| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°214 | Fecha: 11-09-2023 |
|---|---|---|
| | | Página: 9 de 32 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ** | | |
| Nombre de la alerta | APT34 ha sido vinculado a un nuevo ataque de phishing | | |
| Tipo de Ataque | Phishing | Abreviatura | Phishing |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | |
| Código de familia | G | Código de Sub familia | G01 |
| Clasificación temática familia | Fraude | | |

Descripción

1. **ANTECEDENTES:**

   El 09 de agosto del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha tomado conocimiento que APT34 ha sido vinculado a un nuevo ataque de phishing que conduce al despliegue de una variante de una puerta trasera llamada SideTwist.

2. **DETALLES:**

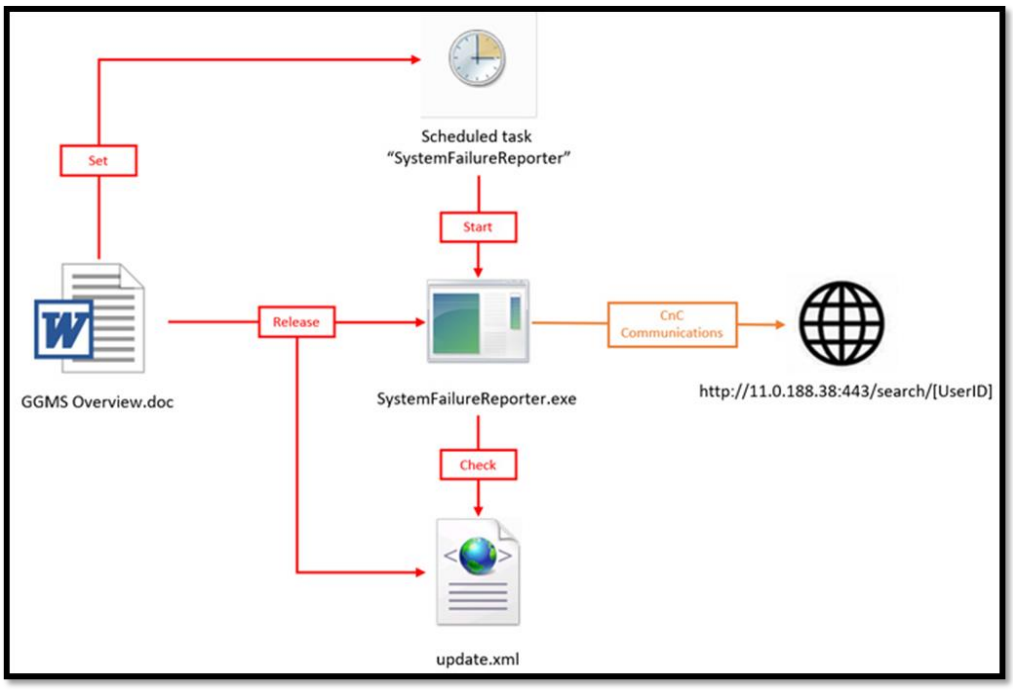
   APT34 tiene un alto nivel de tecnología de ataque, puede diseñar diferentes métodos de intrusión para diferentes tipos de objetivos y tiene capacidad de ataque a la cadena de suministro, tiene un historial de apuntar a sectores verticales de telecomunicaciones, gobierno, defensa, petróleo y servicios financieros.

