| | | |
|---|---|---|
| | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 112** | **Fecha: 13-05-2023** |
| | | **Página 8 de 18** |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ** | | |
| Nombre de la alerta | Hackean cuentas de correo electrónico de Outlook con solo un archivo de música .wav | | |
| Tipo de ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Red, Internet | | |
| Código de familia | H | Código de subfamilia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

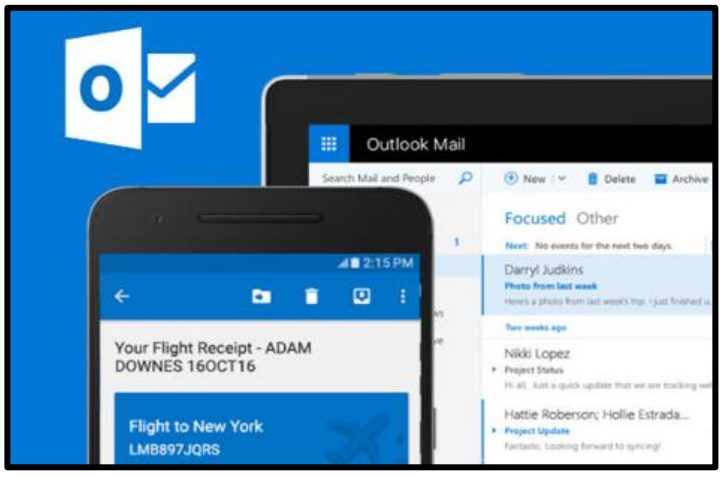
**ANTECEDENTES:**

El 11 de mayo del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se descubrió que, Microsoft emitió un parche actualizado para abordar una vulnerabilidad que se había solucionado previamente en marzo, pero que posteriormente los investigadores de la comunidad de seguridad descubrieron que era ineficaz.

**DETALLES:**

Barnea, investigador de Akamai, encontró un método en torno a la falla que se había solucionado en marzo. De esta manera, un atacante podría aprovechar la vulnerabilidad para obligar a un cliente de Outlook a conectarse a un servidor que estaba controlado por el atacante. Aunque el problema se solucionó en marzo, el investigador encontró una forma de evitar el parche.

Barnea dijo que el problema es una vulnerabilidad de clic cero, lo que significa que se puede activar sin necesidad de interacción por parte del usuario, y que todas las versiones de Windows son vulnerables a ella. Barnea elaboró diciendo que el parche original no tenía sentido por la introducción de un solo personaje nuevo. Sin embargo, él y el equipo de seguridad de Akamai no estuvieron de acuerdo con la forma en que Microsoft categorizó el problema, al que se le asignó una puntuación CVSS de solo 6,5. Lo encontraron cuando estaban analizando el parche para CVE-2023-23397, que solucionó el problema cambiando el flujo de código en Outlook para que ahora verifique si la ruta de la convención de nomenclatura universal (UNC) que recupera el archivo de sonido personalizado hace referencia a una URL de Internet y, si lo hace, utiliza el sonido de recordatorio predeterminado en lugar del personalizado.




**RECOMENDACIONES:**

- Instalar las actualizaciones de seguridad de Microsoft que están disponibles incluyendo las fallas de día cero que se están explotando activamente en ataques.
- Asegurarse que todos los sistemas de su organización estén actualizados. Esto incluye sistemas operativos, aplicaciones y software de seguridad.
- Tener actualizado el Windows defender y un antivirus adicional.

| | |
|---|---|
| Fuentes de información | ▪ hxxps://www.securitynewspaper.com/2023/05/11/hack-into-outlook-email-accounts-with-just-a-music-wav-file/ |

| | | |
|---|---|---|
| DINI | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 112** | **Fecha: 13-05-2023**<br>**Página 12 de 18** |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN NACIONAL DE INTELIGENCIA** | | |
| Nombre de la alerta | Nueva variante de malware de tipo backdoor “BPFDOOR” para Linux | | |
| Tipo de ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Red, Internet | | |
| Código de familia | H | Código de subfamilia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

1. **Resumen:**

Investigadores de la firma de ciberseguridad Deep Instinct, han detectado una nueva variante previamente no documentada y en su mayoría no detectada de una puerta trasera (backdoor) de Linux denominada “BPFdoor”. El malware es extremadamente sigiloso y difícil de detectar, está diseñado específicamente para establecer un acceso remoto persistente a entornos de destino comprometidos durante largos períodos de tiempo. Los actores de amenazas pueden penetrar en el sistema de una víctima y ejecutar código arbitrario sin ser detectados por los firewalls, al mismo tiempo que filtran datos innecesarios.

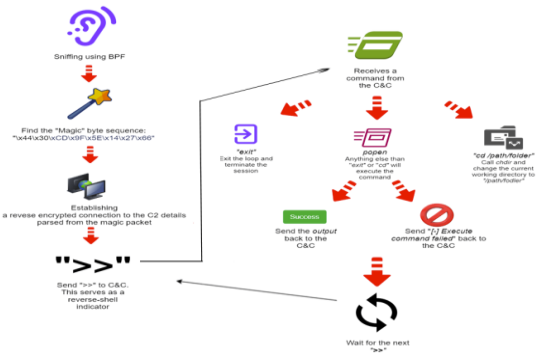
2. **Detalles:**

- BPFdoor es una puerta trasera pasiva, de bajo perfil y específica de Linux que tiene la intención de mantener un punto de apoyo persistente a largo plazo en redes y entornos ya violados y funciona principalmente para garantizar que un atacante pueda volver a ingresar a un sistema infectado durante un período prolongado de tiempo, post-compromiso. BPFdoor conserva su reputación como un malware extremadamente sigiloso y difícil de detectar con esta última iteración.

