Se ha descubierto que los actores de amenazas distribuyen un nuevo ladrón de credenciales escrito en lenguaje de scripting AutoHotkey (AHK) como parte de una campaña en curso que comenzó a principios de 2020.

Los clientes de instituciones financieras de Estados Unidos y Canadá se encuentran entre los principales objetivos de la exfiltración de credenciales, con un enfoque específico en bancos como Scotiabank, Royal Bank of Canada, HSBC, Alterna Bank, Capital One, Manulife y EQ Bank. También se incluye en la lista una firma bancaria india ICICI Bank.

AutoHotkey es un lenguaje de secuencias de comandos personalizado de código abierto para Microsoft Windows, destinado a proporcionar teclas de acceso rápido fáciles para la creación de macros y la automatización de software que permite a los usuarios automatizar tareas repetitivas en cualquier aplicación de Windows.

La cadena de infección de varias etapas comienza con un archivo de Excel con software malicioso-atado que se incrusta con un Visual Basic para Aplicaciones (VBA), que se utiliza posteriormente para crear y ejecutar el script de cliente de descarga («adb.ahk») a través de un compilador de script legítimo ejecutable («adb.exe»).

El script del cliente de descarga también es responsable de lograr la persistencia, perfilar a las víctimas y descargar y ejecutar scripts AHK adicionales desde servidores de comando y control (C&C) ubicados en Estados Unidos, Países Bajos y Suecia.

Lo que hace que este malware sea diferente es que en lugar de recibir comandos directamente del servidor C&C, descarga y ejecuta scripts AHK para realizar diferentes tareas.

> *«Al hacer esto, el atacante puede decidir cargar un script específico para lograr tareas personalizadas para cada usuario o grupo de usuarios. Esto también evita que los componentes principales se revelen públicamente, específicamente a otros*

> *investigadores o sandboxes»,* dijeron los investigadores de Trend Micro.

El principal de ellos es un ladrón de credenciales que se dirige a varios navegadores como Google Chrome, Opera, Microsoft Edge, entre otros. Una vez instalado, el ladrón también intenta descargar un módulo SQLite («sqlite3.dll») en la máquina infectada, usándolo para realizar consultas SQL contra las bases de datos SQLite dentro de las carpetas de aplicaciones de los navegadores.

En el paso final, el ladrón recopila y descifra las credenciales de los navegadores y extrae la información al servidor C&C en texto sin formato a través de una solicitud HTTP POST.

Al afirmar que los componentes de malware están *«bien organizados a nivel de código»,* los investigadores sugieren que la inclusión de instrucciones de uso podrían implicar un grupo de *«piratería para contratar»* que está detrás de la creación de la cadena de ataque y lo ofrece a otros como servicio.

> *«Al utilizar un lenguaje de secuencias de comandos que carece de un compilador incorporado dentro del sistema operativo de la víctima, al cargar componentes maliciosos para realizar varias tareas por separado y al cambiar el servicio de C&C con frecuencia, el atacante ha podido ocultar su intención de los entornos sandbox»,* dijeron los investigadores.