Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°142	Fecha: 19-06-2024
		Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La nueva plataforma PhaaS permite a los atacantes eludir la autenticación de dos factores		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

En el pasado, los actores de amenazas han utilizado ampliamente varios kits de campañas de phishing. Un PhaaS (Phishing-as-a-Platform) popular fue Caffeine, que fue identificado e informado por primera vez por investigadores de Mandiant en el 2022.

Sin embargo, ahora se ha descubierto que Caffeine ha sido rebautizado como ONNX Store y se administra de forma independiente, pero el desarrollador original se encarga del soporte al cliente.

2. DETALLES:

Los actores de amenazas están utilizando actualmente esta nueva plataforma para atacar a instituciones financieras a través de correos electrónicos de phishing. Además, la tienda ONNX ofrece una interfaz fácil de usar a la que se puede acceder a través de bots de Telegram.

También tiene la capacidad de eludir los mecanismos 2FA, lo que aumentará la tasa de éxito de los ataques de compromiso del correo electrónico empresarial.

Las páginas de phishing utilizadas en estas campañas se parecen a la página de inicio de sesión original de Microsoft 365 que convencerá a cualquier usuario desprevenido de que ingrese sus credenciales de autenticación.

Si bien Caffeine kit utilizó un único servidor web compartido para administrar todas las campañas de phishing, esta nueva tienda ONNX permite a los actores de amenazas controlar sus operaciones a través de bots de Telegram y el soporte lo brinda un canal de soporte.

Los Servicios ofrecidos incluyen:

- Generación de plantillas de phishing en Microsoft Office 365.
- Servicio de correo web para enviar correos electrónicos de phishing y utilizar señuelos de ingeniería social.
- Servicios de hosting y RDP a prueba de balas para que los ciberdelincuentes gestionen sus operaciones de forma segura.

Esta nueva configuración utiliza Cloudflare para retrasar el proceso de eliminación de dominios de phishing, lo que proporciona funciones como CAPTCHA anti-bot para evadir las detecciones del escáner de sitios web y proxy de IP para ocultar el proveedor de alojamiento original.

Además de su arsenal, este kit de phishing también utiliza un código Javascript cifrado que sólo se descifrará cuando se cargue la página.

Esto evita que los escáneres antiphishing detecten estos dominios de phishing.

Una vez que el código JS se descifra, dominios de terceros como “httbin[.]org” e “ipapi[.]co” recopilan los metadatos de la red de las víctimas, como el nombre del navegador, la dirección IP y la ubicación, antes de enviarlos a la amenaza. actores.

El método de cifrado también oculta scripts maliciosos que siguen los siguientes enfoques:

- La cadena codificada se decodifica desde base64.

- Cada carácter de la cadena decodificada se realiza mediante operación XOR con un carácter de la clave codificada, recorriendo la clave para el descifrado.
- El resultado es una cadena descifrada (código JavaScript), que luego el navegador ejecuta.

Estos scripts maliciosos ocultos no se pueden ver durante una inspección casual. Sin embargo, si se conocen la clave y la cadena cifrada, se puede descifrar fácilmente.

Sin embargo, el código JS descifrado también fue diseñado para robar el token 2FA ingresado por las víctimas.

Además, también se menciona que esta nueva tienda ONNX admite múltiples campañas maliciosas con funciones de alto rendimiento que utilizan velocidades mejoradas de RAM, CPU y SSD y anchos de banda ilimitados.

Indicadores De Compromiso

URL De Phishing:

- authmicronlineonfication[.]com
- verificar-office-outlook[.]com
- flujo-verificar-iniciar sesión[.]com
- zaq[.]gletber[.]com
- v744[.]r9gh2[.]com
- bsifinancial019[.]ssllst[.]nube
- 473[.]kernam[.]com
- docusign[.]multiparteurope[.]com
- 56789iugtfrd5t69i9ei9die9di9eidy7u889[.]rhiltons[.]com
- agchoice[.]us-hindus[.]com

Archivos PDF Maliciosos:

- 432b1b688e21e43d2ccc68e040b3ecac4734b7d1d4356049f9e1297814627cb3
- 47b12127c3d1d2af24f6d230e8e86a7b0c661b4e70ba3b77a9beca4998a491ea
- 51fdaa65511e7c3a8d4d08af59d310a2ad8a18093ca8d3c817147d79a89f44a1
- f99b01620ef174bb48e22e54327ca9cffa4520868f49a41c524b81ab6d935070
- 52e04c615b08af10b4982506c1cee74cb062116d31f0300ed027f6efd3119b1a
- 3d58733b646431a60d39394be99ff083d6db3583796b503e8422baebed8d097e
- 702008cae9a145741e817e6c6566cd1d79c737d51b718f13a2d16d72a00cd5a7
- 908af49857b6f5d1e0384a5e6fc8ee53ca1df077601843ebdd7fc8a4db8bcb12
- d3b03f79cf1d088d2ed41e25c961e9945533aeabb93eac2d33ebc4b589ba6172
- 4751234ac4e1b0a5d4685b870de1ea1a7754258977f5d1d9534631c09c748732

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados, ni descargar adjuntos de correos desconocidos. En su lugar, visitar el sitio web escribiendo la dirección directamente en su navegador.
- Controlar sus cuentas para detectar cualquier actividad inusual y que tomen precauciones para proteger su información personal.
- Practicar una higiene estricta de contraseñas. Utilizar contraseñas únicas para cada tarjeta y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• https://gbhackers.com/phaas-platform-bypass-2fa/