GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

GUARDIA CIVIL
DIRECCIÓN GENERAL

BOLETÍN COOPERA
GUARDIA CIVIL - SEGURIDAD PRIVADA

Número 01/2022

ÍNDICE

ACTUALIDAD

Fraude con medios de pago no presenciales E-SKIMMING

Antecedentes.

Nuestra Unidad Técnica de Policía Judicial nos alerta de la constatación de una tendencia novedosa en el campo del fraude con medios de pago no presenciales: el **e-*skimming***, también conocido como ***skimming* digital** o ***web skimming.***

El despegue del comercio *online* en los últimos años ha provocado de forma paralela el desarrollo y empleo creciente de modalidades de pago digitales (tarjetas de débito o crédito, plataformas tipo "*Bizum"*...etc) en detrimento del dinero físico.

Este aumento en los pagos de forma telemática conforma también una oportunidad para la delincuencia que ha adaptado su metodología. Tradicionalmente la adquisición ilícita de los datos vinculados a medios de pago se ha materializado de forma física, mediante el uso de dispositivos *skimmer o shimmer* situados en los lectores de tarjeta de cajeros automáticos o en terminales de punto de ventas (TPVs) de los establecimientos comerciales con los que los delincuentes "copiaban" los datos asociados a cada medio de pago.

El incremento del comercio digital ha modificado los patrones de pago de los ciudadanos, trasladando la actividad a pasarelas de pago o el abono directo por los servicios/productos en los sitos web de comercio *online*.

Consecuentemente, los ciberdelincuentes han adaptado su actividad a esta situación mediante el desarrollo de metodología *e-skimming*, conocida también como *skimming digital* o *web skimming*, que no deja de ser una técnica de obtención ilícita de credenciales de pago en tiendas online legítimas. En este caso, la diferencia principal con otro tipo de ataques radica en que ahora el punto de compromiso no es el dispositivo del usuario (como por ejemplo mediante la infección de un *smartphone* con un troyano bancario) sino el sitio web o la pasarela de pago a la que accede para introducir las credenciales de pago.

Este modus operandi se basa en la inserción por parte de los ciberdelincuentes de un código malicioso en las propias páginas web a través de las cuales se procesan los pagos de comercio online. De esta manera, cuando la víctima introduce la información de sus credenciales de pago, esta pasa a un servidor controlado por la organización criminal. Tanto el cliente como la tienda online no son conscientes del compromiso de los datos, llegando en muchos casos incluso a confirmarse la transacción de una forma correcta.

Análisis de la problemática.

El número de organizaciones criminales dedicadas a esta tendencia criminal está en claro aumento, detectándose el incremento de entramados criminales con altos conocimientos técnicos que dirigen su actividad a sitios web de comercio online con medidas de seguridad poco robustas. Salvo alguna excepción, el *e-skimming* afecta principalmente a pequeñas y medianas empresas que no tienen la capacidad para implementar una protección suficiente y que, como resultado, ven comprometida su actividad sin ser conscientes de ello. Por ello, a nivel de EUROPOL se considera esta tendencia una de las principales amenazas para el sector de los medios de pago y comercio digital.

Las primeras referencias a esta tipología delictiva datan del año 2015, cuando se orquestó una campaña criminal internacional de ataques bajo la denominación de *Magecart*. Este ataque se dirigió a las tiendas online creadas con el sistema *Magento*, plataforma de código abierto diseñada para el comercio online con un elevado grado de implementación.

Estas campañas tradicionalmente se vienen orientando hacia los datos vinculados a las credenciales de pago, pero se sospecha que pronto puedan derivar su actividad hacia la obtención ilícita de otro tipo de datos confidenciales, como la información relacionada con el inicio de sesión en diferentes sitios web, o aplicaciones más allá del comercio electrónico.

Normalmente estos ataques se dirigen a comercios online cuyas pasarelas de pago están integradas dentro de la propia tienda, es decir, aquellos que no tienen externalizado el proceso con terceros (generalmente con protecciones más sólidas) y que gestionan íntegramente el proceso de pago directamente en sus sistemas.

Normalmente este modus operandi se desarrolla en tres fases claramente diferenciadas:

- La primera se basa en el proceso de infección del sitio web al que la víctima va a acceder.
- La segunda parte es la dirigida a la obtención de credenciales de pago y datos personales de la víctima que accede a la página web comprometida.
- La última fase se encamina a la explotación de los datos obtenidos ilícitamente.

