



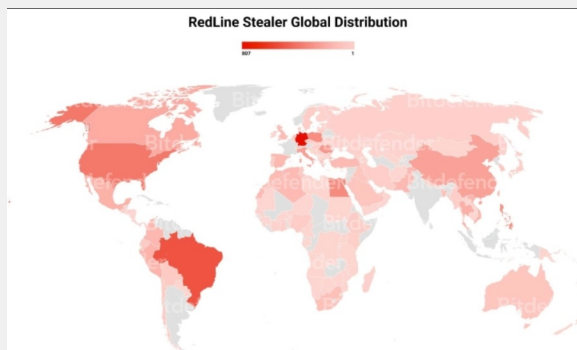
Guatemala • El Salvador • Honduras • R. Dominicana

RedLine Stealer Malware

Nueva campaña RIG Exploit Kit que infecta las PC de las víctimas con RedLine Stealer

Cuando se ejecuta, RedLine Stealer realiza un reconocimiento contra el sistema de destino (incluido el nombre de usuario, el hardware, los navegadores instalados, el software antivirus) y luego filtra los datos (incluidas las contraseñas, las tarjetas de crédito guardadas, las billeteras criptográficas, los inicios de sesión de VPN) a un mando y control remoto. servidor, dijo Bitdefender en un nuevo informe compartido con The Hacker News.

La mayoría de los contagios se localizan en Brasil y Alemania, seguidos de Estados Unidos, Egipto, Canadá, China y Polonia, entre otros.



RedLine Stealer usa múltiples vectores de ataque para llegar a la mayor cantidad de máquinas posibles. Por lo general, los atacantes no llevan a cabo métodos novedosos, sino que simplemente aplican una técnica ya clásica en los malwares de bajo y alto nivel, el uso de la ingeniería social mediante correo electrónico. Los cuales invitan a la víctima en realizar una acción. Ya sea entrando a un enlace random y descargando un archivo o incluso en los mismos correos vienen con un adjunto. También se ha llegado a registrar falsas páginas de softwares, en sitios webs de cracks y en anuncios fraudulentos en Google, técnicas de spam llamadas Malvertising.

Algunos de los adjuntos más comunes con su payload son los siguientes:

- Archivos de Ofimática
- PDF
- RAR y ZIP
- Archivos ejecutables
- JavaScript

ALSO KNOWN AS

RedLine

Global rank

7

Week rank

↑2

Month rank

↑1

IOCs

25274

LAST SEEN AT

2 May, 2022	Malicious activity	ESCAPE FROM TARKOV HACK.zip	trojan	rat	redline
2 May, 2022	Malicious activity	https://1drv.ms/u/s!AoOVwoUqdvaTtwjMwvD3rSjRM	trojan	rat	redline
2 May, 2022	Malicious activity	https://www30.zippyshare.com/d/17jRAiev/27590/MetaMaskChecker.zip	trojan	rat	redline
2 May, 2022	Malicious activity	TonerRecover.zip	trojan	rat	redline
2 May, 2022	Malicious activity	https://1drv.ms/u/s!AoLfb11dKRZab7Cr33aCCtljT4w	trojan	rat	redline
2 May, 2022	Malicious activity	https://telegra.ph/New-CheckRa1n-Windows-Mac-OS-04-25	trojan	rat	redline
2 May, 2022	Malicious activity	https://1drv.ms/u/s!AidHYER3j5Hbqd0W5GS4IEPexs	trojan	rat	redline
2 May, 2022	Malicious activity	https://googlenws.ru/chlen.exe	trojan	rat	redline
2 May, 2022	Malicious activity	https://googlenws.ru/hui.exe	trojan	rat	redline
2 May, 2022	Malicious activity	https://1drv.ms/u/s!Aj66bdzTL-5EaQkVzxt2EiB1V0	trojan	rat	redline



Nuestras Recomendaciones

La mejor manera de proteger su organización o dispositivo de RedLine es tener cuidado con los archivos y enlaces sospechosos que ingresan a su correo electrónico. Su personal debe ser consciente de que incluso las fuentes confiables pueden provocar una infección y el robo de contraseñas u otras credenciales.

Las recomendaciones para evitar o minimizar el riesgo de una infección de Malware son:

- Contar con software antivirus actualizado y sus licencias al día
- Mostrar las extensiones de los archivos que por defecto vienen ocultas, para evitar abrir archivos maliciosos
- Mantener los equipos actualizados, tanto el Sistema Operativo como aplicaciones que se utilicen
- No abrir archivos adjunto ni enlaces en un correo si no conoces a la persona que lo envió
- Mantener monitoreo en toda actividad sospechosa que se detecte en nuestra red
- Capacitar al personal de la empresa para que sea consciente de los riesgos a los que estamos expuestos en Internet

Para un mejor asesoramiento y prevención de amenazas pueden avocarse a nosotros escribiendo a : info@develsecurity.com / soc@develsecurity.com

/ soporte@develsecurity.com.

¡ Con gusto le atenderemos !



GUATEMALA

PBX: + (502) 2307 5700
7ma. avenida 5-45, edificio XPO1 zona 4
nivel 9, Ciudad de Guatemala

EL SALVADOR

PBX: + (503) 2566 5320
Final 105 Av. norte calle Arturo Ambrogi
No. 440 colonia Escalón, San Salvador

HONDURAS

PBX: + (504) 2283 5904
Blv. Morazán, Condominios Centro Morazán
Torre 2, nivel 18 oficina 21804, Honduras

REPÚBLICA DOMINICANA

PBX: +1 (809) 335 4793
Santo Domingo John F. Kennedy 7,
Buenaventura Freites, 10601.T