	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-febrero-2022	**Malware RedLine Stealer**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Contenido dañino
Tipo de incidente: Malware
Nivel de riesgo: Alta

II. ALERTA

RedLine Stealer es un Malware tipo troyano que se difunde a través de internet y cuyo objetivo principal es obtener de manera fraudulenta información de la víctima, este contenido dañino funciona como Malware-as-a-Service

Figura 1. Ilustración asociada a Malware RedLine Stealer

III. INTRODUCCIÓN

El Malware as a Service (**MaaS)** es tratado como otro producto digital, posee sus fases beta, actualizaciones, además puede ser adquirido a un precio estipulado. Este modo de operación no solamente sirve para distribuir malware al blanco deseado; sino también ransomware, ataques DDoS, entre otros.

Con base a lo expuesto anteriormente, RedLine ha estado activo en el mercado desde 2020 y es uno de los MaaS, más usados por los ciberdelincuentes para operaciones de spam, sitios web

maliciosos, entre otros. Las características de este malware son: desarrollado en C#, utiliza una API SOAP para establecer comunicación con su servidor C2, bajo costo de licencia y "facilidad de operación", al igual que otros MaaS; se encuentra disponible una variante oficial y una "crackeada" y los valores dependerán del tiempo de ejecución, por ejemplo: desde un pago mensual de $150 hasta $800 por una licencia de por vida.

En la siguiente gráfica se muestra valores referenciales de este **MaaS.**

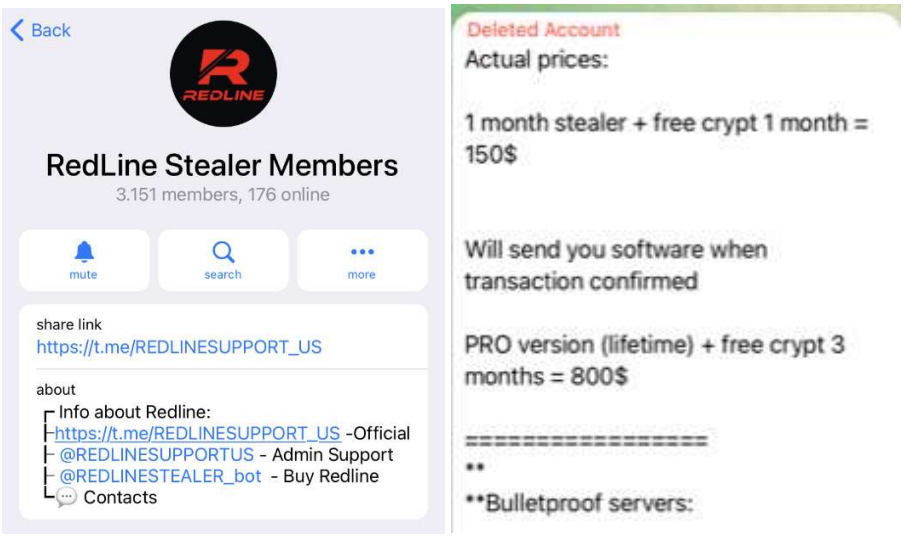

Figura 2. Valores comerciales de RedLine
Fuente: Telegram

En la siguiente gráfica se observa la versión 20.2 de RedLine, esta versión incluye opciones adicionales de administración de datos robados, administración de notificaciones, registro y errores.

	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-febrero-2022	**Malware RedLine Stealer**	V 1.1