Infección del sitio web y obtención de datos de pago.

El primer paso consiste en obtener acceso al servicio de *hosting* donde está alojada la tienda online. Esta fase es la más compleja por su componente tecnológico y normalmente se emplean técnicas de *hacking*, como la explotación de vulnerabilidades en el sistema de gestión de contenidos (*Content Management System*-CMS) y de *plugins* desactualizados, o mediante inyecciones SQL, combinadas con el empleo de ingeniería social mediante campañas de *phishing*.

Una vez conseguido el acceso ilícito al sitio web, los ciberdelincuentes inyectan código malicioso con funciones de *skimming* en las bibliotecas de *JavaScript* de las páginas de pago de los comerciantes, lo que les permite capturar datos personales y toda la información relacionada con las tarjetas de crédito/débito de los usuarios.

Este código malicioso normalmente verifica las diversas entradas del número de cuenta de pago y del cliente, extrayendo los datos en segundo plano a un servidor de mando y control gestionado por los ciberdelincuentes, de forma que la víctima no es consciente de ello. Finalmente, los datos robados son redireccionados hacia el dominio de los atacantes donde se almacenan y se estructuran para la posterior explotación.

Este ataque se centra normalmente en aquellos sitios web que no tienen una política de seguridad de contenidos robusta y que, por lo tanto, no circunscriban la carga de *JavaScript* a una lista de dominios segura. En caso de tenerla, se bloquearía la ejecución de código malicioso proveniente de dominios controlados por los atacantes. No obstante ya se ha dado algún caso en que los cibercrimnales han logrado eludir esta medida.

Otro objetivo de ataque d*el skimming* digital son los sitios web que no aplican protocolos de integridad de recursos secundarios, es decir, aquellos que en su diseño no evitan la carga de *JavaScript* modificados sin permiso y permiten de esta manera a los ciberdelincuentes ejecutar código malicioso embebido en archivos legítimos.

Otro ejemplo de e-*skimming* es la modalidad de malware conocido como *Pipka*. En la misma línea, este código malicioso permite a los ciberdelincuentes configurar los campos de los que extraer la información, incluidos los números de cuenta de pago, los datos de vencimiento de las tarjetas, los valores de verificación de las tarjetas y el nombre y la dirección del titular de la tarjeta de pago. *Pipka* tiene la característica adicional de poder eliminar su componente *JavaScript* malicioso del código del lenguaje de marcado de hipertexto (HTML) tras una ejecución exitosa. Es un ejemplo de los avances realizados en el campo del *e-skimming* y demuestra que los ciberdelincuentes seguirán desarrollando enfoques innovadores orientados a la obtención ilícita de credenciales de pago.

Explotación de los datos.

Actualmente el mercadeo de datos personales a través de internet es uno de los negocios más rentables, especialmente si estos van relacionados con credenciales de pagos o contraseñas de acceso a la banca *online*.

Tradicionalmente los ciberdelincuentes han explotado directamente los datos robados comprando productos o servicios a través de internet, bien para su disfrute particular, bien a través de una red de "mulas" que revendían estas compras a cambio de una comisión.

Aunque esta conducta sigue en uso, la tendencia actual va orientada a la venta de los datos robados mediante paquetes estructurados. Cada vez son más numerosos los foros dedicados a la compraventa de este producto, denominados foros "*carding",* brindando a los ciberdelincuentes la posibilidad de ofrecer los datos de sus tarjetas de crédito robadas de una manera eficiente y con un riesgo relativamente bajo. Hasta ahora los más prolíficos eran aquellos alojados en la *DarkNet*, pero cada vez son más activos en aplicaciones de mensajería *Over the Top* (OTT), tipo *Telegram* o *Signal*, donde se pueden crear grupos privados con un elevado número de miembros.

Aunque la temática principal de estos canales es la compraventa de estos datos, normalmente se amplía a todo el concepto de la operativa CaaS (*Crime as a Service),* donde los propios desarrolladores de *skimming* digital ponen a disposición de los estafadores soluciones técnicas actualizadas fáciles de usar o manuales de "buenas prácticas"en la materia.

Recomendaciones operativas.

