PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc

Lima, 23 de julio de 2022

N° 198-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 198	Fecha: 23-07-2022
		Página 04 de 07

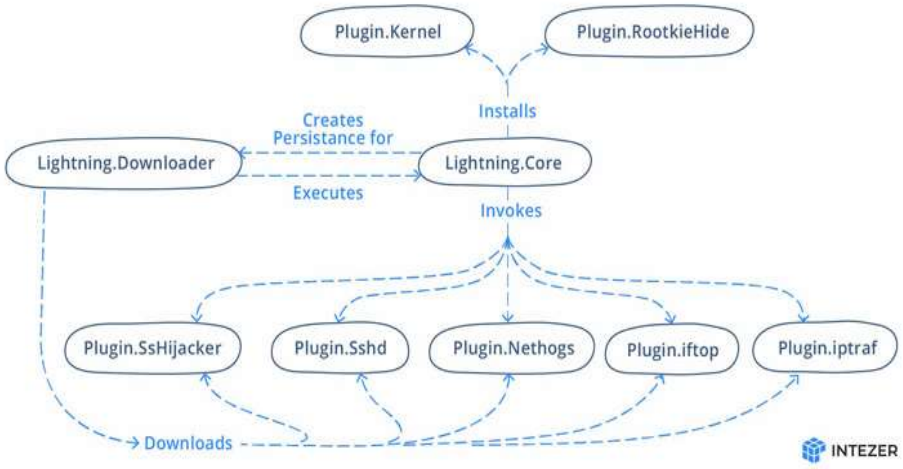
Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Nuevo malware de Linux “Lightning Framework” que se dirige a los sistemas Linux.		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 22 de Julio del 2022, se tomó conocimiento sobre “Lightning Framework”, nuevo malware de Linux similar a “Swiss Army Knife” no detectado que tiene complementos modulares y la capacidad de instalar rootkits.

ANTECEDENTES:

- Esta amenaza de Linux no detectada anteriormente, llamada “Lightning Framework”, está equipada con una gran cantidad de características, lo que la convierte en uno de los malware más complejos desarrollados para atacar los sistemas Linux.
- "El malware tiene capacidades pasivas y activas para la comunicación con el actor de amenazas, incluida la apertura de SSH en una máquina infectada y una configuración de comando y control polimórfica".
- El elemento central del malware es un descargador ("kbioset") y un módulo central ("kkdmflush"), el primero de los cuales está diseñado para recuperar al menos siete complementos diferentes de un servidor remoto que posteriormente son invocados por el componente central.



- Además, el descargador también es responsable de establecer la persistencia del módulo principal del marco. La función principal del módulo de descarga es buscar los otros componentes y ejecutar el módulo central.
- El módulo central, por su parte, establece contacto con el servidor de comando y control (C2) para obtener los comandos necesarios para ejecutar los complementos, al mismo tiempo que se encarga de ocultar su propia presencia en la máquina comprometida.
- Algunos de los comandos notables recibidos del servidor permiten que el malware tome información sensible de la máquina, ejecute comandos de shell, cargue archivos en el servidor C2, escriba datos arbitrarios en el archivo e incluso se actualice y se elimine del host infectado.
- También puede lograr la persistencia mediante la creación de un script llamado “elastisearch” en /etc/rc.d/init.d/ que se ejecuta en cada arranque del sistema para iniciar el módulo de descarga y volver a infectar el dispositivo.

RECOMENDACIONES:

- Mantenga siempre actualizado el sistema operativo y ejecutar análisis antivirus.
- Realice periódicamente copia de seguridad de los datos.

