Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RomCom se distribuye haciéndose pasar por aplicaciones popularmente conocidas.

04/Noviembre/2022

Contenido

INTRODUCCIÓN

El actor de amenazas detrás de RomCom RAT (troyano de acceso remoto) ha actualizado su vector de ataque y ahora está abusando de marcas de software conocidas para su distribución.

APLICATIVOS PIRATA DISTRIBUYEN MALWARE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_11_04
Clasificación de alerta:	Amenaza
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/04/2022
Es día cero (0 day):	No

RESUMEN

En una nueva campaña descubierta por BlackBerry , se encontró a los actores de amenazas RomCom creando sitios web que clonan portales de descarga oficiales para SolarWinds Network Performance Monitor (NPM), el administrador de contraseñas KeePass y PDF Reader Pro, esencialmente disfrazando el malware como programas legítimos.

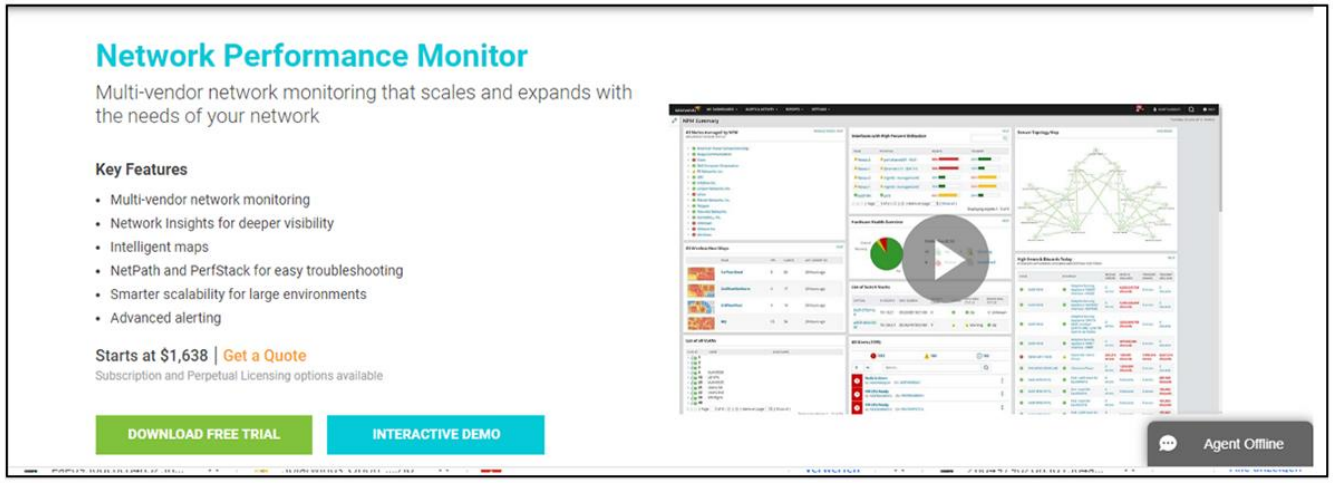
Además, la Unidad 42 descubrió que los atacantes crearon un sitio que se hace pasar por el software Veeam Backup and Recovery.

Además de copiar el código HTML para reproducir los sitios originales, los piratas informáticos también registraron dominios 'parecidos' con errores tipográficos para agregar más autenticidad al sitio malicioso.

BlackBerry detectó previamente el malware RomCom utilizado en ataques contra instituciones militares en Ucrania .

Hacerse pasar por software legítimo

El sitio web que se hace pasar por SolarWinds NPM ofrece una versión con troyano de la prueba gratuita e incluso enlaces a un formulario de registro de SolarWinds real que, si la víctima completa, lleva a ser contactado por un agente de atención al cliente real.