A la vista de lo anterior, pueden adoptarse una serie de medidas que sirvan, no solo para el estudio de su evolución, sino también para facilitar las investigaciones y evitar o, en su defecto minimizar el impacto de esta metodología de fraude:

- Concienciar al sector del comercio *online*, de la posibilidad de ver comprometido su sistema, recomendando:
  - Emplear Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) a la hora de implementar sistemas de pago *online*. Esto incluye el cifrado de los datos de los clientes almacenados, procesados o trasmitidos, así como la solicitud de otros datos que permitan ayudar a confirmar la autenticidad del comprador (como el código CVV de las tarjetas)
  - Habilitar y configurar los dos estándares de seguridad básicos: Tipo CSP (*Content Security Policy*), mediante el cual solo se permite cargar archivos de fuentes previamente autorizadas; Tipo SRI (*Subresource Integrity*), mediante el cual no se permite cargar archivos modificados sin un permiso previo.

- Una alternativa para reducir el riesgo y las consecuencias del *e-skimming* es contratar la pasarela de pago a una entidad de confianza (p.e del sector bancario). Estas pasarelas, generalmente, se encuentran en un entorno seguro controlado por la entidad contratada, por lo que la empresa no tiene que aplicar ninguna media de seguridad sobre la misma, ya que toda la responsabilidad quedará delegada en la entidad contratada.

- Actualizar y parchear todos los sistemas con el software de seguridad a la última versión disponible, especialmente el servidor donde se aloja el contenido. El antivirus debe estar actualizado a la última versión y los firewalls deben ser robustos.

- Separar y segmentar los sistemas de red corporativos para limitar la facilidad con la que los ciberdelincuentes pueden pasar de uno a otro. Aunque esta técnica no reduce directamente el riesgo de sufrir un incidente de seguridad relacionado con el *e-skimming*, minimiza los riesgos de que otras partes de la red se vean afectadas por un incidente que afecte a la tienda.

- Antes de realizar cualquier actualización de *software* en los entornos de producción, es recomendable realizar, previamente, las pruebas en entornos de preproducción, para comprobar que todo funciona correctamente tras la actualización.

- En la medida de lo posible, implementar verificaciones de integridad de código, escaneando el sitio web que procesa el pago en busca de inserciones ilícitas de código malicioso. Supervisar y analizar los *logs* de conexión.

- Cambiar las credenciales predeterminadas y crear contraseñas únicas y robustas en todos los sistemas.

- Limitar en la medida de lo posible cualquier tipo de acceso al sistema en remoto.

- Implementar doble factor de autentificación para el panel de administración de la tienda.

- Aunque el principal vector de riesgo recae en el gestor de pagos, se recomienda al usuario de estos servicios:

  - Tener actualizado a la última versión el sistema operativo, navegadores y antivirus.

  - Instalar complementos en los navegadores que refuercen la seguridad en la navegación, como aquellos diseñados para bloquear la carga de código *Java* en sitios web que no son de confianza.

  - A la hora de efectuar pagos por internet, intentar usar soluciones comerciales que minimicen el riesgo en caso de verse comprometidos los datos vinculados al medio de pago, como las tarjetas monedero con precarga.

  - Confirmar que los sitios web en los que vamos a realizar las compras cumplen unos requisitos básicos de comercio seguro. Para ello deben tener los correspondientes sellos de confianza que aseguren buenas prácticas en protección y privacidad de los consumidores.

2.- La Directora General de la Guardia Civil presenta en Córdoba los Equipos @ de prevención y respuesta en materia de ciberdelincuencia.

La Directora General de la Guardia Civil ha presentado en Córdoba los Equipos @ de asesoramiento, prevención y respuesta en materia de ciberdelincuencia. Ha destacado que actualmente 1 de cada 8 delitos cometidos en demarcación de la Guardia Civil están relacionados con internet.

Se trata de equipos funcionales encargados de reforzar la respuesta en materia de ciberdelincuencia, en particular ante estafas en la red. Asimismo, constituyen el primer nivel de respuesta específica a la cibercriminalidad, apoyando a las unidades territoriales que se encuentran orientadas a la ciudadanía, realizando un primer tratamiento de este tipo de delitos, apoyando a la Policía Judicial específica mediante el análisis de los ciberdelitos, y potenciando la interlocución de calidad con las víctimas.

Se ponen en marcha 84 Equipos @ en toda España formados por más de 300 agentes. Estos Equipos se enmarcan dentro del Plan Estratégico contra la cibercriminalidad del Ministerio del Interior creado para prevenir, proteger y perseguir la cibercriminalidad, y así garantizar la seguridad y la protección de los derechos y libertades de los usuarios en el ciberespacio.

