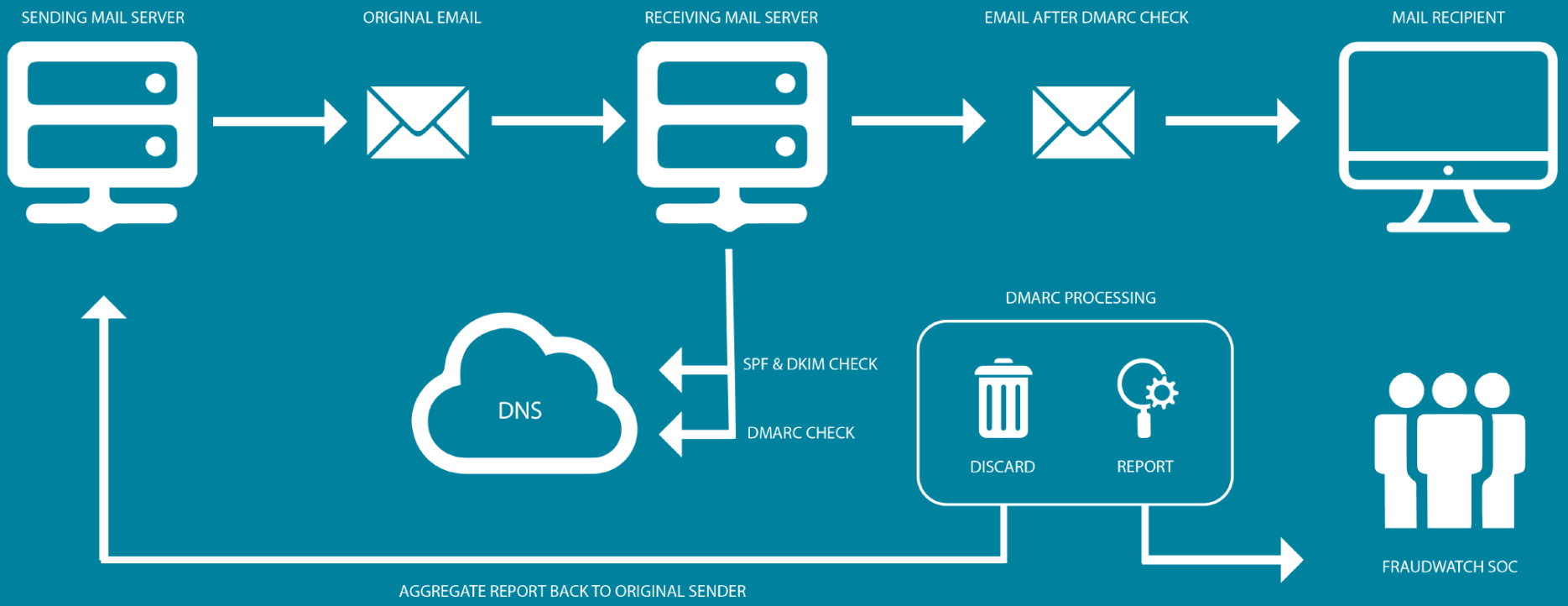
AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

DMARC

¿Qué es Eso?

FraudWatch International



www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

DMARC

Beneficios

- Aumento de la velocidad de mitigación de amenazas
- Mayor visibilidad del dominio de correo electrónico
- Autenticación mejorada
- Concientización sobre el fraude en línea
- Protección del dominio de correo electrónico

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN
SECURITY
EXPERTS

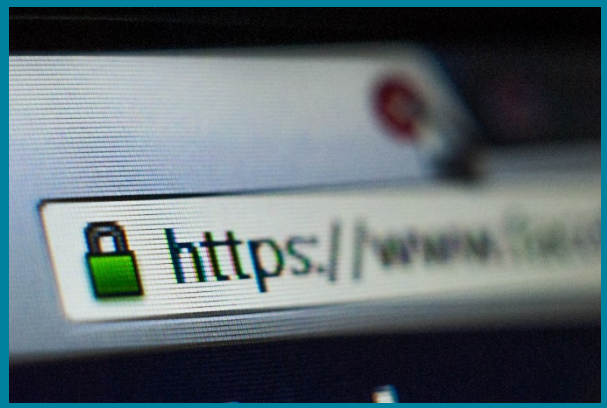
Interceptor

Identificar Cuentas Comprometidas

¿Qué pasaría si pudiera tener notificaciones en tiempo real de cuentas comprometidas al mismo tiempo que los delincuentes lo hacen?

