DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 135**	**Fecha: 09-06-2023**
		Página 5 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña "Operación CMDStealer" utiliza scripts LOLBaS y CMD para robar cuentas bancarias en Perú, México y Portugal		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

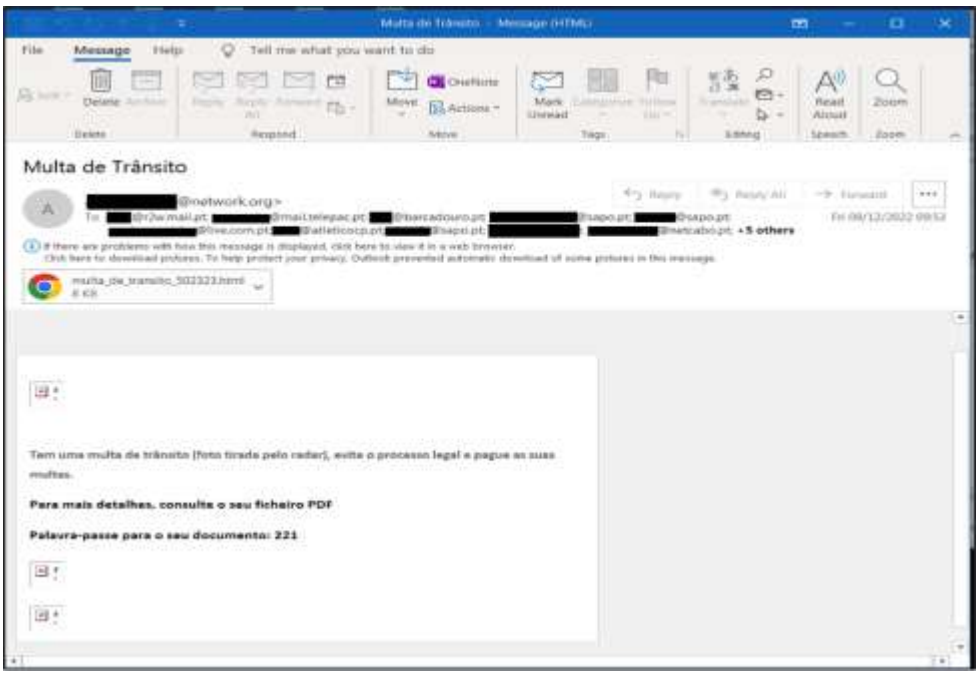
Descripción

1. Resumen:

El Equipo de Investigación e Inteligencia de BlackBerry, ha publicado un informe sobre una nueva campaña denominada "**Operación CMDStealer**", donde señala que un actor de amenaza de origen brasileño, está dirigiendo sus ataques a usuarios de habla hispana y portuguesa (Perú, México y Portugal), empleando tácticas como LOLBaS (Living Off The Land Binaries And Scripts), junto con scripts basados en CMD para llevar a cabo sus actividades maliciosas. Un ataque exitoso podría permitir a un actor de amenazas obtener acceso no autorizado a los sistemas de las víctimas, extraer información confidencial y, en última instancia, comprometer las cuentas bancarias en línea y los sistemas de pago.

2. Detalles:

- Los investigadores de amenazas de BlackBerry indicaron que el actor de amenazas en esta campaña está empleando tácticas como LOLBaS, junto con scripts basados en CMD para llevar a cabo sus ataques. Las víctimas están principalmente en Perú, México y Portugal. Según el análisis de código e idioma, la investigación confía en que el actor de amenaza detrás de esta campaña pertenece a América Latina, específicamente a Brasil.
- En esta campaña, el actor de amenaza utiliza correos electrónicos de phishing en idioma portugués y español, y tácticas de ingeniería social para atacar a las víctimas. Los correos electrónicos explotan problemas comúnmente encontrados, como las infracciones de tránsito y los impuestos, para crear un sentido de urgencia y legitimidad en sus mensajes de phishing. Al hacerse pasar por entidades autorizadas o agencias gubernamentales, los mensajes tienen la intención de engañar a las personas desprevenidas y hacer que revelen sus credenciales bancarias en línea. Los correos electrónicos vienen equipados con un archivo adjunto HTML que contiene código ofuscado para obtener la carga útil de la siguiente etapa de un servidor remoto en forma de un archivo RAR.



