Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

BRAZENBAMBOO APT EXPLOTA UNA VULNERABILIDAD CRÍTICA EN FORTICLIENT PARA ROBAR CREDENCIALES DE USUARIOS

18 / 11 / 2024

CONTENIDO

INTRODUCCIÓN

En un reciente descubrimiento de ciberespionaje, el grupo BrazenBamboo, vinculado a actores estatales chinos, ha estado explotando una vulnerabilidad de día cero en el software FortiClient de Fortinet. Esta falla crítica, que afecta incluso a las versiones más recientes del cliente VPN, permite a los atacantes robar credenciales de usuario de manera eficaz, utilizando un framework malicioso altamente sofisticado conocido como DEEPDATA. Este ataque resalta una vez más la creciente amenaza de los grupos APT que, mediante el uso de herramientas avanzadas y técnicas de explotación, buscan comprometer información sensible a gran escala, afectando a organizaciones en todo el mundo.

BRAZENBAMBOO APT EXPLOTA UNA VULNERABILIDAD CRÍTICA EN FORTICLIENT PARA ROBAR CREDENCIALES DE USUARIOS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_11_18_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	18/11/2024
Es día cero (0 day):	SÍ

RESUMEN

Una amenaza sofisticada y persistente

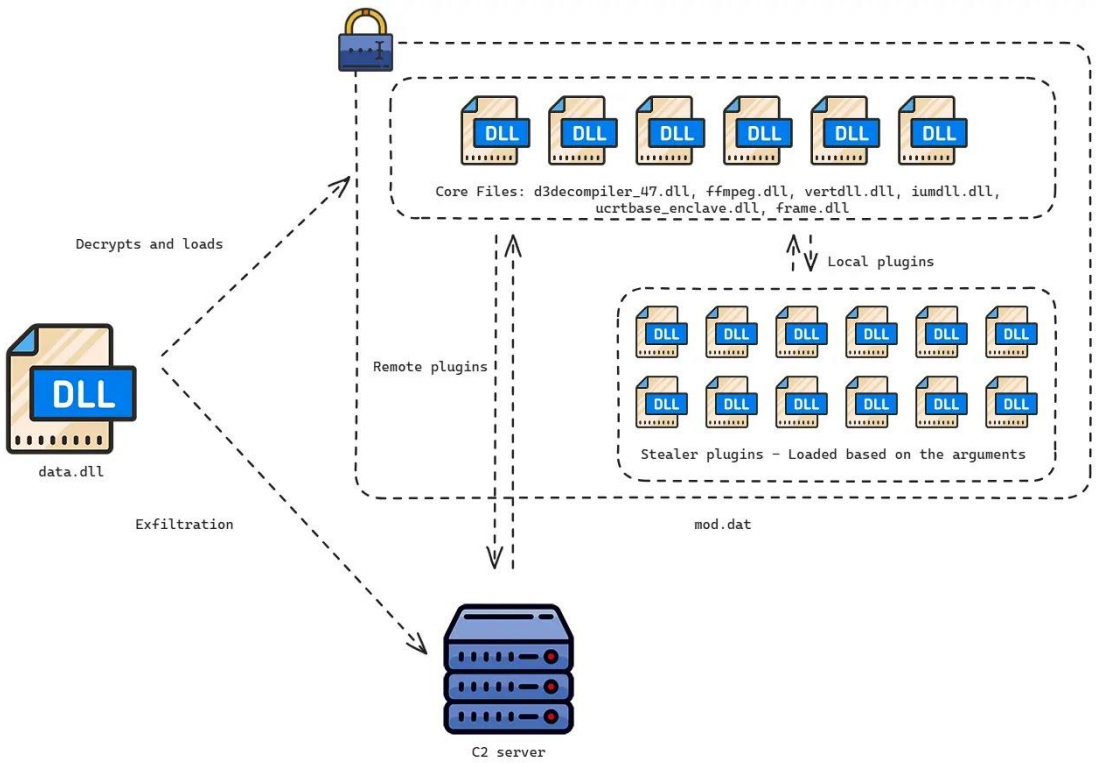
El grupo de cibercriminales conocido como BrazenBamboo ha lanzado una campaña de ciberespionaje altamente avanzada, aprovechando una vulnerabilidad de día cero no parchada en FortiClient, el software de VPN de Fortinet. Este ataque tiene como objetivo robar credenciales de usuarios de empresas y organizaciones que utilizan este software, el cual se encuentra ampliamente distribuido.

Vulnerabilidad en FortiClient

La vulnerabilidad descubierta en julio de 2024 permite a los atacantes extraer credenciales de VPN desde la memoria de los procesos de FortiClient. Este defecto afecta incluso a la versión más reciente del software (v7.4.0) en el momento de su descubrimiento.

El uso de DEEPDATA para la recopilación de información

El grupo BrazenBamboo, vinculado a actores de ciberespionaje respaldados por el Estado chino, utiliza el framework DEEPDATA para llevar a cabo el ataque. Este marco modular incluye un cargador llamado data.dll y varios complementos que permiten recopilar información sensible desde sistemas Windows comprometidos. Entre los complementos, destaca uno llamado msenvico.dll, que es el encargado de extraer información de las sesiones de VPN, tales como nombres de usuario, contraseñas y otros datos relacionados con el acceso remoto.



Funcionalidades avanzadas de DEEPDATA

El malware DEEPDATA no solo se limita al robo de credenciales. Entre sus capacidades, se encuentra la capacidad de recopilar datos de aplicaciones de mensajería, navegadores web, clientes de correo electrónico, e incluso grabar audio, capturar pulsaciones de teclas y exfiltrar archivos de los sistemas infectados. Esta herramienta demuestra la sofisticación y versatilidad de los atacantes, quienes pueden operar en diversos frentes para obtener información crítica.

Infraestructura de C2 altamente organizada

Según análisis, los atacantes han desarrollado una infraestructura avanzada de comando y control (C2), utilizando múltiples servidores para gestionar los payloads de malware y las aplicaciones de administración. A pesar de que esta vulnerabilidad fue reportada a Fortinet en julio de 2024, aún no ha sido resuelta al momento de la publicación de este informe, lo que deja a las organizaciones vulnerables ante un ataque continuo.

Recomendaciones para las organizaciones

Los expertos de ciberseguridad advierten que las organizaciones que utilizan FortiClient deben estar alertas a posibles actualizaciones de seguridad de Fortinet y tomar medidas adicionales para proteger sus credenciales sensibles. Dada la naturaleza avanzada de la amenaza, es crucial implementar controles adicionales de seguridad en las redes corporativas y realizar monitoreos constantes para detectar signos de actividad sospechosa.

Conclusión

Este ataque subraya la persistente amenaza que representan los grupos APT bien financiados y organizados, como BrazenBamboo. La explotación de vulnerabilidades de día cero en software ampliamente utilizado resalta la importancia de la actualización constante de software y de mantener una postura de seguridad proactiva. Las empresas deben prepararse para enfrentar a estos actores maliciosos, quienes continúan evolucionando y perfeccionando sus técnicas para burlar las defensas tradicionales.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20241118_BrazenBamboo

NOTICIA COMPLETA

https://devel.group/blog/brazenbamboo-apt-explota-una-vulnerabilidad-critica-en-forticlient-para-robar-credenciales-de-usuarios/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group