TIC

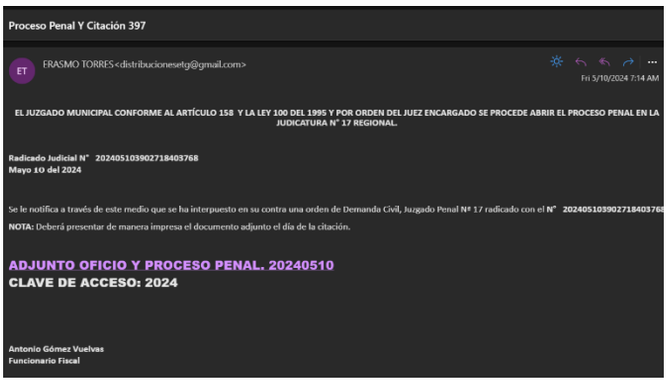
ALERTA

Taxonomía: Malware Análisis de Correo Electrónico con Contenido Malicioso

[COLCERT AL-0705-033]

TLP:CLEAR

Este informe técnico analiza un correo electrónico potencialmente malicioso. El remitente del correo es "Erasmo Torres" desde la dirección de correo electrónico distribucionesetg@gmail.com. El correo simula ser una notificación oficial de un proceso penal y citación judicial.



Análisis del Remitente

- Nombre del Remitente: Erasmo Torres
- Dirección de Correo: distribucionesetg@gmail.com
- Verificación del Remitente: La dirección de correo no pertenece a un dominio oficial gubernamental o judicial. Las entidades oficiales suelen usar dominios específicos, como ".gov" o ".jud".

Análisis del Contenido

- Asunto: "Proceso Penal Y Citación 397"
- Cuerpo del Mensaje:
- El correo menciona el artículo 158 y la ley 100 del 1995, lo que parece un intento de darle legitimidad.
- Se proporciona un número de radicado judicial (20240510390271840376 8) y una fecha de emisión (10 de mayo de 2024).
- Se solicita al destinatario presentar un documento adjunto impreso en una citación judicial.
- Incluye una nota y un enlace con la indicación "**ADJUNTO OFICIO Y PROCESO PENAL. 20240510**" seguido de una clave de acceso "2024".

Indicadores de Phishing

- Remitente Sospechoso: El correo proviene de una dirección no oficial (distribucionesetg@gmail.com).
- Generación de Urgencia y Miedo: El uso de términos legales y la amenaza de un proceso judicial están diseñados para inducir al destinatario a actuar rápidamente sin verificar la autenticidad.
- Solicitudes de Acción: El correo pide abrir un archivo adjunto, lo cual es una táctica común en correos phishing para distribuir malware.
- Enlaces y Archivos: La mención de un adjunto y una clave de acceso sugiere que el archivo podría contener software malicioso o dirigir al destinatario a una página de phishing.
- Hipervínculo externo https[:]//docs[.]google[.]com/uc?export=download&id=1LE5D12saxvJmCVbgrKIsfuQexRO8RKqL

Identificación el archivo

- Nombre del Archivo: TeamViewer_Desktop.exe
- Tamaño del Archivo: 13.42 MB (14068224 bytes)
- Hash del Archivo:
- MD5: 24f50d39dfc7e4780ce3d9e6c16353c4
- SHA-1: 02d749a198c2e716b41342f6fec4bdc65f68a33b
- SHA-256: d8f0a2512c50f4678f0c384cd4d42630e99b0a8e1382f70144faea894088d719

Resultados del Escaneo Antivirus

- Detección: 21/73 motores antivirus detectaron el archivo como malicioso.
- Etiquetas de Amenaza Comunes:
- Trojan.Fragtor/DCRAT: Etiquetado por varios motores antivirus, indicando la presencia de un troyano asociado con control remoto.

Secciones del Binario

- .text: Contiene el código ejecutable principal. Alta entropía indica posible ofuscación.
- .orpc: Sección relacionada con llamadas a procedimientos remotos.
- IPPCODE: Sección de datos posiblemente personalizada.
- .rdata: Datos de solo lectura, incluidas las tablas de importación.
- .data: Datos inicializados.

Información del Binario PE

- Tipo de Archivo: PE32 ejecutable (GUI) para Windows
- Compilador: Microsoft Visual C/C++ (2017 v.15.5-6)
- Timestamp de Compilación: 2024-04-15 15:43:27 UTC
- Firmado: El archivo no está firmado digitalmente.

