

Alerta de seguridad informática	8FPH-00052-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2019
Última revisión	05 de Agosto de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios indicando que tienen un reembolso de \$587,58 Dólares en un sistema llamado Latino Tax. Los usuarios que pueden tener curiosidad podrían intentar ingresar al enlace y entregar sus credenciales en un sitio semejante al Sistema Impuesto Interno.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

[https://n3plcpnl0018\[.\]prod\[.\]ams3\[.\]secureserver\[.\]net/~nqyb3oouwge2/impuesto/](https://n3plcpnl0018[.]prod[.]ams3[.]secureserver[.]net/~nqyb3oouwge2/impuesto/)

Smtip Host

relay12.mail[.]gandi[.]net 217.70.178[.]232

From:

hamburg@finominalo[.]site

Subject:

Resultados del estado de reembolso

Imagen Phishing Correo

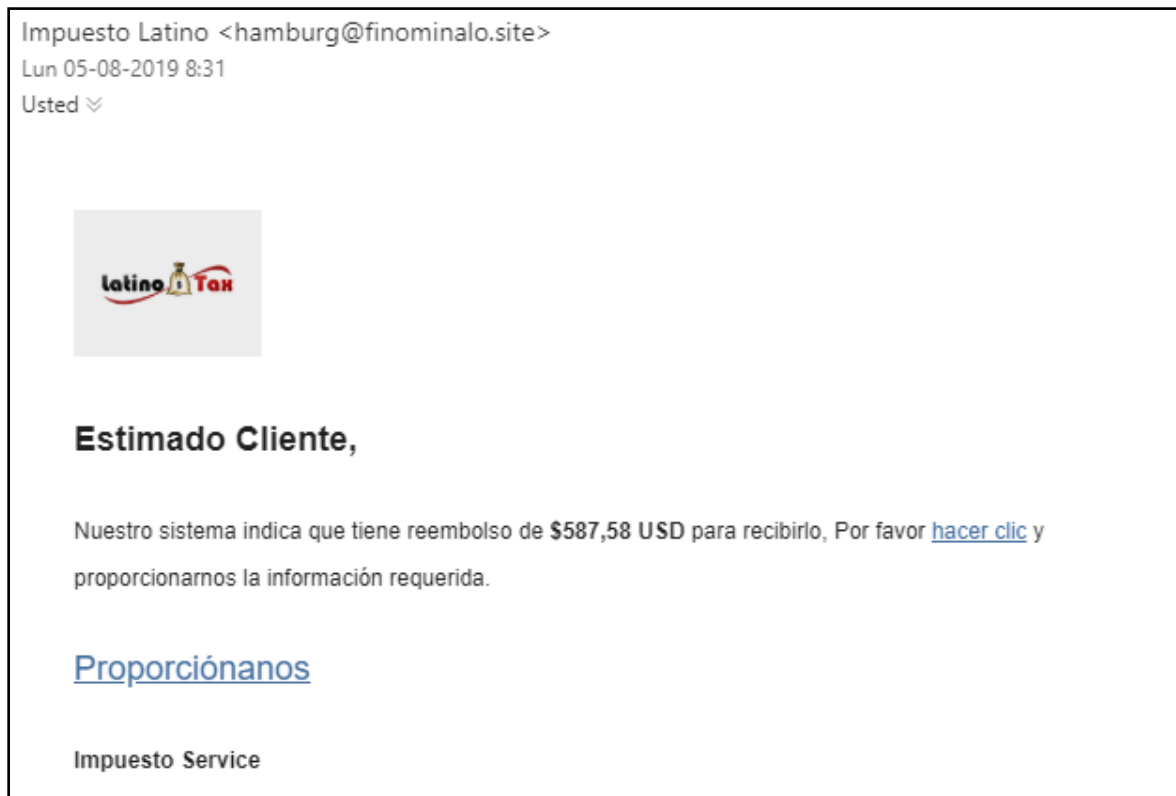



Imagen Sitio Web



The image shows a browser window displaying the login page of the CSIRT website. The browser's address bar shows the URL: <https://n3plcpnl0018.prod.ams3.secureserver.net/~nqyb3oouwge2/impuesto/>. The page has a dark blue header with the text "Ingresar a Mi Sii" in an orange button. Below the header is a navigation menu with links for "Mi Sii", "Servicios online", "Ayuda", and "Contacto". The main content area is titled "Identificación de Contribuyentes" and contains a form with the following fields: "Nombre de pila" (with a dropdown arrow), "Apellido", "Número de identificación nacional", "Código postal", "Número de tarjeta", "Fecha de caducidad" (with a "MM/AA" placeholder), and "CVV". An orange "Ingresar" button is located at the bottom right of the form. The footer is a dark blue bar with five columns of links: "Valores y fechas" (UF, Dólar, UTM-UTA-IPC, Datos y valores de Renta, Datos y valores de IVA, Otros valores), "Normativa y legislación" (Circulares, Resoluciones, Consulta pública de normas, Administrador de contenido normativo, Administrador de Contenido de Jurisprudencia, Legislación tributaria y convenios internacionales, Jurisprudencia y tribunales), "Redes sociales" (Facebook, Twitter, Youtube, RSS, APP's), "Sitios de interés" (Aplicaciones y documentos, Web útiles, Sitios de gobierno relacionados, Organismos relacionados, Intercambios de Información - Estándar CRS), and "Sobre el SII" (Nuestro Servicio, Trabaja con nosotros, Gestión y estadísticas, Términos de uso del sitio web, Recomendaciones de seguridad).

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas
- Visualizar los sitios web que se ingresen que sean los oficiales