EASYSOLUTIONS

DETECT MONITORING SERVICES Y DETECT SAFE BROWSING:

Herramientas Poderosas, Proactivas y Colaborativas Contra Ataques de Phishing, Pharming y Malware.

RESUMEN

Los robos de credenciales de acceso a cuentas bancarias esta en aumento, especialmente con ataques de Phishing, Pharming y Malware, que aprovechan la vulnerabilidad del usuario final. Para una protección eficaz contra estas amenazas es indispensable adoptar una estrategia de proteccion proactiva que incluya a los usuarios. Detect Monitoring Services y Detect Safe Browsing son dos herramientas de vanguardia que pueden detener ataques antes de que ocurran y que ayudan a cumplir con regulaciones de seguridad, que cada día son mas exigentes para las instituciones financieras.

TABLA DE CONTENIDO

AMENAZAS CRECIENTES

1

Casos Emergentes de Phishing y Malware con Motivaciones Financieras

Las instituciones financieras están en desventaja cuando se trata de proteger a sus clientes no precavidos contra el fraude. Los estafadores en línea son muy conscientes de esta realidad, por lo que constantemente lanzan sofisticados ataques organizados para obtener información sensible de las cuentas como nombres de usuario, contraseñas y respuestas a preguntas de reto. Con esta información, se pueden apropiar de cuentas corporativas y de esta forma, realizar fraudes en transacciones electrónicas y de ACH que ascienden a millones de dólares en pérdidas anuales.

Los cibercriminales tienen varios métodos para robar credenciales, pero los más usados son aquellos relacionados con ataques de phishing y malware que infectan los computadores de escritorio y portátiles de las pequeñas y medianas empresas. En un ataque de phishing, los estafadores se hacen pasar por una entidad confiable en una comunicación electrónica como un correo electrónico. Estos correos son diseñados con tanta precisión que pueden imitar gran variedad de fuentes legítimas como sitios web sociales, socios comerciales, instituciones financieras y administradores de IT.

Con frecuencia, estos correos dirigen a los desprevenidos usuarios a un sitio web fraudulento donde proporcionan información sensible de sus cuentas, que luego es capturada por los criminales.

En cuanto al malware, el computador de un empleado de una compañía puede verse comprometido al abrir un documento corrupto adjunto a un correo electrónico o al dar click en un link que conecta a un sitio malicioso. Las memorias USB y redes sociales legítimas también sirven como portadores para esparcir el malware. Por ejemplo, los virus y troyanos pueden ser descargados al hacer click en un video o foto infectada.

En ataques recientes, los criminales han combinado el phishing y el malware. Primero, envían correos electrónicos diseñados con tanta precisión que imitan a los de una organización acreditada. Estos sofisticados correos se ven y se sienten tan reales que incluso los individuos más cuidadosos son engañados y terminan dando click en el contenido malicioso. Estos links llevan a los incautos empleados a sitios web fraudulentos que también parecen auténticos, donde otro click los lleva a descargar malware y su computador queda así infectado.

AMENAZAS CRECIENTES

1

Institución Financiera	Organización Atacada	Pérdidas Económicas Estimadas
Comerica Bank	Experi-Metal Inc.	$550K
Professional Business Bank	Village View Escrow	$465K
BankcorpSouth	Choice Escrow	$440K
PlainsCapital Bank	Hillary Machinery	$800K
Bankers Trust	Catholic Diocese of Des Moines	$600K
Ocean Bank	Patco	$500K

El malware instala keyloggers que capturan las credenciales tan pronto como el usuario ingresa sus datos en el sitio de la banca en línea. Con esta información en sus manos, el criminal obtiene acceso completo a la cuenta y por lo tanto, tiene el poder para realizar transferencias. Finalmente, los fondos suelen ser enviados al exterior por medio de transferencias electrónicas extra bancarias y el dinero sustraído se pierde para siempre.

Uno de los mayores obstáculos para la institución financiera es que debe asumir que las sesiones bancarias y las subsecuentes transferencias realizadas por el criminal son legítimas. Cuando la compañía afectada descubre que hubo una brecha en la seguridad, casi siempre es demasiado tarde para recuperar el dinero. Además, cuando los negocios comerciales y los individuos sufren la apropiación de sus cuentas, la institución financiera asociada debe responder por las pérdidas económicas. Innumerables horas de investigación, daños irreparables a la reputación y disputas legales que casi nunca favorecen a la institución, sólo agravan la situación.

El modelo actual de negocios no va a cambiar en el futuro inmediato. Las compañías e individuos por igual seguirán realizando transacciones en línea a través de sus computadores, ya que sus actividades diarias así lo requieren. Sin duda alguna, las compañías seguirán siendo objeto de sofisticados ataques de ingeniería social, que tendrán éxito al robar directamente las credenciales o instalar malware que realizará esta labor más adelante. Por lo tanto, las instituciones financieras tienen dos opciones: seguir reembolsando los dineros perdidos a las víctimas de apropiación de cuentas corporativas o comenzar a implementar nuevas soluciones proactivas que puedan prevenir en primer lugar la apropiación.