Contenido de correo electrónico de phishing

- Los investigadores, indicaron que, en el análisis de las cargas finales, se observó una variedad de técnicas, como el uso de VBE scripts, imágenes ISO y paquetes MSI. En este caso, el actor de amenazas detrás de la campaña utilizó guiones basados en CMD, guiones AutoIt y LOLBaS.
- Los archivos, que están geocercados a un país específico, incluyen un archivo. CMD, que, a su vez, alberga un script AutoIt que está diseñado para descargar un script de Visual Basic para llevar a cabo el robo de Microsoft Outlook y los datos de contraseña del navegador.
- Los scripts basados en LOLBaS y CMD ayudan a los actores de amenazas a evitar la detección mediante medidas de seguridad tradicionales. Los scripts aprovechan las herramientas y comandos integrados de Windows, permitiendo que el actor de la amenaza evada las soluciones de la plataforma de protección a EndPoints (EPP) y sistemas de seguridad. Al utilizar estas técnicas, los actores pueden obtener acceso no autorizado a los sistemas de las víctimas, extraer información confidencial y, en última instancia, comprometer las cuentas bancarias en línea y los sistemas de pago. La información recopilada se transmite de vuelta al servidor del atacante a través de un método de solicitud HTTP POST.
- La infraestructura de phishing y C2 (comando y control) está alojada en servicios con numerosos dominios asociados con una sola dirección, incluidos los servicios de flujo rápido. Dichos servicios contribuyen en gran medida a ofuscar el análisis de tráfico de NetFlow y el seguimiento de la infraestructura. Los dominios utilizados también utilizan en gran medida información redactada “whois” y datos de registro oscuros. Cada etapa de este ladrón utiliza dominios que han redactado información durante años.
- Para llevar a cabo los esquemas, los malos actores utilizaron ataques de phishing para obtener acceso a cuentas de correo electrónico corporativas y engañar a sus socios comerciales para que envíen dinero a cuentas bancarias controladas por delincuentes, una técnica llamada compromiso de correo electrónico comercial.

3. Indicadores de compromiso:

Hash:

- SHA256: f6e84e43323ed9d8531fa2aeeb3c181c8f84fcbe950ce6dcdd8c3fa0b02c6cc0;
- MD5: e64f28174f646e26199d6b7735c84195;
- SHA256: 0a277e51598ef364d5e0006817d32487eb9c0a3c150b7169cbc0bb7348088e63;
- MD5: f7f602f9b7fd04b64fbafe4dbfefa066;
- SHA256: 2d87b9b071ace9f2ebfa33c1c0c21202f39876b312e135a491bf57ba731b798c;
- MD5: fdcc1e1e3ccf30c63660e1f75042be43;
- SHA256: 40017793f40a192b1dfdfc960742dd539b19fee9b15213307c8319fd88eee57f;
- MD5: e212e8d740310cc565bc89c3b7966804;
- SHA256: cb1d1f039c07bd03b6eb14248a897dcefdefc28ae6f523b7c6f549c3c155640b.

4. Recomendaciones:

- La defensa contra las ejecuciones de LOLBaS requiere una estrategia de varias capas. Primero, las organizaciones deben implementar soluciones sólidas de seguridad de punto final para detectar y bloquear comportamientos sospechosos y la ejecución no autorizada de LOLBaS;
- Las organizaciones deben hacer cumplir el principio de menor privilegio, como confianza cero, confirmando que los usuarios solo tienen los permisos necesarios para realizar sus tareas, lo que limita el impacto potencial de la ejecución de LOLBaS;
- Se debe proporcionar capacitación regular en concientización sobre seguridad para educar a los empleados sobre los riesgos asociados con la ingeniería social. El monitoreo continuo y la auditoría de los registros del sistema también pueden ayudar a detectar e investigar cualquier actividad sospechosa relacionada con LOLBaS.

Fuente de Información:	• hxxps://blogs.blackberry.com/en/2023/05/cmdstealer-targets-portugal-peru-and-mexico • hxxps://lolbas-project.github.io/