- Detección inmediata de los sitios de phishing
- Bloquear transacciones en la cuenta: reducir las pérdidas por fraude
- Educar al usuario comprometido
- Desalentar delincuentes

No es la solucion perfecta, ¡pero está cerca!



www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN
SECURITY
EXPERTS

Interceptor

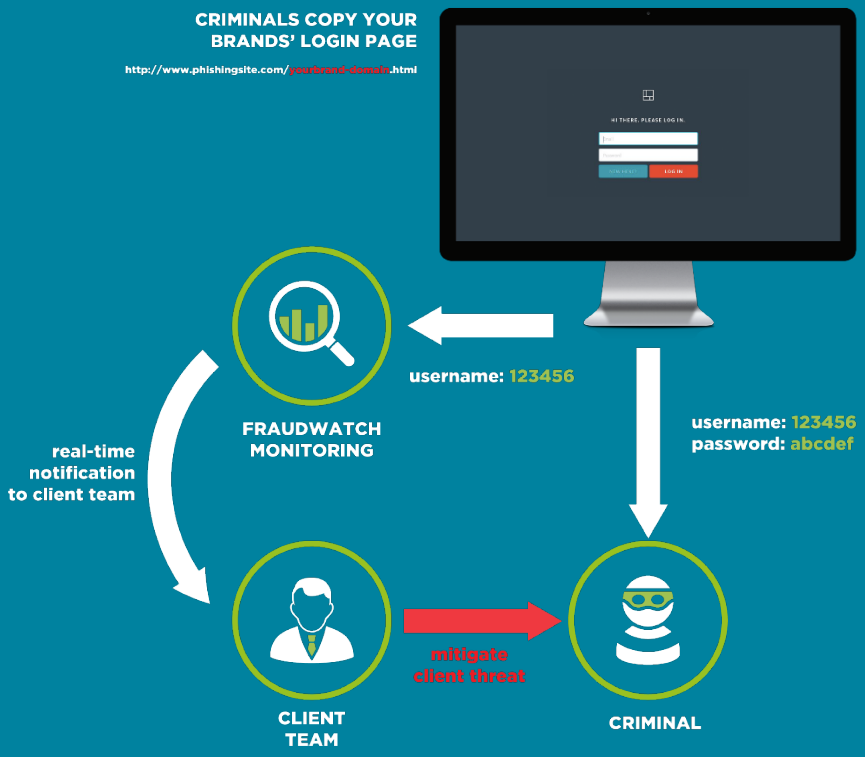
Monitoreo de Credenciales de Cliente

FraudWatch International codifica en forma avanzada el script Interceptor específico del sitio del cliente.

El script de FraudWatch International Interceptor permanece inactivo en el sitio genuino y no realiza ninguna función.

El script de FraudWatch International Interceptor captura el nombre de usuario / ID de cliente directamente desde el sitio de phishing en tiempo real.

CÓMO INTERCEPTOR AYUDA A SU MARCA



www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

Anti-Malware

Evaluación | Monitoreo | Derribar

Los archivos de malware se distribuyen más comúnmente por correo electrónico haciéndose pasar por una factura o archivo legítimo. Una vez abierto por el consumidor estos archivos de malware se instalarán en su máquina (en la mayoría de los casos, en silencio).

Cuando el usuario va a abrir su banco online u otro inicio de sesión donde se dirige el ataque, sus credenciales se pasarán directamente al criminal, a menudo sin que el usuario lo sepa. Los delincuentes están cambiando constantemente sus técnicas de distribución e infección para permanecer sin ser detectados.

Malware no sólo está dirigido a PC, con una gran aumento en el mercado móvil / tablets, Malware esta convirtiéndose en la tendencia cambiante.