Easy Solutions ha desarrollado dos tecnologías poderosas, proactivas y colaborativas que protegen tanto a la institución financiera, como a sus clientes de los ataques de phishing, pharming y malware.

DETECT MONITORING SERVICES

2

Protección Proactiva Contra Phishing

Detect Monitoring Services (DMS) es un nivel de seguridad dominante que detecta y elimina a los usuarios maliciosos que visitan el sitio web de una institución financiera. DMS utiliza tecnología que recoge en tiempo real información de alto nivel de la conexión del usuario, como la geo-localización asociada de la dirección IP, proveedor del servicio de Internet, historial de visitas del usuario, hora del día, tipo de sistema operativo usado y demás información relevante. La información capturada es usada para alimentar un motor de correlación que identifica al usuario malicioso.

En esta etapa, el equipo de Easy Solutions que se encarga de monitorear las conexiones al sitio web 7x24x365, recibe inmediatamente una alerta y rastrea la actividad en línea del usuario.

El equipo de DMS observa e investiga las acciones del usuario. Por ejemplo, ¿el usuario solo está explorando el sitio web, lo está copiando o está inyectando un código malicioso para explotar una vulnerabilidad en la seguridad de una aplicación del sitio web? Si hay actividad maliciosa no autorizada por parte del usuario, equipo de DMS notifica a la institución financiera y luego desactiva cualquier sitio de phishing fraudulento que haya sido creado. En resumen, DMS protege a todas las entidades en línea de la institución financiera protegida.

Hoy más que nunca las instituciones financieras necesitan proteger proactivamente sus canales bancarios en línea, ya que los cibercriminales buscan activamente explotar sitios web vulnerables. DMS es un servicio con una tecnología inteligente que da el poder a las instituciones financieras para que trabajen en la zona proactiva de detección de actividad maliciosa y phishing y para que frenen ataques incluso antes de ser lanzados.

*Anti-Phishing Working Group 2H 2010

DETECT SAFE BROWSING

3

Protección al Nivel del Usuario Final

Easy Solutions ha cubierto el gran vacío existente en la seguridad al nivel del usuario final y ha creado Detect Safe Browsing (DSB) para llenarlo. DSB es una aplicación sencilla pero poderosa que protege a los usuarios finales de modalidades de fraude en la banca electrónica, como phishing o pharming, donde los antivirus y software para la eliminación de malware no son efectivos. DSB proporciona protección en tiempo real contra el malware y se instala y opera en el computador del usuario final que realiza la transacción bancaria en línea.

El archivo Hosts representa un serio vector de ataque para el software malicioso, debido a que su función es asociar nombres de servidores con direcciones IP. Si el archivo Hosts es modificado y envenenado por virus con motivaciones financieras o troyanos, el usuario es redireccionado del destino deseado hacia sitios web fraudulentos. Estos sitios diseñados por medio de ingeniería social parecen auténticos y capturan la información sensible de los usuarios incautos.

DSB funciona de la siguiente forma: antes de que el usuario se conecte al sitio web de la banca en línea, DSB realiza un escaneo rápido del archivo Hosts y de los procesos en funcionamiento en el computador del usuario final. Si DSB detecta un proceso malicioso que está envenenando el servidor DNS o el archivo Hosts, TANTO el usuario final COMO la institución financiera son notificados instantáneamente.

Al usuario se le advertirá que su computador está infectado y se le recomendará enfáticamente no proseguir con la sesión bancaria en línea. La institución financiera puede monitorear cuidadosamente las transacciones del usuario hasta que el proceso malicioso sea detenido y eliminado por el usuario.

DSB también verifica que la dirección IP que el usuario final desea visitar coincida con la dirección IP protegida consignada en el servidor de Easy Solutions. La validación de la IP proporciona protección en tiempo real contra pharming y evita que el usuario sea redireccionado a páginas web falsificadas, donde su información personal puede ser robada.