Estos grupos representan el primer nivel de respuesta específica a la cibercriminalidad, apoyando a las unidades territoriales y a Policía Judicial, potenciando una interlocución de calidad con las víctimas.

Se encargarán entre otras cosas de realizar investigaciones básicas relativas a la cibercriminalidad con arreglo a lo recogido al Plan de Actuación de Policía Judicial de cada Comandancia, elevando a los equipos especializados las investigaciones más complejas.

3.- Cambios en la Dirección de Seguridad del Real Madrid Club de Fútbol.

Don Julio Cendal, Policía Nacional, ha sido el Director de Seguridad del Real Madrid Club de Fútbol durante los últimos 24 años; ahora ha alcanzado el momento de su merecida jubilación y por ello este Servicio de Protección y Seguridad (SEPROSE) quiere expresar nuestra más profunda consideración por su infatigable dedicación a este cometido durante estos años.

Igualmente desde esta publicación damos la bienvenida y queremos felicitar por su nombramiento como nuevo Director de Seguridad del Real Madrid C.F a nuestro Coronel D. José Antonio Mellado Valverde, que hasta ahora desempeñaba funciones como Jefe de la División en el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) de la Secretaría de Estado de Seguridad del Ministerio del Interior.

NOTICIAS DE INTERÉS

1.- La Guardia Civil libera más de 260 kilos de pulpos vivos atrapados en “nasas” furtivas en Santoña.

La Guardia Civil, en el marco de la Operación SANTOLAGARRO, ha logrado liberar 265 kilos de pulpos atrapados en nasas furtivas en la costa de Santoña.

Los agentes descubrieron “in fraganti” a un pesquero con 3 tripulantes capturando los ejemplares que por la noche “alaban” líneas de tubos para posteriormente recoger las capturas y volver a dejar las líneas caladas en el fondo. Así, nunca las transportaban sobre el pesquero ni las trasladaban al puerto, por lo que su detección era difícil.

La Guardia Civil había establecido un operativo de seguimiento y localizó al pesquero sospechoso por la noche en el momento que izaba una línea de tubos, siendo sorprendidos los tripulantes del pesquero al realizar el alzado y captura de los ejemplares de pulpo.

Se pudo comprobar que los pescadores para agilizar la extracción del pulpo de los tubos, derramaban por la pieza una disolución de amoniaco, resultando nocivo para el animal.

Durante una semana, mediante instrumentos instalados en los patrulleros Río Nervión y Río Guadalorce, se localizaron y rescataron del fondo del lecho de la bahía un total de 567 “tubos”, además de devolver al mar con vida unos 265 kilos de pulpo.

Los tres infractores se enfrentan a sendas denuncias graves en materia de pesca por marisquear en aguas interiores en horarios no permitidos, por el volumen de las capturas halladas, y por la pesca con arte prohibido no habilitado en el Cantábrico; todo ello en consonancia con la Orden MED 7/2021 de Cantabria por la que se regulan las vedas, tallas mínimas y regida de marisco, con multas de 601 a 60.000€ cada una de ellas. Actualmente continúan las investigaciones.

La pesca indiscriminada del pulpo y la utilización de aparejos ilegales, amenazan la especie y dañan el lecho marino. Por ello se encuentran regulados tanto los métodos adecuados para su captura, la talla mínima del octópodo, el número de piezas permitidas en la pesca, como la documentación exigible, poseer los permisos necesarios, seguros, etc.

La operación SANTOLAGARRO ha sido llevada a cabo por agentes del Seprona y Servicio Marítimo de Bizkaia y Cantabria.

La Guardia Civil desea recordar que debemos proteger el lecho marino, estos denominados “cimientos” del océano sirven de sustento de la vida marina. Si esta cadena trófica o alimentaria se destruye peligra su ecosistema, seamos responsables. Ayúdanos a preservar esta riqueza.

2.- La Guardia Civil desarticula una organización criminal especializada en el robo en entidades bancarias.

La Guardia Civil ha desarrollado la operación COGO logrando detener a 9 personas, 6 de ellos sorprendidos en el momento de intentar robar el contenido de un furgón de seguridad en una entidad bancaria en la capital. Los detenidos son miembros de una organización especializada en el hurto de importantes cantidades de dinero, cheques y documentación de entidades bancarias a la que se le imputan un total de 64 delitos.