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

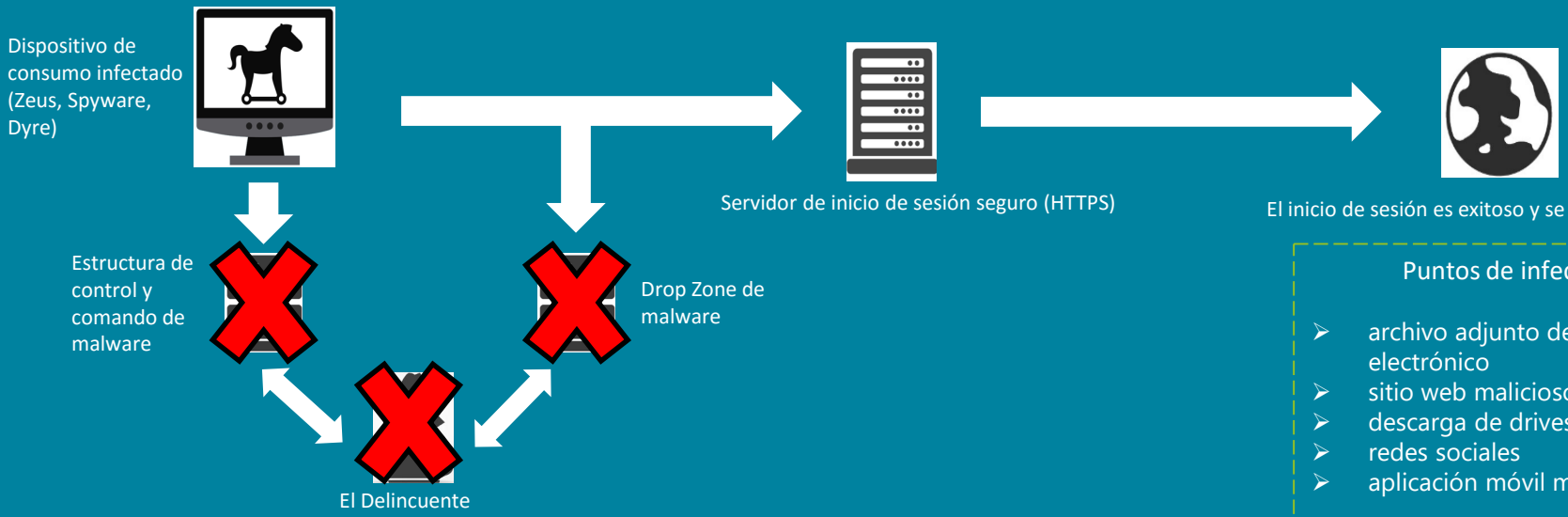
HUMAN
SECURITY
EXPERTS

Anti-Malware

Evaluación | Monitoreo | Derribar

Sesión de inicio de sesión seguro normal

Sesión de inicio de sesión de dispositivo comprometido



Puntos de infección:

- archivo adjunto de correo electrónico
- sitio web malicioso
- descarga de drives
- redes sociales
- aplicación móvil maliciosa

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

Anti-Malware

Soluciones de FraudWatch International

MONITOREO EN TIEMPO REAL

Detección de ataque

- Monitoreo de fuentes de datos de malware: proveedores globales de AV y organizaciones de identificación de malware
- Global honeypots / trampas de spam para capturar muestras de malware
- Supervisión de las fuentes de datos del cliente
- Seguimiento de la clandestinidad de Malware para analizar las tendencias de desarrollo de Malware

EL ANÁLISIS FORENSE

- Amplio análisis de malware para identificar todos los vectores de ataque relevantes y el comportamiento de malware
- Información forense agregada a PhishPortal para referencia del cliente:
- - Copias de archivos Malware relevantes
- - Dirección IP / alojamiento de información
- - Capturas de pantalla (si corresponde)

MITIGACIÓN DE AMENAZAS Y TAKEDOWN DE INCIDENTES

Mitigación

Cierre de todos los vectores de ataque relevantes para interrumpir el malware en todas las formas posibles (descarga de malware / puntos de infección, Command and control, Drop Zones y redirecciones de malware)

Takedown de incidents

El tiempo de taedown más rápido posible, siempre
Relaciones directas con:
Método de codificación de datos:
- Web Hosts / ISP's
- Registradores de dominio
- Equipos locales CERT

Contacto simultáneo de múltiples canales
Correo electrónico y contacto telefónico
Nunca nos damos por vencidos!

