Grupo de ransomware: Agent Tesla

Resumen ejecutivo

Agent Tesla es un ***Remote Access Trojan*** **(RAT)** e ***infostealer*** activo desde 2014 y distribuido bajo un modelo de ***malware-as-a-service*** (MaaS), ampliamente utilizado en campañas de cibercrimen. Agent Tesla constituye una de las amenazas más detectadas en España por su **capacidad para robar información de equipos comprometidos y exfiltrar credenciales.** El malware se propaga principalmente a través de **campañas de phishing** con adjuntos dañinos o documentos que descargan posteriormente el *payload*.

Una vez instalado, Agent Tesla emplea **técnicas de ofuscación** y **persistencia**, y se especializa en el robo de credenciales de navegadores, clientes de correo, VPNs y aplicaciones corporativas. Además, incorpora funciones de ***keylogging***, **capturas** de **pantalla** y **acceso** al **portapapeles**. Sus variantes más recientes amplían los **métodos** de **exfiltración** a través de canales HTTP, SMTP y FTP, lo que permite enviar la información robada a servidores controlados por el atacante de forma flexible y difícil de rastrear.

Por su amplia distribución global y su capacidad para comprometer credenciales y facilitar accesos posteriores, Agent Tesla representa un **riesgo alto para organizaciones privadas de múltiples sectores, administración pública y ciudadanía**.

Agent Tesla debe considerarse una amenaza **persistente y muy utilizada** en campañas de robo de información y compromisos iniciales. Las defensas recomendadas incluyen reforzar la **protección frente a phishing**, desplegar **MFA** y utilizar soluciones **EDR** para detectar comportamientos anómalos asociados al malware.

Grupo de ransomware: Agent Tesla

Agent Tesla es un malware tipo RAT e *infostealer* activo desde 2014 y distribuido como MaaS. Aunque este malware se presente como un software de monitorización “legítima”, la documentación y el soporte que proporcionan incluyen indicaciones explícitas para evadir antivirus y explotar vulnerabilidades, lo que evidencia una orientación claramente criminal. Esta combinación de modelo comercial estructurado (MaaS), continua evolución técnica y baja barrera de entrada para atacantes convierte a Agent Tesla en una amenaza persistente ampliamente utilizada.

Países y sectores afectados

Agent Tesla mantiene una **actividad global** desde hace más de una década, con especial prevalencia en Europa, Asia y América.

En el ámbito estatal, la actividad de este malware durante el año 2024 había disminuido, desplazado parcialmente por otros *infostealers* más recientes. No obstante, el malware sigue activo, ya que durante los primeros meses de 2025 se registró una oleada de correos dañinos asociada a campañas de phishing, en la que Agent Tesla fue nuevamente identificado entre los *infostealers* distribuidos.

En cuanto a los sectores afectados, Agent Tesla no se orienta a industrias específicas, sino que se **propaga de forma masiva**. Aun así, los sectores más impactados suelen ser aquellos donde las **credenciales corporativas representan un activo crítico**, como servicios profesionales, logística, manufactura, educación, tecnología y administraciones públicas. Además, las pequeñas y medianas empresas continúan siendo uno de los objetivos más habituales debido a la naturaleza indiscriminada de las campañas de distribución.

Análisis técnico

Desde un punto de vista técnico, Agent Tesla es un RAT e infostealer distribuido predominantemente mediante phishing con adjuntos dañinos. Una vez ejecutado, se ofusca para evadir su detección y establecer persistencia para asegurar su ejecución en cada arranque o inicio de sesión del usuario.

En la fase de recolección, recorre el sistema en busca de software específico y almacenes de credenciales. Paralelamente, activa funciones de keylogging, captura de pantalla y acceso al portapapeles.

Por último, la exfiltración de datos la realiza de forma flexible a través de múltiples protocolos, configurables por el atacante, como por ejemplo, HTTP, SMTP, FTP,… En algunos casos utiliza el navegador TOR como proxy para ocultarse y dificultar la atribución.