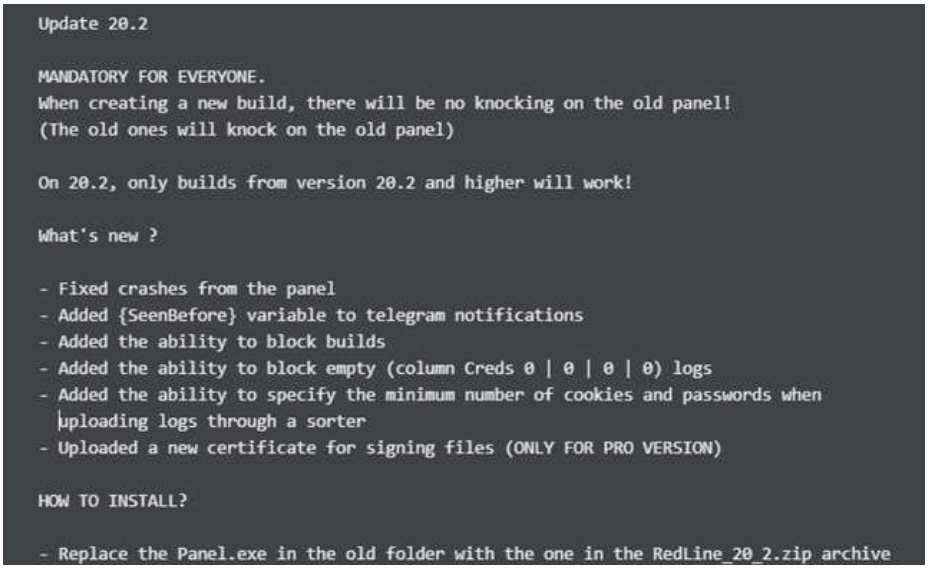

Figura 3. Versión 20.2 de RedLine
Fuente: Cyberint

RedLine muestra un panel de control para sus suscriptores; desde el cual pueden gestionar configuraciones de campaña, crear cargas útiles y revisar la información robada de las víctimas.

En la siguiente figura se observa la pantalla de inicio del malware RedLine.

	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-febrero-2022	**Malware RedLine Stealer**	V 1.1

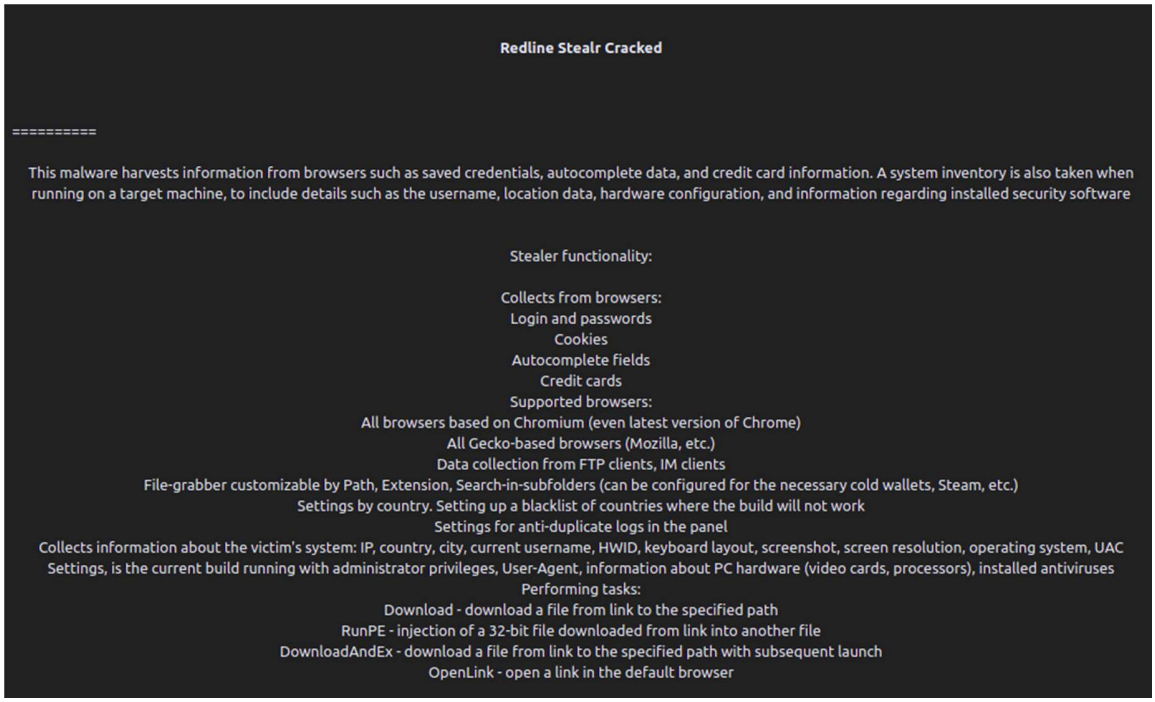

Figura 4. Ventana de inicio de RedLine
Fuente: Cyberint

Como se mencionó anteriormente, este MaaS presenta ciertas “carácterísitcas” entre ellas su facilidad de uso.

