| | | |
|---|---|---|
| DINI | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 138** | **Fecha: 13-06-2023**<br>**Página 26 de 32** |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN NACIONAL DE INTELIGENCIA** | | |
| Nombre de la alerta | Nueva campaña de ciberespionaje y cibercrimen por el grupo "Asila Ambuscade" dirigido a entidades públicas y privadas en todo el mundo | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Red, Internet | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

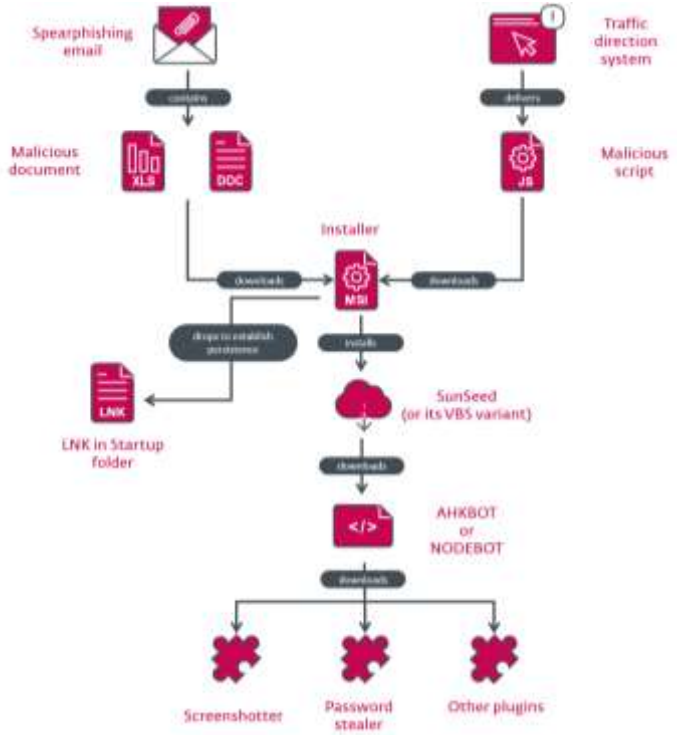
**1. Resumen:**

Investigadores de ESET, han publicado un informe sobre una nueva campaña de ciberespionaje y cibercrimen por parte del grupo "Asylum Ambuscade" desde al menos 2020 y dirigido a funcionarios gubernamentales y empleados de empresas estatales en Asia, África, Europa y América del Sur. Un ataque exitoso podría permitir a un actor de amenaza robar información confidencial y credenciales de correo web de los portales de correo web oficiales del gobierno o de una potencial víctima.

