Un grupo de amenazas persistentes avanzadas (APT) conocido como Void Banshee ha sido observado explotando una vulnerabilidad de seguridad recientemente divulgada en el motor del navegador Microsoft MHTML como un zero-day para entregar un ladrón de información llamado Atlantida.

La firma de ciberseguridad Trend Micro, que detectó la actividad a mediados de mayo de 2024, indicó que la vulnerabilidad – identificada como CVE-2024-38112 – se utilizó como parte de una cadena de ataque en múltiples etapas que emplea archivos de acceso directo de internet (URL) especialmente diseñados.

> *«Variantes de la campaña Atlantida han estado muy activas durante 2024 y han evolucionado para usar CVE-2024-38112 como parte de las cadenas de infección de Void Banshee. La capacidad de grupos APT como Void Banshee para explotar servicios deshabilitados como [Internet Explorer] representa una amenaza significativa para las organizaciones a nivel mundial»*, dijeron los investigadores de seguridad Peter Girnus y Aliakbar Zahravi.

Estos hallazgos coinciden con divulgaciones previas de Check Point sobre una campaña que aprovecha la misma vulnerabilidad para distribuir el ladrón de información. Cabe destacar que Microsoft abordó CVE-2024-38112 como parte de las actualizaciones de Patch Tuesday la semana pasada.

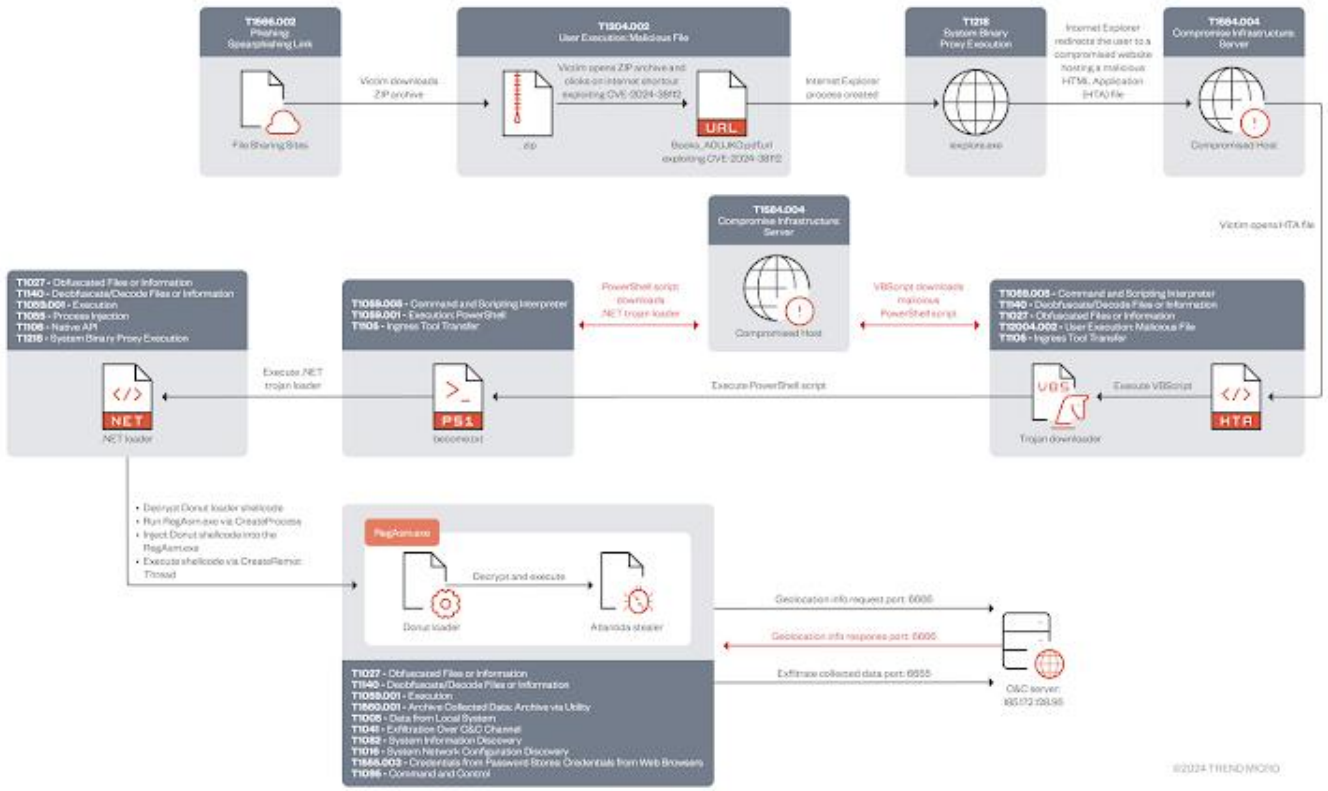
CVE-2024-38112 ha sido descrito por Microsoft como una vulnerabilidad de suplantación en el motor del navegador MSHTML (también conocido como Trident) utilizado en el ahora descontinuado Internet Explorer. Sin embargo, la Iniciativa de Día Cero (ZDI) ha afirmado que se trata de una falla de ejecución de código remoto.