	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-febrero-2022	**Malware RedLine Stealer**	V 1.1

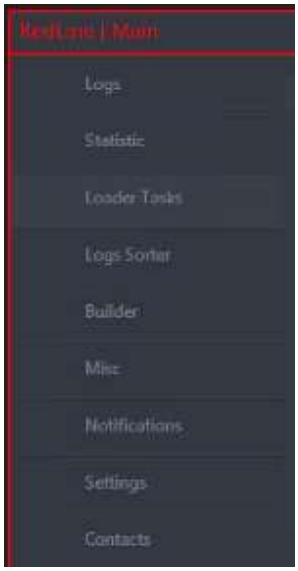

Figura 5. Menú de RedLine
Fuente: Cyberint

IV. VECTOR DE ATAQUE:

Existen maneras de distribución de RedLine, entre las que se mencionan:

- Ingeniería social mediante correo electrónico; entre los adjuntos más comunes con los payload se encuentran: Archivos de Ofimática, PDF, RAR y ZIP, Archivos ejecutables, JavaScript.
- Campañas de Malverstising.
- Archivo adjunto en portales de descargas anónimos como AnonFiles.
- Grupos de Chat de Telegram, Discord.

En la siguiente figura se observa el ejecutable de RedLine.

	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-febrero-2022	**Malware RedLine Stealer**	V 1.1

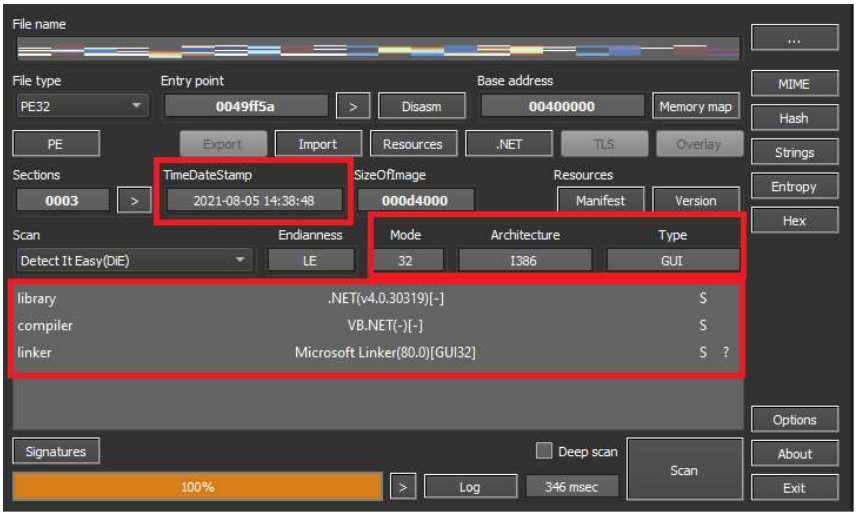

Figura 6. Análisis del Ejecutable de RedLine
Fuente: Cyble

Luego de la ejecución del malware, este envía los datos XML a C2, como se observa en la siguiente gráfica.

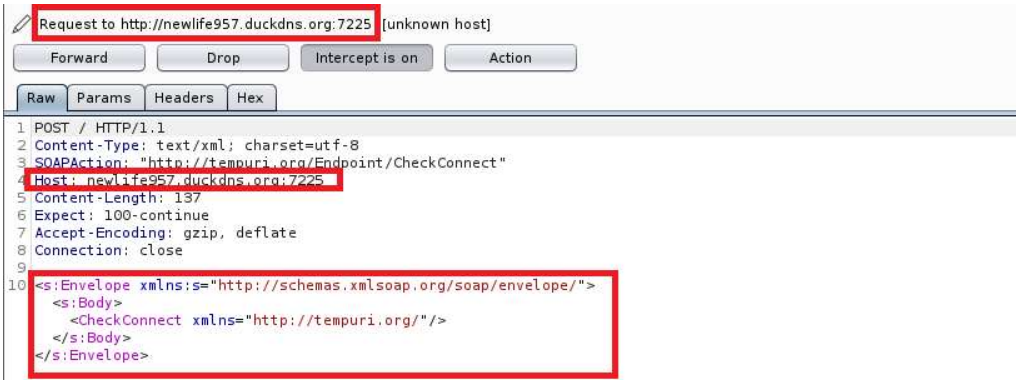

Figura 7. Envío de información por parte de RedLine
Fuente: Cyble

Cuando el malware intenta comunicarse con el C2 del atacante, el C2 envía el resultado con la etiqueta <*CheckConnectResult*> con el valor verdadero para que el malware sepa que el C2 está funcionando, como se muestra en la siguiente figura.