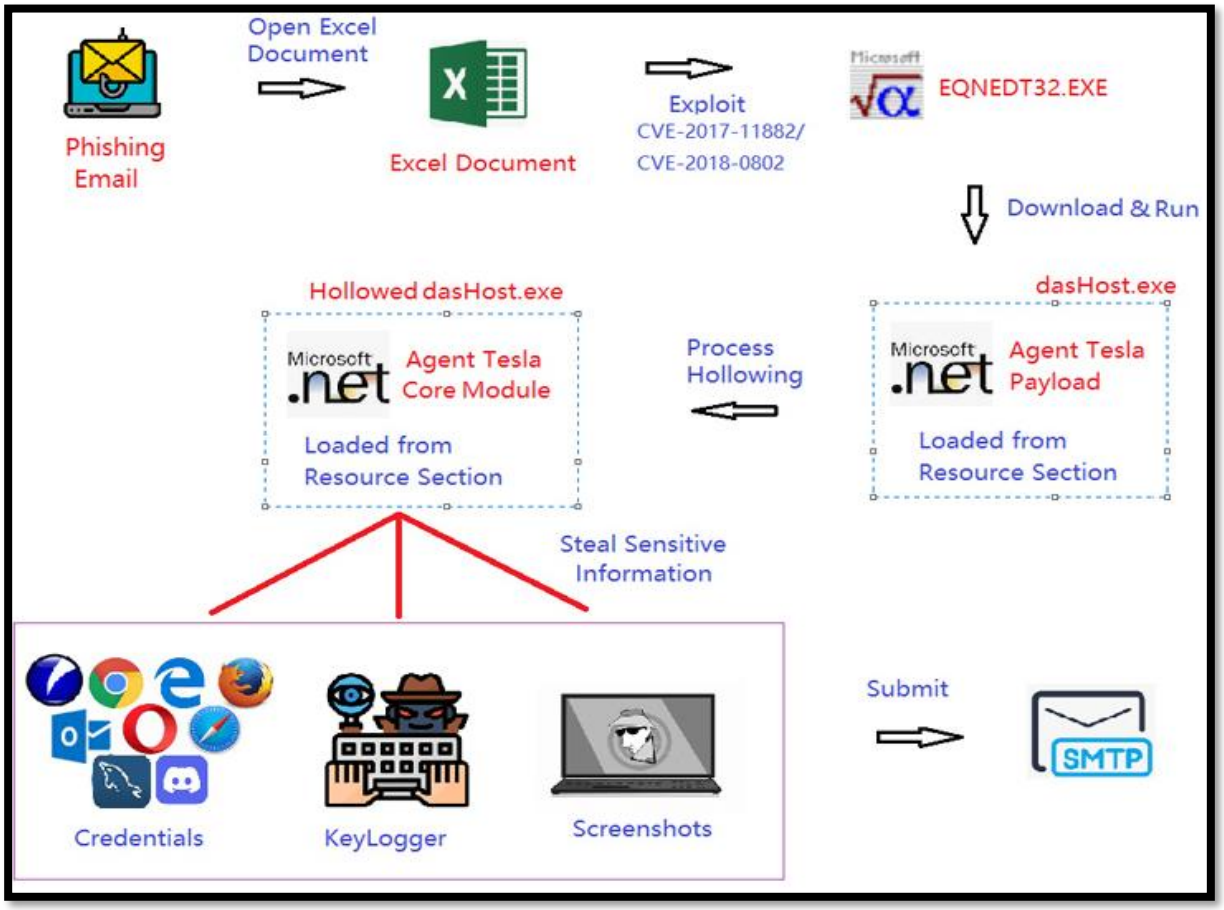
   Una de las características clave del equipo de piratería es su capacidad para crear herramientas nuevas y actualizadas para minimizar las probabilidades de detección y afianzarse en los hosts comprometidos durante largos períodos de tiempo.

   La cadena de ataque identificada por NSFOCUS comienza con un documento cebo de Microsoft Word que se incrusta dentro de una macro maliciosa que, a su vez, extrae y lanza la carga útil codificada en Base64 almacenada en el archivo.

   CVE-2017-11882 sigue siendo una de las fallas más favorecidas hasta la fecha, explotada por "467 malware, 53 actores de amenazas y 14 ransomware" y tan recientemente como el 31 de agosto de 2023.

   También sigue al descubrimiento de otro ataque de phishing que emplea señuelos de archivos de imágenes ISO para lanzar cepas de malware como Agent Tesla, LimeRAT y Remcos RAT en hosts infectados.






**3. RECOMENDACIONES:**

- Mantener tus sistemas actualizados.
- Asegurarse de que todos los sistemas operativos, aplicaciones y software del dispositivo estén actualizados con las últimas versiones y parches de seguridad.
- Mantener actualizado el antivirus.
- Evitar la descarga ni abra archivos de fuentes no confiables.

| | |
|---|---|
| Fuente de Información: | • hxxps://thehackernews.com/2023/09/alert-phishing-campaigns-deliver-new.html |