El sitio web falsificado de Solarwinds (BlackBerry)

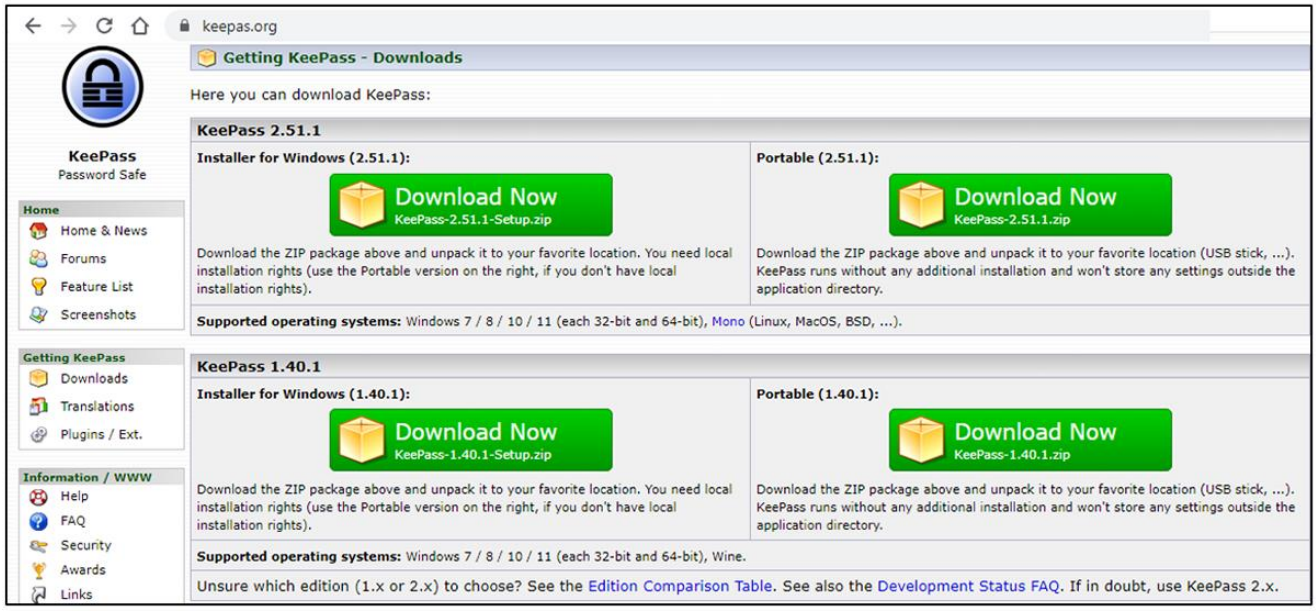
Sin embargo, la aplicación descargada se modificó para incluir una DLL maliciosa que descarga y ejecuta una copia de RomCom RAT desde la carpeta "C:\Users\user\AppData\Local\Temp\winver.dll".

Name	Date modified	Type	Size
config	04/08/2022 11:04	File folder	
help	04/08/2022 11:04	File folder	
installation	04/08/2022 11:27	File folder	
logs	14/07/2022 09:15	File folder	
mapistub.dll	14/06/2022 21:53	Application extens...	156 KB
mfcore.dll	13/07/2022 01:41	Application extens...	4,688 KB
mfh264enc.dll	13/07/2022 01:41	Application extens...	568 KB
mprapi.dll	14/06/2022 21:53	Application extens...	514 KB
MSMPEG2ENC.DLL	14/06/2022 21:53	Application extens...	922 KB
scansetting.dat	13/07/2022 01:41	DAT File	291 KB
SearchFolder.dll	14/06/2022 21:53	Application extens...	403 KB
sfc.dll	14/06/2022 21:53	Application extens...	13 KB
Solarwinds-Orion-NPM-Eval.exe	04/08/2022 11:26	Application	109,283 KB
spacebridge.dll	13/07/2022 01:41	Application extens...	177 KB
sti.dat	13/07/2022 01:41	DAT File	325 KB
tquery.dll	13/07/2022 01:41	Application extens...	3,230 KB
Windows.Media.dll	14/06/2022 21:53	Application extens...	7,374 KB
Windows.UI.Core.TextInput.dll	13/07/2022 01:41	Application extens...	1,016 KB
WordBreakers.dll	13/07/2022 01:41	Application extens...	43 KB
WSManMigrationPlugin.dll	13/07/2022 01:41	Application extens...	87 KB
WsmAuto.dll	13/07/2022 01:41	Application extens...	176 KB