Figura 8. Envío de información por parte de RedLine
Fuente: Cyble

Posteriormente el malware envía una solicitud de "configuración del entorno" al C2 atacante; el C2 recibe y envía la respuesta envía los detalles de configuración al malware.

Figura 9. Información intercambiada entre C2 y el malware.
Fuente: Cyble

	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-febrero-2022	**Malware RedLine Stealer**	V 1.1

V. IMPACTO:

Este malware tiene afectación directa con la confidencialidad de la información; ya que RedLine realiza estas actividades:

- Recopila información de Navegadores (basados en Chromium y Gecko), credenciales guardadas, datos de autocompletado e información de tarjetas de crédito.
- También realiza un inventario del sistema cuando se ejecuta en una máquina de destino, para incluir detalles como el nombre de usuario, los datos de ubicación, la configuración del hardware y la información sobre el software de seguridad instalado.
- Desplegar un Backdoor para establecer comunicación y acceso a la máquina.
- Las versiones más recientes de RedLine agregaron la capacidad de robar criptomonedas.

- Los clientes de FTP e IM también son el objetivo de esta familia, y este malware tiene la capacidad de cargar y descargar archivos, ejecutar comandos y enviar periódicamente información sobre la computadora infectada.
- Implementar una extensión maliciosa en el navegador para registrar toda la información que la víctima este agregando, como un Keylogger y la posibilidad de tomar screenshot sin que el usuario se entere.

VI. INDICADORES DE COMPROMISO:

Propiedades Básicas	
SHA-256	8788930d5bf09c258af90bcf3f19f2c41cb4dabd93ef34d3b787cc564a23a9ee 87f8199f30c9bd50654dd432ad94aedced4b2f81d67995a9b62afaee1aa3cbfb 899863f4905401af16477a1ebbe593b05be6d25329db6c4ef294e872d6356bf8 8c5b4b59158b312796889601432317 3aeaf2160b5db535eeec8f1468208912f8 8ca2148c028fa80f102a0366bb03f8de2ea6572b00c5bdb1842c3fc090bfe306 8ef9d91092116117714033f25ca136675794e2e4a34d50ec5f3b7016fb7600d3 8fa87a4b240ecb2c3b8aa82348e74296d945168a6c805b1f4db3a854232981ce 8feda77ca3c3fa7bd352ac93efe10db631e428ea8079874f3248dbd1f84d05d1 92855b88ec5535f833090b28434fd596cb3058af93582df0859b2b57a6a884d2 92855b88ec5535f833090b28434fd596cb3058af93582df0859b2b57a6a884d2 93c898e900b2f5b2df2eb45ea60f30735444c4bc40166bf6bb487c4846f525bc 95f79fdcfb83a5035a2e3fa8621a653a0022925a9d1cb8729b8956db202fc3d8 9072f90e16a2357f2d7e34713fe7458e65aae6e77eeb2c67177cf87d145eb1a6 f224b56301de1b40dd9929e88dacc5f0519723570c822f8ed5971da3e2b88200

	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-febrero-2022	**Malware RedLine Stealer**	V 1.1

