Un troyano bancario denominado Mispadu se ha vinculado a múltiples campañas de spam, dirigidas a países como Bolivia, Chile, México, Perú y Portugal, con el objetivo de robar credenciales y entregar otras cargas útiles.

La actividad, que comenzó en agosto de 2022, sigue en la actualidad, según Ocelot Team, de la compañía latinoamericana de ciberseguridad, Metabase Q, en un informe compartido con Masterhacks Blog.

Mispadu, también conocido como URSA, fue documentado por primera vez por ESET en noviembre de 2019, describiendo su capacidad para perpetrar robos monetarios y de credenciales, además de actuar como una puerta trasera al tomar capturas de pantalla y pulsaciones de teclas.

> *«Una de sus principales estrategias es comprometer sitios web legítimos, buscar versiones vulnerables de WordPress, convertirlos en su servidor de comando y control para propagar el malware desde allí, filtrar países que no desean infectar, dejar caer distintos tipos de malware basado en el país infectado»*, dijeron los investigadores Fernando García y Dan Regalado.

También se dice que comparte similitudes con otros troyanos bancarios que apuntan a la región, como Grandoreiro, Javali y Lampion. Las cadenas de ataque que involucran el malware Delphi aprovechan los mensajes de correo electrónico que instan a los destinatarios a abrir facturas vencidas falsas, lo que desencadena un proceso de infección de varias etapas.

Si una víctima abre el archivo adjunto HTML enviado por medio del correo electrónico no deseado, verifica que el archivo se abrió desde un dispositivo de escritorio y después se redirige a un servidor remoto para obtener el malware de primera etapa.

El archivo RAR o ZIP, cuando se inicia, está diseñado para hacer uso de certificados digitales falsos, uno que es el malware Mispadu y el otro, un instalador de AutoIT, para decodificar y ejecutar el troyano abusando de la utilidad de línea de comandos certutil legítima.

Mispadu está equipado para recopilar la lista de soluciones antivirus instaladas en el host comprometido, desviar las credenciales de Google Chrome y Microsoft Outlook, y facilitar la recuperación de malware adicional.

Esto incluye cuentagotas ofuscado de Visual Basic Script, que sirve para descargar otra carga útil de un dominio codificado, una herramienta de acceso remoto basada en .NET que puede ejecutar comandos emitidos por un servidor controlado por actor y un cargador escrito en Rust, que a su vez, ejecuta un cargador de PowerShell para ejecutar archivos directamente desde la memoria.

Además, el malware utiliza pantallas superpuestas maliciosas para obtener credenciales asociadas con portales de banca en línea y otra información confidencial.

Metabase Q dijo que el enfoque de certutil permitió a Mispadu eludir la detección de una amplia gama de software de seguridad y recolectar más de 90,000 credenciales de cuentas bancarias de más de 17,500 sitios web únicos.