DETECT SAFE BROWSING

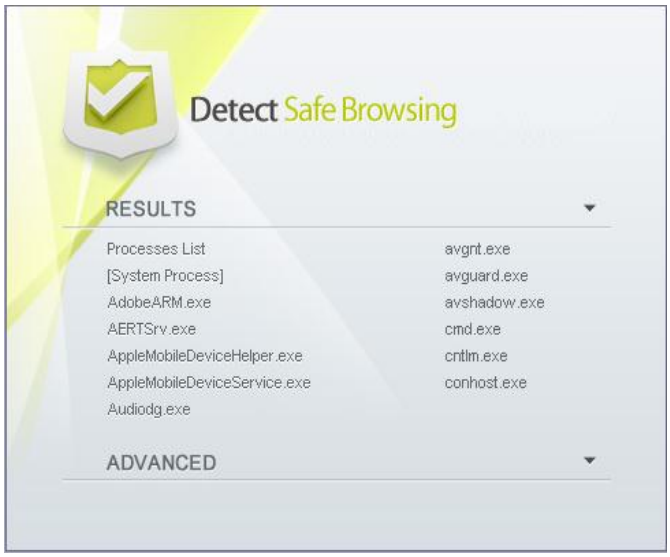
3

Características Clave de Detect Safe Browsing

DSB puede ser customizado para cumplir con las necesidades de gestión de marca de cualquier institución financiera. Ha sido diseñado para ser no intrusivo, efectivo y veloz; el proceso de escaneo solo dura algunos milisegundos. La aplicación se instala una sola vez y el usuario final no necesita hacer actualizaciones, solo se actualiza el servidor de Easy Solutions. A medida que nuevos procesos de malware son desarrollados y evolucionan, Easy Solutions los agrega a una lista negra en constante actualización. La actividad maliciosa también es registrada y se generan reportes históricos, que mantienen a las instituciones financieras conectadas y al tanto de las amenazas que las afectan a ellas y a sus clientes.

DBS detecta y protege contra las siguientes amenazas:

- Envenenamiento del archivo Hosts
- Ataques de Pharming
- Ataques de Malware, incluyendo:
  - Key loggers y screen loggers
  - Malware con motivaciones financieras
  - Man in the middle (Proxy)
  - Man in the middle (Envenenamiento del ARP)
  - Man in the middle (Debilidades en el SSL)



DMS Y DSB TRABAJANDO JUNTOS

4

Productos Innovadores que Cambian las Reglas de la Industria

Es importante resaltar y comprender que DMS y DSB se alimentan mutuamente. Por ejemplo, si DSB detecta actividad maliciosa en el dispositivo de un usuario final, lo más probable es que más usuarios también hayan sido afectados. En este caso, el equipo de DMS recibe la información y comienza el proceso de desactivación. Así, todos los usuarios se benefician de la protección colaborativa en tiempo real, un elemento diferenciador en la industria.

También cabe anotar que, a la luz de las recientes demandas interpuestas por las compañías en contra de sus instituciones financieras por ofrecer inadecuadamente "soluciones de seguridad comercialmente razonables", tanto DMS como DSB pueden ofrecer a los bancos tranquilidad en los estrados judiciales. Cuando una institución financiera ofrece DSB a sus clientes, los negocios que sean víctimas del malware no podrán argumentar que nunca se les ofreció una solución de seguridad al nivel del usuario final. Las instituciones también pueden recalcar que DMS está protegiendo proactivamente sus canales bancarios en línea.

MS y DSB también pueden ayudar a las instituciones financieras a cumplir con regulaciones. Los organismos reguladores exigen que las instituciones lleven a cabo evaluaciones de su seguridad y herramientas de IT con regularidad. Cuando se descubren vulnerabilidades, estos organismos quieren ver qué acciones toman las instituciones para aliviar el problema. DMS y DSB son soluciones que ayudan a mitigar el fraude bancario en línea al frenar el phishing, pharming y malware.

Las instituciones financieras entienden que la guerra contra el fraude electrónico no terminará pronto y que deben implementar soluciones que lo combatan efectivamente; también saben que hay una creciente lista de regulaciones que deben seguir. DMS y DSB ofrecen a las instituciones financieras un nivel de seguridad asequible y no intrusivo, que protege al sitio web bancario en línea y a los altamente riesgosos equipos de los usuarios finales.

COMIENCE A PROTEGER A SU INSTITUCIÓN FINANCIERA Y SUS CLIENTES CON DETECT MONITORING SERVICE Y DETECT SAFE BROWSING

Para información adicional o demostraciones de DMS y DSB, por favor escriba a info@easysol.net o visite el sitio web de Easy Solutions.

ACERCA DE EASY SOLUTIONS

5

Easy Solutions es el único proveedor de seguridad que se enfoca exclusivamente en la prevención del fraude, proporcionando servicios antiphishing, autenticación multi-factor y detección de anomalías transaccionales.

Easy Solutions posee un enfoque integral para manejar la prevención del fraude multi-canal y trabaja en alianza con líderes de la industria de otras áreas de seguridad soportando un amplio rango de plataformas heterogéneas.

EASYSOLUTIONS

Headquarters:
1401 Sawgrass Corporate Parkway, Sunrise, FL 33323 – Tel. +1-866-5244782

Latin America:
Cra. 13A No. 98 – 21 Of. 401 Bogota, Colombia – Tel. +57 1- 7425570.

www.easysol.net