Fuentes de información	▪ https://thehackernews.com/2022/07/new-linux-malware-framework-let.html ▪ https://cyber-reports.com/2022/07/22/new-lightning-framework-linux-malware-installs-rootkits-backdoors/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 198	Fecha: 23-07-2022
		Página 05 de 07

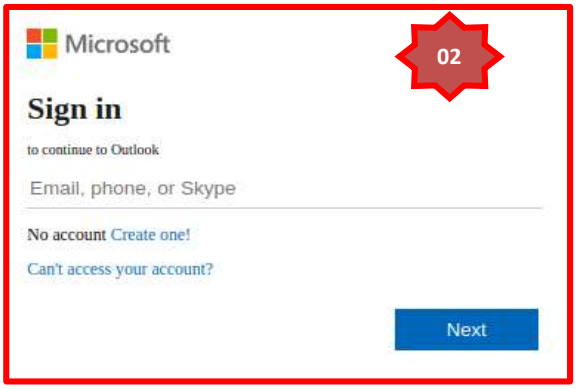
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantación de la identidad de la empresa "Proofpoint", el cual ofrece seguridad al correo electrónico y perdidas de datos de archivos de Microsoft (Correo, Outlook y Office365).		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

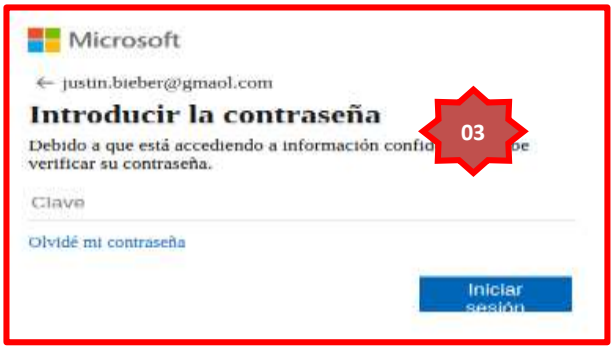
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio de la empresa estadounidense de seguridad empresarial, el cual ofrece un software como servicio y productos para la seguridad del correo electrónico, la prevención de pérdida de datos, el descubrimiento electrónico y el archivo de correo electrónico, con la finalidad de obtener las credenciales de acceso (correos y contraseñas) de los usuarios de la compañía tecnológica Microsoft.

2. ***Detalles del proceso de Phishing***

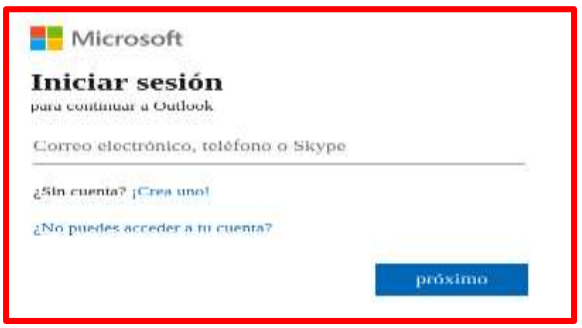
Sitio web falso que suplanta la identidad del servicio de la empresa "Proofpoint", solicita a la víctima, que inicie sesión en cualquier servicio de Microsoft (Correo, Outlook y Office365).



Luego de ingresar a cualquier servicio, le solicita a la víctima, que ingrese la dirección del correo electrónico.