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

Social Media

Monitoreo | Takedown

Usos potenciales para un perfil falso de redes sociales:

- Dirigir a los clientes a un sitio de phishing para obtener información de inicio de sesión
- Intentos de Ingeniería Social
- Dirigir a los clientes a una descarga de archivos maliciosos para infectar su PC o dispositivo móvil
- Vender información o una lista de contactos de los clientes de una empresa (seguidores) a un competidor
- Comunicar información falsa en un intento de influir en el precio de las acciones de una empresa
- Simplemente venda un perfil de redes sociales exitoso al propietario legítimo de la marca

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN
SECURITY
EXPERTS

Social Media

Respuesta a Incidentes

MONITOREO EN TIEMPO REAL

Detección de ataque
Monitoreo en tiempo real de las redes de redes sociales, incluidas (pero no limitadas a):

- Facebook
- Instagram
- Twitter
- LinkedIn
- YouTube

EL ANÁLISIS FORENSE

- Análisis de páginas de redes sociales sospechosas por infracción de marcas relevantes y derechos de autor.
- Las páginas sospechosas / perfiles de redes sociales se informan al cliente para la aprobación de su eliminación, para garantizar que no se eliminen páginas legítimas.

MITIGACIÓN DE AMENAZAS Y DESCANSO DE INCIDENTES

Incident Takedown

- Social Media providers are contacted and relevant trademark / copyright infringement requests are raised in order to have clients intellectual property removed.

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

Mobile Apps

Monitoreo | Takedown

Usos potenciales para falsas Aplicaciones móviles:

- Enviar credenciales de inicio de sesión directamente al criminal (Phishing)
- Permitir que las sesiones del navegador sean secuestradas (Malware)
- Toma el control del dispositivo móvil (Malware)
- Facilitar ataques de Man in the middle (Malware)
- Instalar otras formas de malware en el dispositivo, como adware o ransomware

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN
SECURITY
EXPERTS

Mobile Apps

Respuesta a Incidentes

MONITOREO EN TIEMPO REAL

Detección de ataque

- Monitoreo en tiempo real de las tiendas de aplicaciones oficiales:
  - Google Play
  - iTunes Store
  - Tienda Blackberry
  - Tienda OVI (Nokia)
  - Tienda de Windows

- Monitoreo de tiendas de aplicaciones de terceros para encontrar .apk (Android) y .ipa (iPhone) archivos maliciosos – esto incluye aplicaciones de iPhone jailbreak

EL ANÁLISIS FORENSE

- Análisis de aplicaciones móviles sospechosas para ver si están dirigidas al cliente
- Todas las aplicaciones no autorizadas se envían directamente al cliente para su aprobación de eliminación para garantizar que no se desconecten aplicaciones legítimas
- Si las aplicaciones se comunican con cualquier página de phishing en línea, también se analizarán y eliminarán como un incidente de phishing

MITIGACIÓN DE AMENAZAS Y TAKEDOWN DE INCIDENTES

Desmontaje de incidents

- Las tiendas de aplicaciones móviles relevantes se contactan directamente con cartas de cese and desist para eliminar las aplicaciones relevantes.

- Los equipos locales de CERT también son contactados para obtener más ayuda si es necesario

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN SECURITY EXPERTS

PhishPortal

Portal de Clientes para Informes de Servicios

- Portal de cliente en línea
- Gestión de incidentes en tiempo real
- Comunicación en tiempo real
- Análisis forense y de amenazas
- Suite de informes completo
- Informes mensuales ejecutivos de clientes

www.phishportal.com
www.fraudwatchinternational.com

AU +61 3 9887 6777
US +1 415 449 8800
UK +44 20 3974 1444

HUMAN
SECURITY
EXPERTS

FIN DE LA PRESENTACIÓN

Si tiene alguna pregunta sobre la información en esta presentación, no dude en preguntarnos ahora o más tarde enviándonos un correo electrónico a sales@fraudwatchinternational.com

GLOBAL SERVICE COVERAGE

Offices in: Melbourne, San Francisco, London & Dubai

FraudWatch International