> *«¿Qué sucede cuando el proveedor dice que la solución debería ser una actualización de defensa en profundidad en lugar de un CVE completo? ¿Qué sucede cuando el proveedor dice que el impacto es suplantación, pero el error*

> *resulta en ejecución de código remoto?»*, señaló Dustin Childs de ZDI.

Las cadenas de ataque implican el uso de correos electrónicos de spear-phishing que contienen enlaces a archivos ZIP alojados en sitios de intercambio de archivos, que contienen archivos URL que explotan CVE-2024-38112 para redirigir a la víctima a un sitio comprometido que aloja una aplicación HTML maliciosa (HTA).

Abrir el archivo HTA provoca la ejecución de un script de Visual Basic (VBS) que, a su vez, descarga y ejecuta un script de PowerShell responsable de recuperar un cargador troyano .NET, que finalmente utiliza el proyecto de shellcode Donut para descifrar y ejecutar el ladrón de información Atlantida dentro de la memoria del proceso RegAsm.exe.



Atlantida, basado en ladrones de información de código abierto como NecroStealer y PredatorTheStealer, está diseñado para extraer archivos, capturas de pantalla, geolocalización y datos sensibles de navegadores web y otras aplicaciones, incluyendo Telegram, Steam, FileZilla y varias billeteras de criptomonedas.

> *«Al usar archivos URL especialmente diseñados que contenían el manejador de protocolo MHTML y la directiva x-usc!, Void Banshee pudo acceder y ejecutar archivos de aplicación HTML (HTA) directamente a través del proceso de IE deshabilitado,»* dijeron los investigadores.
>
> *«Este método de explotación es similar a CVE-2021-40444, otra vulnerabilidad de MSHTML que se utilizó en ataques de día cero.»*

No se sabe mucho sobre Void Banshee aparte del hecho de que tiene un historial de atacar regiones de América del Norte, Europa y el sudeste asiático para el robo de información y el beneficio financiero.

Este desarrollo se produce cuando Cloudflare reveló que los actores de amenazas están incorporando rápidamente exploits de prueba de concepto (PoC) en su arsenal, a veces tan rápido como 22 minutos después de su publicación, como se observó en el caso de CVE-2024-27198.

> *«La velocidad de explotación de CVEs divulgadas es a menudo más rápida que la velocidad a la que los humanos pueden crear reglas WAF o crear y desplegar parches para mitigar ataques,»* dijo la empresa de infraestructura web.

También sigue al descubrimiento de una nueva campaña que aprovecha los anuncios de Facebook que promueven temas falsos de Windows para distribuir otro ladrón de información

conocido como SYS01stealer, que apunta a secuestrar cuentas comerciales de Facebook y propagar aún más el malware.

> *«Siendo un ladrón de información, SYS01 se enfoca en exfiltrar datos del navegador como credenciales, historial y cookies. Una gran parte de su carga útil se centra en obtener tokens de acceso para cuentas de Facebook, específicamente aquellas con cuentas comerciales de Facebook, lo que puede ayudar a los actores de amenazas a propagar el malware»*, dijo Trustwave.