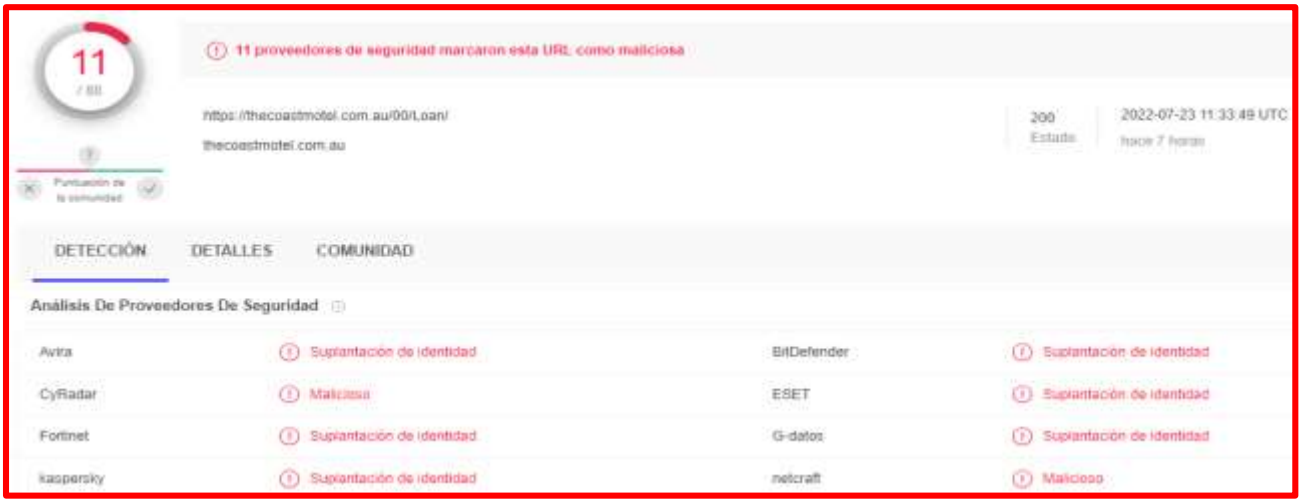


Después de ingresar la dirección de correo electrónico, pide ingresar la clave de acceso, para recién iniciar sesión.



Pasado unos segundos, se visualiza un mensaje donde "Lo sentimos, se ha obtenido problemas para iniciar sesión", aludiendo un aparente error; sin embargo, los datos fueron capturados.

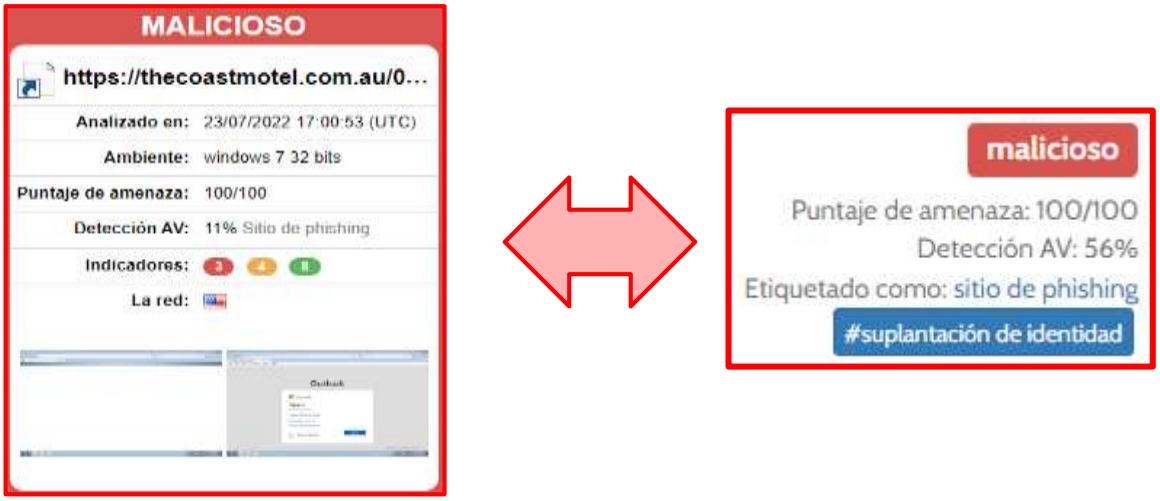
3. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que ONCE (11) proveedores de seguridad informática alertan como ***SUPLANTACIÓN DE IDENTIDAD - PHISHING.***



4. Indicadores de compromiso (IoC)

- URL : hxxps://thecoastmotel[.]com[.]au/00/Loan/
- Dominio : thecoastmotel.com.au
- SHA-256 : 8a476404c3bbbc0e8f34a5f40aa01858d7de712802341b43a6a882a13270d4be
- IP : 52[.]64[.]149[.]50
- Tamaño : 5.94 KB
- Servidor : Apache

5. Otras detecciones:



6. ***Algunas Recomendaciones***:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Realizar las actualizaciones correspondientes desde fuentes originales.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético