Ramnit Lab

Propiedad	Detalle
Plataforma	CyberDefenders
Categoría	Endpoint Forensics
Dificultad	Fácil
Estado	Completado
Proyecto Completo	matircode.dev

---

1. Resumen Ejecutivo

Antecedentes e Inicialización

La presente investigación forense digital se inició tras la activación de una alerta en el Sistema de Detección de Intrusos (IDS), la cual identificó telemetría anómala saliente desde una estación de trabajo corporativa. Ante la sospecha fundada de un compromiso por software malicioso activo, se procedió a realizar la adquisición en caliente de la memoria RAM del sistema afectado para preservar los artefactos volátiles y reconstruir las acciones del adversario.

Alcance de la Investigación

El análisis se ejecuta sobre el volcado de memoria provisto, persiguiendo los siguientes objetivos tácticos:

1. Identificar el proceso o procesos maliciosos responsables del compromiso y su linaje en el sistema.
2. Localizar artefactos de red activos o sockets que evidencien conexiones hacia la infraestructura de Comando y Control (C2).
3. Determinar la existencia de técnicas de evasión de defensas, tales como inyección de código en procesos legítimos.
4. Extraer firmas criptográficas (hashes) y metadatos temporales de los binarios involucrados para su posterior correlación con fuentes de Threat Intelligence.

---

2. Línea de Tiempo del Incidente (Timeline)

Lista cronológica detallada de las acciones del actor de amenazas, deducidas a través del análisis del tráfico de red y los artefactos disponibles.

Marca de Tiempo (UTC)	Evento / Acción del Atacante	Artefacto / Fuente de Log / Filtro
2019-12-01 08:36:04	[Metadato de Desarrollo] Fecha y hora de compilación original del binario base de Ramnit.	VirusTotal (PE Header Metadata: TimeDateStamp)
2024-02-01 19:48:50	Ejecución inicial del binario malicioso mimetizado como instalador de navegador.	Volatility 3: `windows.pstree` / PID: 4628
2024-02-01 19:48:51	Intento de balizamiento de red saliente (TCP SYN) hacia la infraestructura de Comando y Control (C2) de Ramnit.	Volatility 3: `windows.netstat` / Socket: 58.64.204.181:5202

---

3. Mapeo de Amenazas (MITRE ATT&CK Framework)

Correlación formal de las Tácticas, Técnicas y Procedimientos (TTPs) identificadas durante la investigación con el marco de trabajo de MITRE ATT&CK.

Táctica: Defensa Evasion (TA0005)

- **Técnica:** Masquerading: Match Legitimate Name or Location (T1036.005)
- **Análisis Técnico:** El artefacto malicioso se identificó bajo el nombre de `ChromeSetup.exe` (PID 4628). El adversario abusó del mimetismo de nombres para camuflar el troyano Ramnit como un instalador legítimo de software. La sospecha analítica se confirmó debido a su persistencia extendida en memoria (violando el ciclo de vida corto de un instalador real), sus conexiones de red anómalas fuera del rango de Google y la presencia de páginas de memoria inyectadas con privilegios RWX.

Táctica: Command and Control (TA0011)

- **Técnica:** Non-Standard Port (T1571)
- **Análisis Técnico:** El troyano configuró canales de balizamiento salientes direccionados de forma explícita hacia el puerto **5202/TCP** de un servidor externo. El uso de puertos no estándar para el tráfico web permite al malware evadir firmas de inspección básicas y firewalls perimetrales desconfigurados que no realizan análisis profundo de paquetes (DPI).

4. Indicadores de Compromiso (IoCs) Encontrados

Datos tácticos extraídos del análisis que sirven para alimentar las reglas de detección en sistemas defensivos como Firewalls, EDR o SIEM.

Indicadores de Red (Network Artifacts)

- **Dirección IP de C2:** `58.64.204.181` (Puerto de escucha: 5202 / Protocolo: TCP)
- **Geolocalización del C2:** Hong Kong (Región Administrativa Especial)
- **Dominio C2 Identificado:** `dnsnb8.net`

Indicadores de Host (Host Artifacts)

- **Artefacto malicioso:** `ChromeSetup.exe` (Mimetismo de instalador legítimo)
- **Identificador de Proceso (PID):** `4628`
- **Ruta Absoluta en Disco:** `C:\Users\alex\Downloads\ChromeSetup.exe`
- **Hash SHA-1:** `280c9d36039f9432433893dee6126d72b9112ad2`
- **Metadato PE (Compile Time):** 2019-12-01 08:36 (UTC)

---

5. Recomendaciones de Mitigación y Erradicación

Planes de acción correctiva y preventiva sugeridos para el equipo de ingeniería con el fin de neutralizar la amenaza persistente y robustecer la postura de seguridad.

1. **Aislamiento Inmediato del Endpoint:** Desconectar de forma lógica el host comprometido de la red local mediante capacidades de contención del EDR o mediante cambios forzados en el puerto del switch (VLAN de cuarentena). Esto frenará la persistencia operativa y mitigará la propagación lateral recursiva característica de Ramnit.
2. **Bloqueo Perimetral de IoCs:** Desplegar una regla de denegación estricta (*Drop*) en los Firewalls corporativos para bloquear todo tráfico saliente hacia el segmento o IP `58.64.204.181`.
3. **Implementar políticas de *Sinkholing*** en los servidores DNS internos para interceptar y anular las peticiones de resolución dirigidas al dominio malicioso `dnsnb8.net`.
4. **Erradicación y Saneamiento Local:** Terminar el árbol de procesos vinculado al PID 4628 y remover de forma segura el binario alojado en `C:\Users\alex\Downloads\ChromeSetup.exe`. Debido a las capacidades parasitarias de Ramnit (infección de ejecutables locales `.exe`, `.dll` y archivos `.html`), se debe ejecutar

un escaneo heurístico completo en el disco duro antes de reincorporar el activo a producción.

5. **Endurecimiento de Directivas (Hardening):** Restringir la ejecución de binarios no firmados o scripts directamente desde carpetas con permisos de escritura de usuario (`\Downloads` , `\AppData\Local\Temp`) mediante el uso de AppLocker o Windows Defender Application Control (WDAC).

---

6. Resolución del Desafío (CyberDefenders Q&A)

Sección técnica destinada a la resolución y validación de los requerimientos específicos del laboratorio, detallando el procedimiento analítico y la respectiva evidencia gráfica.

Pregunta 1: What is the name of the process responsible for the suspicious activity?

- **Respuesta:** `ChromeSetup.exe`
- **Metodología de Análisis:** Al auditar el árbol de procesos mediante el plugin `windows.pstree` , se identificó la presencia de un binario sospechoso denominado `ChromeSetup.exe` ejecutándose bajo el contexto de usuario. Aunque el nombre simula ser un instalador legítimo de Google Chrome, su persistencia en memoria y la posterior telemetría de red confirman que actúa como el vector de ejecución principal del malware Ramnit en el endpoint.

```
** 4568 4508    explorer.exe    0xca82b7440340  55      -       1       False   2024-02-01 19:48:26.000000      N/A
*** 7780        4568    OneDrive.exe    0xca82b814a0c0  21      -       1       True    2024-02-01 19:48:42.000000
*** 7540        4568    SecurityHealth  0xca82b7858080  3       -       1       False   2024-02-01 19:48:41.000000
*** 7684        4568    vmtoolsd.exe    0xca82b7dbe080  8       -       1       False   2024-02-01 19:48:41.000000
*** 4628        4568    ChromeSetup.ex  0xca82b830a300  4       -       1       True    2024-02-01 19:48:50.000000
* 836   624     fontdrvhost.ex  0xca82b299c140  6       -       1       False   2024-02-01 19:48:24.000000      N/A
```

Pregunta 2: What is the exact path of the executable for the malicious process?

- **Respuesta:** `C:\Users\alex\Downloads\ChromeSetup.exe`
- **Metodología de Análisis:** Tras aislar el proceso sospechoso `ChromeSetup.exe` (PID 4628), se ejecutó el plugin de Volatility 3 `windows.cmdline` . La telemetría recuperada del espacio de memoria del kernel reveló el comando exacto con el que fue invocado, exponiendo que el binario se alojaba y ejecutaba directamente desde el directorio de descargas del perfil del usuario comprometido (`alex`).

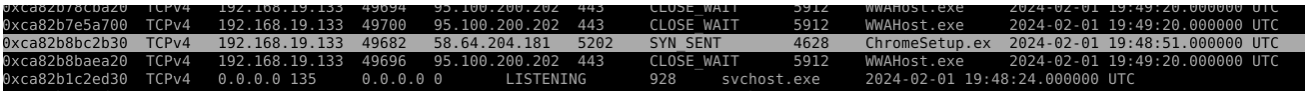
```
❯ /opt/volatility3/vol.py -f memory.dmp windows.cmdline --pid 4628
Volatility 3 Framework 2.0.2
Progress:  100.00               PDB scanning finished
PID     Process Args

4628    ChromeSetup.ex  "C:\Users\alex\Downloads\ChromeSetup.exe"
```

Pregunta 3: Identifying network connections is crucial for understanding the malware's communication strategy. What IP address did the malware attempt to connect to?

- **Respuesta:** `58.64.204.181`
- **Metodología de Análisis:** Una vez estabilizado el entorno operativo de Volatility 3 mediante un entorno virtual dedicado, se procedió a ejecutar el módulo de red `windows.netstat` (o `windows.netscan` según la compilación de la arquitectura del perfil) para auditar las conexiones activas en el volcado de memoria.

  Al filtrar los resultados por el PID 4628, correspondiente al proceso sospechoso `ChromeSetup.exe`, se descubrió un socket saliente direccionado hacia la IP externa `58.64.204.181` en el puerto `5202`. El estado de la conexión en `SYN_SENT` confirma un intento activo por parte del troyano Ramnit de establecer el canal de comunicación persistente con su infraestructura C2.



```
0xca82b78cba20  TCPv4  192.168.19.133  49694  95.100.200.202  443   CLOSE_WAIT  5912  WWAHost.exe     2024-02-01 19:49:20.000000 UTC
0xca82b7e5a700  TCPv4  192.168.19.133  49700  95.100.200.202  443   CLOSE_WAIT  5912  WWAHost.exe     2024-02-01 19:49:20.000000 UTC
0xca82b8bc2b30  TCPv4  192.168.19.133  49682  58.64.204.181   5202  SYN_SENT    4628  ChromeSetup.ex  2024-02-01 19:48:51.000000 UTC
0xca82b8baea20  TCPv4  192.168.19.133  49696  95.100.200.202  443   CLOSE_WAIT  5912  WWAHost.exe     2024-02-01 19:49:20.000000 UTC
0xca82b1c2ed30  TCPv4  0.0.0.0 135     0.0.0.0 0       LISTENING       928     svchost.exe     2024-02-01 19:48:24.000000 UTC
```

Pregunta 4: To determine the specific geographical origin of the attack, Which city is associated with the IP address the malware communicated with?

- **Respuesta:** `Hong Kong`
- **Metodología de Análisis:** Tras aislar la dirección IP del servidor de Comando y Control (C2) (`58.64.204.181`) mediante el análisis forense de memoria, se procedió a ejecutar una fase de enriquecimiento táctico utilizando técnicas de inteligencia de fuentes abiertas (OSINT). Al consultar bases de datos de geolocalización de direccionamiento IP público, se determinó con precisión que el servidor con el que interactuaba el troyano Ramnit está ubicado en la ciudad de **Hong Kong**, lo que ayuda a establecer el origen geográfico de la infraestructura del atacante.

Pregunta 5: Hashes serve as unique identifiers for files, assisting in the detection of similar threats across different machines. What is the SHA1 hash of the malware executable?

- **Respuesta:** `280c9d36039f9432433893dee6126d72b9112ad2`
- **Metodología de Análisis:** Una vez aislado el PID 4628 correspondiente al proceso sospechoso, se procedió a realizar la extracción física del ejecutable desde la memoria volátil utilizando el plugin `windows.dumpfiles`.

  Del conjunto de artefactos generados por Volatility 3, se seleccionó específicamente el archivo representativo del objeto de sección de imagen en el kernel (`ImageSectionObject`), nombrado como `file.0xca82b85325a0.0xca82b7e06c80.ImageSectionObject.ChromeSetup.exe.img`, debido a que preserva de forma fidedigna la estructura del ejecutable en memoria. Finalmente, se utilizó la herramienta de consola de Linux `sha1sum` para calcular la firma criptográfica única del binario comprometido.

Pregunta 6: Examining the malware's development timeline can provide insights into its deployment. What is the compilation timestamp for the malware?

- **Respuesta:** `2019-12-01 08:36`
- **Metodología de Análisis:** Con la firma criptográfica SHA-1 obtenida directamente del volcado de memoria (`280c9d36039f9432433893dee6126d72b9112ad2`), se procedió a realizar una consulta avanzada de Inteligencia de Amenazas en la plataforma VirusTotal.

  Al auditar la sección de metadatos del encabezado PE (*Portable Executable*) del archivo, específicamente en el campo interno `TimeDateStamp` de la estructura `IMAGE_FILE_HEADER`, se extrajo de forma fidedigna la marca de tiempo en la que el

compilador empaquetó originalmente el código ejecutable, fijando cronológicamente su creación el 1 de diciembre de 2019 a las 08:36 UTC.

History

Creation Time	2019-12-01 08:36:04 UTC
First Submission	2024-02-03 00:02:57 UTC
Last Submission	2026-05-29 16:05:19 UTC
Last Analysis	2026-04-30 09:40:35 UTC

Pregunta 7: Identifying the domains associated with this malware is crucial for blocking future malicious communications and detecting any ongoing interactions with those domains within our network. Can you provide the domain connected to the malware?

- **Respuesta:** `dnsnb8.net`
- **Metodología de Análisis:** Tras extraer con éxito la firma criptográfica SHA-1 de la sección de imagen mapeada del binario (`280c9d36039f9432433893dee6126d72b9112ad2`), se ejecutó un análisis de relaciones complejas en bases de datos globales de Threat Intelligence (VirusTotal).

  Al inspeccionar los registros de DNS pasivo (*Passive DNS*) y las actividades de resolución de red documentadas en entornos de Sandbox para esta variante de Ramnit, se aisló el dominio de Comando y Control (C2) activo `dnsnb8.net`. El malware abusa de este dominio dinámico para mantener la persistencia operativa y la comunicación con sus operadores, permitiéndole pivotar de infraestructura IP de forma transparente ante bloqueos perimetrales.

Contacted Domains (4)

Domain	Detections	Created	Registrar
ddos.dnsnb8.net	12 / 91	2020-08-13	DYNADOT LLC
dnsnb8.net	12 / 91	2020-08-13	DYNADOT LLC
res.public.onecdn.static.microsoft	1 / 91	2023-05-05	MarkMonitor Inc.
www.microsoft.com	0 / 91	1991-05-02	-