COLCERT

TIC

ALERTA

Taxonomía: Malware Análisis de Correo Electrónico con Contenido Malicioso

[COLCERT AL-0705-033]

TLP:CLEAR

- **Importaciones del Archivo:** Bibliotecas comunes de Windows, incluyendo:
- dbghelp.dll
- KERNEL32.dll
- MAGNIFICATION.dll
- d2d1.dll

Recursos Contenidos

RT_ICON: 5 iconos.
RT_VERSION: Información de versión.
RT_GROUP_ICON: Grupo de iconos.
RT_MANIFEST: Manifiesto del archivo.
RT_BITMAP: Bitmaps.

Firma de Red y Comportamiento

- C2 Comunicación: Comunicaciones detectadas con dominios y direcciones IP sospechosas, incluidas conexiones a entusmanosdios.duckdns.org.
- JA3 Fingerprints: Firma SSL maliciosa detectada (AsyncRAT).

Técnicas y Tácticas de MITRE ATT&CK

TA0002 - Execution: Uso de API nativa para ejecutar comportamientos.
TA0003 - Persistence: Configuración del sistema para ejecutar programas en el arranque o inicio de sesión.
TA0004 - Privilege Escalation: Logon Autostart Execution.
TA0005 - Defense Evasion: Archivos u información obfuscados.
TA0006 - Credential Access: Volcado de credenciales del sistema operativo.
TA0007 - Discovery: Descubrimiento de información del sistema.
TA0011 - Command and Control: Uso de protocolos de capa de aplicación para comunicación C2.

Actividades de Comportamiento del Sistema

Archivos Abiertos. El malware modifica y abre múltiples archivos DLL relacionados con Java y .NET, entre otros. A continuación se muestra el listado de los archivos abiertos:

- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\k7rn7l32.dll
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\ntd3ll.dll
- C:\Program Files (x86)\Windows Defender\MpOAV.dll
- C:\Program Files\dotnet\k7rn7l32.dll
- C:\Program Files\dotnet\ntd3ll.dll
- C:\ProgramData\Microsoft\Crypto\OIDInfo
- C:\Users\<USER>\.dotnet\tools\k7rn7l32.dll
- C:\Users\<USER>\.dotnet\tools\ntd3ll.dll
- C:\Users\<USER>\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\csc.exe.log
- C:\Users\<USER>\AppData\Local\Microsoft\WindowsApps\k7rn7l32.dll

Impacto Potencial

El malware AsyncRAT permite a los atacantes obtener control remoto total del sistema infectado, lo que puede llevar a la exfiltración de datos sensibles, acceso a información privada como credenciales y registros de pulsaciones de teclado, y uso de la cámara web sin el conocimiento del usuario. Además, la capacidad del malware para evadir defensas y mantenerse persistente mediante modificaciones en el registro y conexiones con servidores de comando y control, amplifica el riesgo de espionaje y robo de información confidencial. Esto podría resultar en graves consecuencias financieras y de reputación para la organización afectada.

Un incidente de esta naturaleza puede permitir control remoto total del sistema.

Actividades Descargados

El malware descarga y crea archivos en el sistema. A continuación se muestra el listado de los archivos descargados:

- 77EC63BDA74BD0D0E0426DC8F8008506 (CAB file)
- %USERPROFILE%\Documents\Tunaop
- %USERPROFILE%\Documents\Tunaop\Chica.exe

Análisis dinámico de la muestra

Indicadores de Compromiso (IoC)

- C2 (Command and Control): entusmanosdios.duckdns.org
- IP:179[.]13 [.] 2 [.] 154
- Puerto: 2260
- Mutex: DcRatMutex_qwqdanchun
- Certificado: Cert1

MIICMDCCAZmgAwIBAgIVAMTaJFsgawxb4AwebDPgrN9TNtT9MA0GCSqGSIb3DQEBDQUAMGQxFTATBgNVBAMMDERjUmF0IFNlcnZlcjETM

Estos Indicadores de Compromiso relacionados con un servidor de comando y control (C2) utilizado por un malware. Estos indicadores incluyen un dominio específico, una dirección IP, un puerto, un mutex, y un certificado digital. Estos datos son cruciales para identificar y mitigar amenazas en una red, permitiendo a los equipos de seguridad tomar medidas preventivas y de respuesta ante incidentes.