- El malware está asociado con un actor de amenazas chino, Red Menshen (también conocido como Red Dev 18), que se ha observado apuntando a proveedores de telecomunicaciones en Medio Oriente y Asia, así como a entidades en los sectores de gobierno, educación y logística desde 2021.

- Una de las diferencias más significativas en comparación con la variante anterior de BPFdoor radica en la eliminación de muchos de sus indicadores codificados, lo que hace que la versión más nueva sea más difícil de detectar. Desde que se vio por primera vez en VirusTotal en febrero de 2023, la nueva variante no se detectó y sigue sin detectarse.

- El malware BPFDoor recibe su nombre del uso de Berkeley Packet Filters (BPF), una tecnología que permite analizar y filtrar el tráfico de red en sistemas Linux, para comunicaciones de red y procesar comandos entrantes. El malware está diseñado para establecer un acceso remoto persistente a entornos de destino comprometidos durante largos períodos de tiempo. Al hacerlo, los actores de amenazas pueden penetrar en el sistema de una víctima y ejecutar código arbitrario sin ser detectados por los firewalls, al mismo tiempo que filtran datos innecesarios. Los hallazgos de Deep Instinct provienen de un artefacto BPFDoor que se cargó en VirusTotal el 8 de febrero de 2023. Al momento de escribir, solo tres proveedores de seguridad han marcado el binario ELF como malicioso.



- Una de las características clave que hace que la nueva versión de BPFDoor sea aún más evasiva es la eliminación de muchos indicadores codificados y, en su lugar, incorpora una biblioteca estática para el cifrado (libtomcrypt) y un shell inverso para la comunicación de Comando y Control (C2).

- BPFDoor está configurado para ignorar varias señales del sistema operativo para evitar que se cierre. Luego asigna un búfer de memoria y crea un socket especial de detección de paquetes que monitorea el tráfico entrante con una secuencia específica de Magic Byte conectando un filtro BPF al socket sin formato.

- Los investigadores indicaron que "Cuando BPFdoor encuentra un paquete que contiene sus Magic Bytes en el tráfico filtrado, lo tratará como un mensaje de su operador y analizará dos campos y se bifurcará nuevamente. El proceso principal continuará y monitoreará el tráfico filtrado que ingresa a través del socket, mientras que el proceso secundario tratará los campos analizados previamente como una combinación de puerto IP de comando y control e intentará contactarlo".

- En la etapa final, el backdoor "BPFDoor" configura una sesión de shell inversa cifrada con el servidor C2 y espera que se ejecuten más instrucciones en la máquina comprometida.

**3. Indicadores de Compromiso (IoC):**

- afa8a32ec29a31f152ba20a30eb483520fe50f2dce6c9aa9135d88f7c9c511d7 – BPFDoor ELF SHA256
- /var/run/initd.lock – BPFDoor "mutex".

**MITRE ATT&CK:**

| Táctica | Técnica | Descripción | Observable |
|---|---|---|---|
| Mando y Control Defensa Evasión Persistencia | T1205 - Señalización de tráfico | El atacante emplea valores "mágicos" para desencadenar la respuesta. | Secuencia de bytes "mágica" |
| Mando y Control Defensa Evasión Persistencia | T1205.002 - Señalización de Tráfico: Filtros de Toma | El atacante conecta el filtro a un socket de red. | Uso del filtro de paquetes de Berkley |
| Comando y control | T1573 - Canal encriptado | El atacante emplea comunicación encriptada de Comando y Control. | Uso de libtomcrypt |
| Ejecución | T1106: API nativa | El atacante recurre a las API nativas del sistema operativo para ejecutar comportamientos. | uso de papa |

**4. Recomendaciones:**

- Monitorear el sistema de seguridad en tiempo real;
- Utilizar un software antivirus sofisticado que ayude a detectar y prevenir una amplia variedad de amenazas, incluido malware, backdoor, spyware, troyanos y piratas informáticos criptográficos;
- Cambiar las contraseñas regularmente (no usar contraseñas por defecto);
- Utilizar un firewall o cortafuegos para la protección contra malware de tipo backdoor, ya que monitorean todo el tráfico que entra y sale en su red;
- No realizar descargas de sitios web no confiables o de dudosa reputación;
- Concientizar al personal sobre las nuevas amenazas existentes en el entorno digital.

| | |
|---|---|
| Fuentes de información | ▪ hxxps://www.deepinstinct.com/blog/bpfdoor-malware-evolves-stealthy-sniffing-backdoor-ups-its-game<br>▪ hxxps://www.crowdstrike.com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/<br>▪ hxxps://www.elastic.co/security-labs/a-peek-behind-the-bpfdoor |