**2. Detalles:**

- "Asylum Ambuscade" es un grupo de ciberdelincuencia que ha estado realizando operaciones de ciberespionaje de forma paralela. Fueron expuestos públicamente por primera vez en marzo de 2022 por investigadores de Proofpoint después de que el grupo se dirigiera al personal del gobierno europeo involucrado en ayudar a los refugiados ucranianos, solo unas semanas después del comienzo de la guerra entre Rusia y Ucrania.
- Los investigadores indicaron que el grupo "Asylum Ambuscade" participó principalmente en campañas de delitos cibernéticos durante los últimos tres años, con más de 4500 víctimas identificadas en todo el mundo, incluidos comerciantes de criptomonedas, pequeñas y medianas empresas (PYMES) e individuos. La mayoría de las víctimas del actor de amenazas se encuentran en América del Norte, pero ESET también identificó entidades comprometidas en Asia, África, Europa y América del Sur.
- En esta campaña, La cadena de compromiso comienza con un correo electrónico de spearphishing que tiene un archivo adjunto de hoja de cálculo de Excel malicioso. El código VBA malicioso que contiene descarga un paquete MSI desde un servidor remoto e instala **SunSeed**, un descargador escrito en Lua. Los investigadores indicaron que observaron algunas variaciones en los archivos adjuntos. En la campaña de junio de 2022, el grupo utilizó un exploit de la vulnerabilidad de Follina (CVE-2022-30190) en lugar de un código VBA malicioso.
- Luego, si la máquina es de su interés, los atacantes implementan la siguiente etapa del ataque: AHKBOT. Este es un programa de descarga escrito en AutoHotkey que se puede ampliar con complementos, también escritos en AutoHotkey, para espiar la máquina de la víctima.
- La cadena de compromiso del software criminal de Asylum Ambuscade es, en general, muy similar a la que se descubrió para las campañas de ciberespionaje. La principal diferencia es el vector de compromiso, que puede ser:
  - Un anuncio de Google malicioso que redirige a un sitio web que entrega un archivo JavaScript malicioso (como se destaca en la publicación de blog de SANS)
  - Múltiples redirecciones HTTP en un Sistema de dirección de tráfico (TDS). El TDS utilizado por el grupo se denomina 404 TDS por Proofpoint. No es exclusivo de Asylum Ambuscade y se observó que, por ejemplo, fue utilizado por otro actor de amenazas para entregar Qbot.
- Para evadir la detección de los productos de seguridad, el actor de amenazas utiliza diferentes variantes del descargador **SunSeed**, que se escribieron en Lua, Tcl y VBS (Visual Basic), y del descargador de segunda etapa AHKBOT, escrito en AutoHotkey o Node.js (llamado Nodebot).
- Los investigadores de ESET, indicaron que las campañas de ciberespionaje y cibercrimen son operadas por el mismo grupo, ya que las cadenas de compromiso son casi idénticas en todas las campañas. En particular, SunSeed y AHKBOT se han utilizado ampliamente tanto para la ciberdelincuencia como para el ciberespionaje.

- Por otro lado, indicaron, que no creían que las herramientas SunSeed y AHKBOT se vendan en el mercado clandestino. Estas herramientas no son muy sofisticadas en comparación con otras herramientas de crimeware a la venta, la cantidad de víctimas es bastante baja si se trata de un conjunto de herramientas compartido entre varios grupos y la infraestructura de red es uniforme en todas las campañas.




Cadena de compromiso

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

- SHA-1: 2B42FD41A1C8AC12221857DD2DF93164A71B95D7;
- SHA-1: D5F8ACAD643EE8E1D33D184DAEA0C8EA8E7FD6F8;
- SHA-1: 57157C5D3C1BB3EB3E86B24B1F4240C867A5E94F;
- IP: 5.39.222[.]150, 5.44.42[.]27, 5.230.68[.]137;
- Ver lista completa de IoC y Técnicas MITRE ATT&CK utilizados por el atacante en esta campaña aquí.

**4. Recomendaciones:**

- La educación y la concienciación son fundamentales para prevenir ataques de phishing. Es importante que los usuarios estén informados sobre los riesgos y las técnicas utilizadas por los hackers para engañarlos;
- Antes de hacer clic en un enlace o descargar un archivo adjunto, es importante verificar la dirección de correo electrónico del remitente y la dirección web a la que se dirige el enlace;
- Contar con un buen antivirus y software de seguridad en el equipo puede ayudar a prevenir la descarga de malware y a detectar intentos de phishing;
- Mantener actualizado el software del equipo y de los navegadores web puede ayudar a prevenir ataques de phishing que explotan vulnerabilidades conocidas;
- Utilizar contraseñas seguras y cambiarlas con regularidad puede ayudar a prevenir el acceso no autorizado a cuentas personales y confidenciales.

| | |
|---|---|
| Fuentes de información | • hxxps://www.welivesecurity.com/2023/06/08/asylum-ambuscade-crimeware-or-cyberespionage/<br>• hxxps://www.trendmicro.com/en_us/research/20/l/stealth-credential-stealer-targets-us-canadian-bank-customers.html<br>• hxxps://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me |