Propiedades Básicas		
	ffee20e0c17936875243ac105258abcf77e70001a0e8adc80aedbc5cfa9a7660 88ff40bd93793556764e79cbf7606d4448e935ad5ba53eb9ee6849550d4cba7f 6be3a52cd5c077794a03f0596d1cbf3aee2635d268b03b476f6a2eaeb87d411c	
Direcciones IPs C2	2[.]56[.]59[.]42 2[.]56[.]56[.]126 103[.]246[.]144[.]29 148[.]251[.]234[.]83 148[.]251[.]234[.]93 151[.]115[.]10[.]1 160[.]153[.]249[.]159 185[.]112[.]83[.]8 185[.]215[.]113[.]208 185[.]215[.]113[.]29 185[.]215[.]113[.]114 193[.]150[.]103[.]37 194[.]180[.]174[.]41 212[.]193[.]30[.]29 212[.]193[.]30[.]45 23[.]88[.]114[.]184 37[.]230[.]138[.]66 45[.]129[.]99[.]59	45[.]144[.]225[.]57 45[.]147[.]196[.]146 85[.]209[.]157[.]230 91[.]219[.]236[.]18 91[.]224[.]22[.]193 94[.]140[.]115[.]160 140[.]82[.]121[.]3 149[.]28[.]78[.]238 156[.]67[.]74[.]197 162[.]0[.]210[.]44 185[.]112[.]83[.]49 185[.]204[.]109[.]248 192[.]243[.]59[.]13 91[.]243[.]32[.]73 37[.]0[.]8[.]88 193[].142[.]59[.]119 136[.]144[.]41[.]201
Dominios	disandillanne[.]xyz jainestaynor[.]xyz htagzdownload[.]pw isns[.]net gianninidesign[.]com krupskaya[.]com m-onetrading-jp[.]com majul[.]com thuocnam[.]tk psoeiras[.]net www[.]thechiropractor[.]vegas www[.]anderherzog[.]info www[.]aqueouso[.]com www[.]daniela[.]red www[.]hempzone-cosmetic[.]com www[.]rszkjx-vps-hosting[.]website	c9d0e790b353537889bd47a364f5acff4 3c11f244[.]xyz api3[.]testrequest[.]info stewei[.]s3[.]pl-waw[.]scw[.]cloud ad-postback[.]biz ad-storage[.]biz vataeagene[.]xyz b[.]dxyzgame[.]com b[.]xyzgameb[.]com c[.]xyzgamec[.]com d[.]gogamed[.]com capitalfm997[.]com curtainshare[.]su datingmart[.]me eurekabike[.]com freshstart-upsolutions[.]me

	EC-2021-032	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-febrero-2022	**Malware RedLine Stealer**	V 1.1

Propiedades Básicas		
	www[.]learnavstandards[.]com www[.]collabasia[.]xyz www[.]altshiftdel[.]com www[.]kasikormbank[.]com gonajah[.]com fastklick[.]biz stylesheet[.]faseaegasdfase[.]com tg8[.]cllgxx[.]com 360devtracking[.]com baanrabiengfah[.]com	glitterandsparkle[.]net jangeamele[.]xyz jggrmmojcc[.]com online-stock-solutions[.]com service-domain[.]xyz webdeadshare24[.]me gp[.]gamebuy768[.]com ip[.]sexygame[.]jp source3[.]boys4dayz[.]com licensechecklive[.]xyz

Tabla 1. IOC malware RedLine
Fuente: GitHub

VII. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Monitorear continuamente comportamientos inusuales de puntos finales, como solicitudes a dominios de baja reputación, puede indicar un compromiso temprano.
- Evitar abrir enlaces y archivos adjuntos de correo electrónico que no sean de confianza sin verificar su autenticidad.
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Utilice contraseñas seguras y aplique la autenticación multifactor siempre que sea posible.
- Tener actualizado y utilizar, un software anti-virus.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

VIII. REFERENCIAS:

CronUp. (29 de 12 de 2021). *GitHub*. Obtenido de GitHub: https://github.com/CronUp/Malware-IOCs/blob/main/2021-12-29_Malvertising2RedLine

CRONUP. (15 de 02 de 2022). *CRONUP Ciberseguridad*. Obtenido de CRONUP Ciberseguridad: https://www.cronup.com/top-malware-series-redline-stealer/

Cyberint. (18 de 8 de 2021). *Cyberint*. Obtenido de Cyberint: https://cyberint.com/blog/research/redline-stealer/

Cyble. (12 de 08 de 2021). *Cyble Research Lab*. Obtenido de Cyble Research Lab: https://blog.cyble.com/2021/08/12/a-deep-dive-analysis-of-redline-stealer-malware/

Fernández, L. (27 de 01 de 2020). *RedesZone*. Obtenido de RedesZone: https://www.redeszone.net/tutoriales/seguridad/malware-as-a-service-maas-que-es/

Malpedia. (s.f.). *Malpedia*. Obtenido de Malpedia: https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

Pedro, T. (17 de 11 de 2021). *INFOSEC*. Obtenido de INFOSEC: https://resources.infosecinstitute.com/topic/redline-stealer-malware-full-analysis/