Características técnicas principales:

- **Tipo y plataforma**: RAT/infostealer escrito en .NET y diseñado para sistemas Windows
- **Modelo de distribución:** Malware-as-a-Service (MaaS), vendido o alquilado en foros clandestinos, con versiones y actualizaciones periódicas.
- **Vector de infección habitual:** Correos de phishing con adjuntos dañinos o documentos Office que descargan o lanzan el payload.
- **Recolecta información del sistema**: Información del sistema operativo, configuración del equipo, nombre de usuario, IP pública, información de hardware, etc..
- **Persistencia:** Capacidad para auto-instalarse en el sistema, asegurando que el malware sobreviva a reinicios y se mantenga persistente en el equipo.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	**T1566.001** — Phishing: Spearphishing Attachment
Execution	**T1053.005** — Scheduled Task/Job: Scheduled Task **T1203** — Exploitation for Client Execution **T1204.002** — User Execution: Malicious File **T1047** — Windows Management Instrumentation
Persistence	**T1547.001** — Registry Run Keys / Startup Folder **T1112** — Modify Registry
Privilege Escalation	**T1055** — Process Injection: Dynamic-link Library Injection **T1055.012** — Process Hollowing
Defense Evasion	**T1497** — Virtualization/Sandbox Evasion **T1218.009** — System Binary Proxy Execution: Regsvcs/Regasm **T1027** — Obfuscated Files or Information **T1564 —** Hidden Artifacts **T1140** — Deobfuscate/Decode Files or Information **T1562.001** — Impair Defenses: Disable or Modify Tools
Credential Access	**T1555** — Credentials from Password Stores
Discovery	**T1057** — Process Discovery **T1016** — System Network Configuration Discovery **T1082** — System Information Discovery **T1016.002** — Wi-Fi Discovery **T1033** — System Owner/User Discovery
Collection	**T1560** — Archive Collected Data **T1185** — Browser Session Hijacking **T1115** — Clipboard Data **T1056** — Input Capture: Keylogging **T1113** —Screen Capture
Command and Control	**T1071** — Application Layer Protocol **T1105** — Ingress Tool Transfer
Exfiltration	**T1048.003** — Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

Medidas de mitigación

Proactivas

- ❑ Implementar MFA para reducir el impacto del robo de credenciales y acceso no autorizado. (T1555 - Credentials from Password Stores)
- ❑ Bloquear macros y deshabilitar contenido activo en documentos Office provenientes de correo electrónico. (T1203 - Exploitation for Client Execution)
- ❑ Activar listas de aplicaciones permitidas (allowlisting) para impedir la ejecución de binarios desconocidos. (T1047 - Windows Management Instrumentation)
- ❑ Restringir privilegios y aplicar un modelo de mínimos privilegios para evitar persistencia y ejecución de componentes dañinos. (T1562 - Impair Defenses)
- ❑ Formación continua en concienciación, especialmente en detección de correos y adjuntos sospechosos.(T1566.001 - Phishing: Spearphishing Attachment)

Reactivas

- ❑ Usar EDR o antivirus con capacidades de detección de *keyloggers* y actividad *fileless*, clave en variantes recientes. (T1203 - Exploitation for Client Execution)
- ❑ Monitorizar tráfico saliente y bloquear conexiones SMTP/FTP/HTTP no autorizadas, usados para exfiltración. (T1048.003 - Exfiltration Over Unencrypted Non-C2 Protocol)

Conclusiones y recomendaciones

Agent Tesla sigue siendo un *infostealer* **activo y persistente**, aunque su presencia ha descendido frente a otros malware más recientes y agresivos. Aun así, mantiene campañas de phishing que afectan tanto a grandes empresas como a pymes, y su modelo ***Malware-as-a-Service*** permite que actores con distintos niveles de sofisticación continúen explotándolo. Sus técnicas (robo de credenciales, *keylogging*, captura de pantalla, exfiltración y persistencia) lo convierten en una **amenaza significativa para para el tejido empresarial, la administración pública y la ciudadanía.**

Para **reducir el riesgo**, se recomienda implementar filtrado de correo avanzado, bloquear la ejecución de macros y archivos dañinos, reforzar los accesos con MFA y limitar los privilegios de usuario. Además, es clave monitorizar el tráfico saliente para detectar posibles exfiltraciones, mantener sistemas y aplicaciones actualizadas, y emplear soluciones EDR que identifiquen comportamientos sospechosos. Además, la formación continua del personal en detección de phishing y buenas prácticas de seguridad sigue siendo fundamental para prevenir infecciones desde las fases iniciales.

