Advertencia de Seguridad

Campaña de Malware Activa: Infostealer.Win32.Tinba.FEC3

COLCERT AD-0810-022

TLP:CLEAR

¿Qué es Infostealer.Win32.Tinba.FEC3?

Se trata de un malware de tipo infostealer, diseñado para robar información sensible como credenciales, datos almacenados y actividad en el sistema. Su capacidad para evadir los mecanismos de seguridad tradicionales lo convierte en una amenaza crítica para cualquier infraestructura.

Capacidades del Malware:

Software malicioso diseñado específicamente para robar información sensible de los sistemas infectados. Su principal objetivo es capturar y exfiltrar datos confidenciales del usuario o de la organización, como:

- **Credenciales de acceso:** nombres de usuario y contraseñas.
- **Información financiera:** números de tarjetas de crédito, cuentas bancarias.
- **Historial de navegación:** cookies, datos de formularios guardados, y más.
- **Archivos sensibles:** documentos y otros archivos que puedan ser de valor.

Detalles de la Amenaza:

- **Nombre del archivo:** PROCESO No 2010-00367-00 SEPTIEMBRE 19 DE 2024.exe
- **Clasificación:** Infostealer.Win32.Tinba.FEC3
- **Tamaño:** 3.07 MB
- **Impacto:** Alto
- **Credibilidad y Confianza:** A1

Acciones Observadas:

1. **Modificación del registro:** Cambia claves de inicio en Windows para garantizar que se ejecute cada vez que el sistema arranque.
2. **Evasión avanzada:** Utiliza técnicas como la carga de código reflejado para evitar ser detectado por los antivirus, ejecutándose directamente en la memoria.
3. **Captura de información:** Registra todo lo que el usuario escribe (keylogging), toma capturas de pantalla y envía datos sensibles a un servidor de comando y control (C2).
4. **Comunicaciones maliciosas:** Conexión a dominios sospechosos como jorgeperezpu145[.]con-ip[.]com y a la IP 199[.]16[.]199[.]4 a través de protocolos HTTPS.

Características.

1. **Tamaño reducido:** Tinba es conocido por ser uno de los troyanos bancarios más pequeños en términos de tamaño de archivo, lo que facilita su distribución y ocultación.
2. **Robo de credenciales:** Este malware se especializa en robar credenciales de inicio de sesión y otra información sensible cuando los usuarios acceden a sitios web de bancos.
3. **Webinjects:** Utiliza técnicas de inyección web para presentar formularios falsos y mensajes engañosos a los usuarios, solicitando información personal y financiera.
4. **Mecanismos de resiliencia:** Tinba incorpora varios mecanismos para evitar la detección y asegurar su persistencia, como la generación de dominios (DGA) para comunicarse con sus servidores de comando y control (C&C) incluso si los originales son derribados.

COLCERT

Advertencia de Seguridad

Campaña de Malware Activa: Infostealer.Win32.Tinba.FEC3

COLCERT AD-0810-022

Procesos generados:

- **PID:** 5604 - Ejecuta el archivo malicioso desde la carpeta temporal del usuario.
- **PID:** 1280 - Se ejecuta csc.exe, que es parte del .NET Framework, y es comúnmente utilizado para compilar código en tiempo real.
- **PID:** 2272 - Se ejecuta ngentask.exe, otro componente del .NET Framework que podría estar relacionado con la optimización de la carga del malware.
- **PID:** 1456 - Se ejecuta ngen.exe, relacionado con la compilación de código en un sistema .NET para mejorar la ejecución.

Acciones del Malware:

- **Persistencia:** Modifica claves de registro y crea servicios para garantizar su ejecución.
- **Evasión:** Oculta su código en la memoria para evitar ser detectado por los antivirus.
- **Captura de Datos:** Roba contraseñas, nombres de usuario y realiza capturas de pantalla.
- **Comunicaciones C2:** Conecta con dominios maliciosos (ej. jorgeperezpu145[.]con-ip[.]com) para enviar datos robados.

Indicadores de Compromiso (IOCs):

- ✓ **Dominios maliciosos:** jorgeperezpu145[.]con-ip[.]com
- ✓ **Conexión externa:** 199[.]16[.]199[.]4 usando el proceso svchost.exe.

Recomendaciones para el Equipo de TI

1. **Aislamiento del sistema comprometido**:El sistema afectado debe ser aislado inmediatamente de la red para evitar la exfiltración de datos o la recepción de más comandos maliciosos del servidor C2.
2. **Análisis de red:**Revisar todos los logs de tráfico de red y buscar cualquier conexión hacia los dominios mencionados. Además, se debe analizar el tráfico DNS para detectar otros dominios sospechosos o maliciosos.
3. **Limpieza del registro:**Revisar las claves del registro modificadas por el malware y eliminarlas. Esto incluye las claves de inicio en Windows y los servicios creados por el malware.
4. **Revisión y actualización de políticas de seguridad:**Actualizar las políticas de antivirus y ejecutar un análisis completo en todos los sistemas para detectar posibles infecciones adicionales. También es recomendable implementar herramientas EDR (Endpoint Detection and Response) que puedan detectar y mitigar comportamientos sospechosos como la carga de código reflejado.
5. **Monitoreo de DNS y conexiones externas:**Implementar controles de monitoreo de DNS para identificar posibles consultas a dominios maliciosos en tiempo real y bloquear cualquier intento de conexión saliente a los dominios mencionados.

COLCERT

Advertencia de Seguridad

Campaña de Malware Activa: Infostealer.Win32.Tinba.FEC3

COLCERT AD-0810-022

"Es importante que todo el equipo de seguridad digital mantenga una vigilancia constante sobre las comunicaciones maliciosas observadas en la campaña. La captura de información sensible y la capacidad de evasión avanzada de este malware subrayan la importancia de monitorear en tiempo real las conexiones de red y realizar análisis profundos de los sistemas comprometidos.

Las medidas preventivas deben ser ejecutadas de inmediato para mitigar el riesgo y proteger la integridad de la información."

FUENTES:

- CVE Database - https://cve.mitre.org
- MISP - https://www.misp-project.org
- MITRE ATT&CK - https://attack.mitre.org
- NIST - Guías de seguridad cibernética - https://www.nist.gov
- Sandbox MINTIC – COLCERT - https://detectic.colcert.gov.co/external-user/upload-sample

NIVEL DE RIESGO

ALTO

COLCERT