Esta operación se inició como consecuencia de varios robos cometidos en entidades bancarias en la provincia de Toledo, destacando un hurto en una entidad bancaria de la localidad de Illescas el pasado día 2 de julio. En este caso, los ahora detenidos sustrajeron 148.000 euros de la caja fuerte cuando se estaba reponiendo dinero en los distintos cajeros automáticos y los autores aprovecharon para acceder al interior y hacerse con esta suma de dinero en efectivo.

Continuando con las investigaciones, los agentes averiguaron la relación de las personas autoras de este hurto con otros que se habían llevado a cabo en distintas sucursales bancarias de la provincia, en localidades como Valmojado, Olías del Rey, Seseña o Toledo capital. En poco tiempo, se esclarecieron nuevos delitos cometidos por este grupo criminal cometidos en las provincias de Albacete, Logroño, Zaragoza, Cantabria, Girona, Barcelona o Madrid, en los que entre todos ellos habrían llegado a sustraer más de medio millón de euros.

Este grupo criminal constaba de numerosas personas que contaban además con numerosas identidades falsas. Alguno de sus integrantes llegaba a acumular hasta 12 identidades falsas diferentes, lo que dificultaba su labor policial para su localización y plena identificación.

3.- La Guardia Civil detiene en Valencia a uno de los mayores estafadores con falsas inversiones en criptomonedas a nivel europeo.

La Guardia Civil, en el marco de la operación “BITDROP”, ha detenido en Valencia a uno de los mayores estafadores con falsas inversiones en criptomonedas a nivel europeo. Se trata de un hombre de 45 años, de nacionalidad portuguesa, al que se le imputa 7 delitos de estafa y blanqueo de capitales.

La operación se inició el pasado mes de agosto, tras tener conocimiento los agentes de los hechos a través de la colaboración con seguridad privada. Se han intervenido 7 vehículos de alta gama, dispositivos electrónicos y diversa documentación. El total del patrimonio bloqueado asciende a más de dos millones y medio de euros.

El detenido había creado una supuesta plataforma de inversiones en criptomonedas en una página web, la cual se daba a conocer a través de diversos foros, programas de radio, eventos deportivos e incluso movimientos benéficos, para así lograr captar la atención y la inversión de numerosas personas en España y Portugal.

La plataforma ofrecía una rentabilidad mínima del 2,5 % semanal a los inversores en función de la cantidad que aportaban, llegando a adquirir roles y así poder atraer a otros inversores.

La estafa se basaba en el método “esquema ponzi” que consiste en un tipo de estafa que trata de inducir a engaño a los perjudicados, quienes se creen que las ganancias obtenidas provienen de una actividad legal, si bien los fondos tienen origen en otros inversores engañados.

De esta manera, la inversión en criptomonedas era todo un éxito, por lo que las víctimas invertían mayores cantidades de dinero y atraían a más inversores. Fruto de las investigaciones de los agentes, se logró identificar a varios perjudicados en España. Además, se descubrió que el detenido había conseguido delinquir en Luxemburgo, Suiza y Portugal. Portugal.

Igualmente, se han bloqueado 13 vehículos e intervenidos otros 7, todos ellos de alta gama.

El total del patrimonio bloqueado, entre vehículos y cuentas bancarias, asciende a más de dos millones y medio de euros.

4.- Convocatoria para Instructor de tiro del personal de seguridad privada.

Resolución de 13 de octubre de 2021, de la Dirección General de la Guardia Civil, por la que se convocan pruebas para la obtención de la habilitación como instructor de tiro del personal de seguridad privada para el año 2022.

Período de presentación de instancias: del 10 al 23 de enero de 2022, ambos inclusive.

https://www.guardiacivil.es/es/servicios/tablonanuncios/instructiro/index.html

5.- Convocatoria para Guardas Rurales y sus especialidades.

Calendario y bases de las convocatorias para el año 2022.

Resolución de 21 de octubre de 2021, de la Secretaría de Estado de Seguridad, por la que se aprueban, para el año 2022, el calendario y las bases de las convocatorias de la pruebas de selección para Guardas Rurales y sus especialidades. Período de presentación de instancias:

Convocatoria 1/2022: del 07 al 20 de marzo de 2022, ambos inclusive.

Convocatoria 2/2022: del 05 al 18 de septiembre de 2022, ambos inclusive.

https://www.guardiacivil.es/es/servicios/tablonanuncios/guacampo/index.html