COLCERT

ALERTA

Taxonomía: Malware Análisis de Correo Electrónico con Contenido Malicioso

[COLCERT AL-0705-033]

IP de Comando y Control C2

IP:179[.]13 [.] 2 [.] 154

TLP:CLEAR

El análisis de seguridad realizado sobre la dirección IP ha revelado la presencia de varios dominios asociados categorizados como "Malware" y "DNS dinámico". Estos dominios, muestran actividades potencialmente maliciosas, están siendo utilizados para evadir la detección y el bloqueo, representando una amenaza significativa para la seguridad de la red.

ASN : 32098
Descripción del propietario de la red
Colombia Móvil CO 86400

País/Región : Colombia
Prefijo : 160.0.0.0./3

Dominios Detectados:

- auyametemplanza.duckdns.org

  •Tipo: A
  •Categoría de Seguridad: Malware, Dynamic DNS
  •TTL: 60 segundos
  •Primera Detección: 12/04/2024
  •Última Detección: 16/06/2024

- estesidiosplat.duckdns.org

  •Tipo: A
  •Categoría de Seguridad: Malware, Dynamic DNS
  •TTL: 60 segundos
  •Primera Detección: 11/04/2024
  •Última Detección: 16/06/2024

- esteesdiosmio.duckdns.org

  •Tipo: A
  •Categoría de Seguridad: Malware, Dynamic DNS
  •TTL: 60 segundos
  •Primera Detección: 22/05/2024
  •Última Detección: 16/06/2024

•www.auyametemplanza.duckdns.org

•Tipo: A

•Categoría de Seguridad: Malware, Dynamic DNS
•TTL: 60 segundos
•Primera Detección: 12/04/2024
•Última Detección: 12/04/2024

•vinijr27.duckdns.org

•Tipo: A

•Categoría de Seguridad: Malware, Dynamic DNS
•TTL: 60 segundos
•Primera Detección: 29/05/2023
•Última Detección: 01/06/2023

En el análisis realizado se han identificado varios dominios categorizados como "Malware" y "DNS dinámico" asociados con la dirección IP evaluada, indicando actividades maliciosas y tácticas de evasión de detección. Estos hallazgos subrayan la necesidad de implementar medidas inmediatas para bloquear estos dominios y llevar a cabo un análisis exhaustivo para detectar cualquier posible compromiso en la red. La adopción de políticas de seguridad robustas y el monitoreo continuo son cruciales para mitigar estas amenazas y asegurar la protección de la infraestructura de la red.

COLCERT

ALERTA

Taxonomía: Malware Análisis de Correo Electrónico con Contenido Malicioso

[COLCERT AL-0705-033]

TLP:CLEAR

Claves del Registro Modificadas

El malware realiza modificaciones en las claves del registro para lograr persistencia.

- HKEY_CURRENT_USER\Environment
- HKEY_CURRENT_USER\Environment\windir
- HKEY_CURRENT_USER\SOFTWARE\Classes
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SmokerLtd
- HKEY_CURRENT_USER\Software
- HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\70\52C64B7E
- HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\70\52C64B7E\@%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe,-124
- HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\70\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
- HKEY_CURRENT_USER\Software\Classes\ms-settings
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\ActiveMovie\devenum\Version
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SmokerLtd
- HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\Run\SmokerLtd

Procesos creados

- El malware crea múltiples procesos relacionados con servicios y ejecución de comandos.

- C:\Users\<USER>\AppData\Local\Temp\TeamViewer_Desktop.exe"
- C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"
- C:\Windows\system32\services.exe
- C:\Windows\system32\svchost.exe -k DcomLaunch -p
- %SAMPLEPATH%\TeamViewer_Desktop.exe
- C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
- C:\Windows\system32\SecurityHealthService.exe
- "%SAMPLEPATH%\TeamViewer_Desktop.exe"
- "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe"

Interpretación de resultados

El análisis tanto estático como dinámico del archivo malicioso "PROCESO PENAL Y RADICADO ENVIADO 7.exe" revela que se trata de una variante del troyano AsyncRAT. Este malware se caracteriza por su capacidad de permitir el control remoto de sistemas infectados, proporcionando acceso a datos del usuario, la cámara web y registrando pulsaciones de teclado. El archivo ejecutable presenta múltiples indicadores de comportamiento malicioso, incluyendo técnicas avanzadas de evasión, persistencia a través de modificaciones en las claves del registro y comunicaciones C2 con el dominio entusmanosdios.duckdns.org. La presencia de un mutex específico (DcRatMutex_qwqdanchun) y la modificación de archivos DLL relacionados con Java y .NET refuerzan la sofisticación del malware en sus esfuerzos para mantenerse oculto y operativo en el sistema comprometido.

Recomendaciones:

- Capacitar a los empleados para identificar correos electrónicos sospechosos y comprender los intentos de phishing.
- Implementar un Sistema de Detección de Intrusiones (IDS) para monitorear actividades inusuales y alertar sobre amenazas en tiempo real.
- Mantener las firmas antivirus actualizadas para proteger contra las últimas variantes de malware.
- Realizar copias de seguridad regulares de datos importantes y mantenerlas en un lugar seguro.

Recomendaciones Técnicas:

Los equipos de TI de las entidades públicas y privadas pueden tomar varias acciones con la información compartida en el informe. Así:

Bloqueo de Dominios y Direcciones IP:

- Inmediato Bloqueo: Configurar los firewalls y otros sistemas de seguridad para bloquear los dominios y direcciones IP mencionadas en el informe.

- Monitoreo Continuo: Implementar monitoreo continuo para detectar cualquier intento de acceso a estos dominios y direcciones IP.

NIVEL DE RIESGO

Alto

COLCERT

TIC

ALERTA

Taxonomía: Malware Análisis de Correo Electrónico con Contenido Malicioso

[COLCERT AL-0705-033]

TLP:CLEAR

Recomendaciones Técnicas:

- Actualización de Listas de Seguridad:
  - DNS y Proxy: Actualizar las listas negras de servidores DNS y proxies con los dominios categorizados como "Malware" y "DNS dinámico".
  - Sistemas IDS/IPS: Configurar los sistemas de detección y prevención de intrusiones (IDS/IPS) para alertar sobre cualquier **tráfico** relacionado con estas direcciones IP y dominios.
- Análisis y Monitoreo Interno:
  - Escaneo de la Red: Realizar un escaneo completo de la red para identificar cualquier señal de compromiso asociado con los indicadores proporcionados (IoC).
  - Revisión de Logs: Revisar los logs de los sistemas y dispositivos de red para detectar cualquier actividad sospechosa relacionada con los dominios y direcciones IP mencionadas.
- Capacitación y Concientización:
  - Formación de Personal: Capacitar al personal de TI y de seguridad en la identificación y respuesta a amenazas relacionadas con los indicadores de compromiso mencionados.
  - Concientización del Usuario Final: Informar a los usuarios finales sobre las amenazas y proporcionar pautas para evitar caer en trampas de phishing y otros vectores de ataque.
- Reforzamiento de Políticas de Seguridad:
  - Actualización de Políticas: Revisar y actualizar las políticas de seguridad para incluir medidas específicas contra las amenazas identificadas.
  - Implementación de Controles Adicionales: Considerar la implementación de controles adicionales, como autenticación multifactor (MFA) y segmentación de red, para aumentar la seguridad.
- Coordinación con Proveedores y Socios:
  - Notificación a Proveedores: Informar a los proveedores de servicios de internet (ISP) y otros socios relevantes sobre las amenazas para que tomen medidas similares.
  - Colaboración en Seguridad: Colaborar con otras entidades y organizaciones para compartir información sobre amenazas y mejores prácticas de seguridad.
- Revisión y Mejora de Infraestructura:
  - Evaluación de Vulnerabilidades: Realizar evaluaciones regulares de vulnerabilidades para identificar y mitigar posibles puntos de entrada para atacantes.
  - Actualización de Sistemas: Asegurar que todos los sistemas operativos, software y dispositivos de red estén actualizados con los últimos parches y actualizaciones de seguridad.

Con la información proporcionada en el informe, los equipos de TI pueden fortalecer significativamente sus defensas contra las amenazas de malware y DNS dinámico. Implementando estas acciones y manteniendo un enfoque proactivo en la seguridad, las entidades públicas y privadas pueden reducir el riesgo de compromisos y asegurar la protección de su infraestructura crítica.

Fuentes

- "The Art of Deception" de Kevin Mitnick: Un libro sobre tácticas de ingeniería social y cómo protegerse contra ellas.
- "Malware Analyst's Cookbook and DVD" de Michael Ligh, Steven Adair, Blake Hartstein y Matthew Richard: Un recurso detallado sobre análisis de malware.
- Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). "A framework for detection and measurement of phishing attacks". Proceedings of the 2007 ACM workshop on Recurring malcode.
- VirusTotal: www.virustotal.com – Herramienta para analizar archivos y URLs en busca de malware.
- CISA (Cybersecurity & Infrastructure Security Agency): www.cisa.gov – Guías y recomendaciones de ciberseguridad.
- Colcert.

COLCERT