Contenido del ZIP de Solarwinds descargado (BlackBerry)

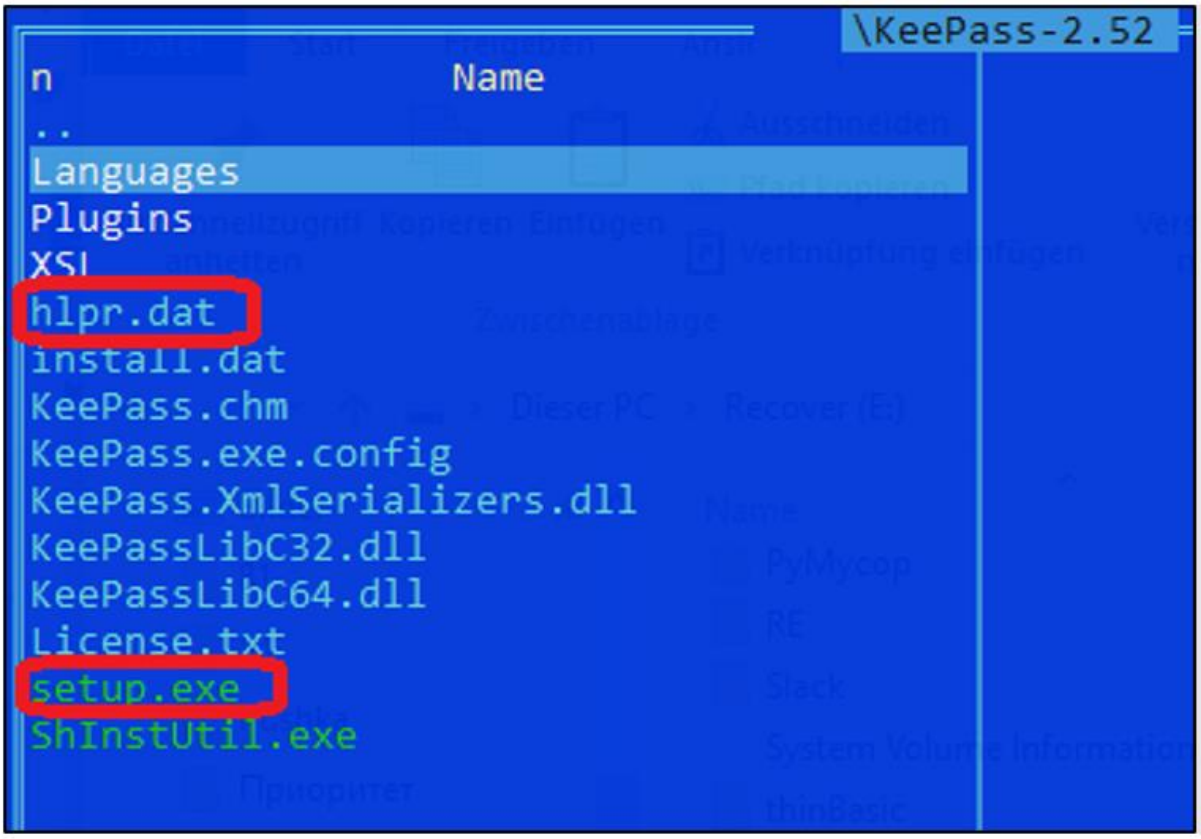
Curiosamente, el ejecutable descargado ("Solarwinds-Orion-NPM-Eval.exe") está firmado con el mismo certificado digital que los operadores de RAT utilizaron en la campaña de Ucrania, que muestra al propietario como "Wechapaisch Consulting & Construction Limited".

En el caso del sitio clonado para KeePass, que BlackBerry descubrió recién el 1 de noviembre de 2022, los actores de la amenaza están distribuyendo un archivo llamado "KeePass-2.52.zip".



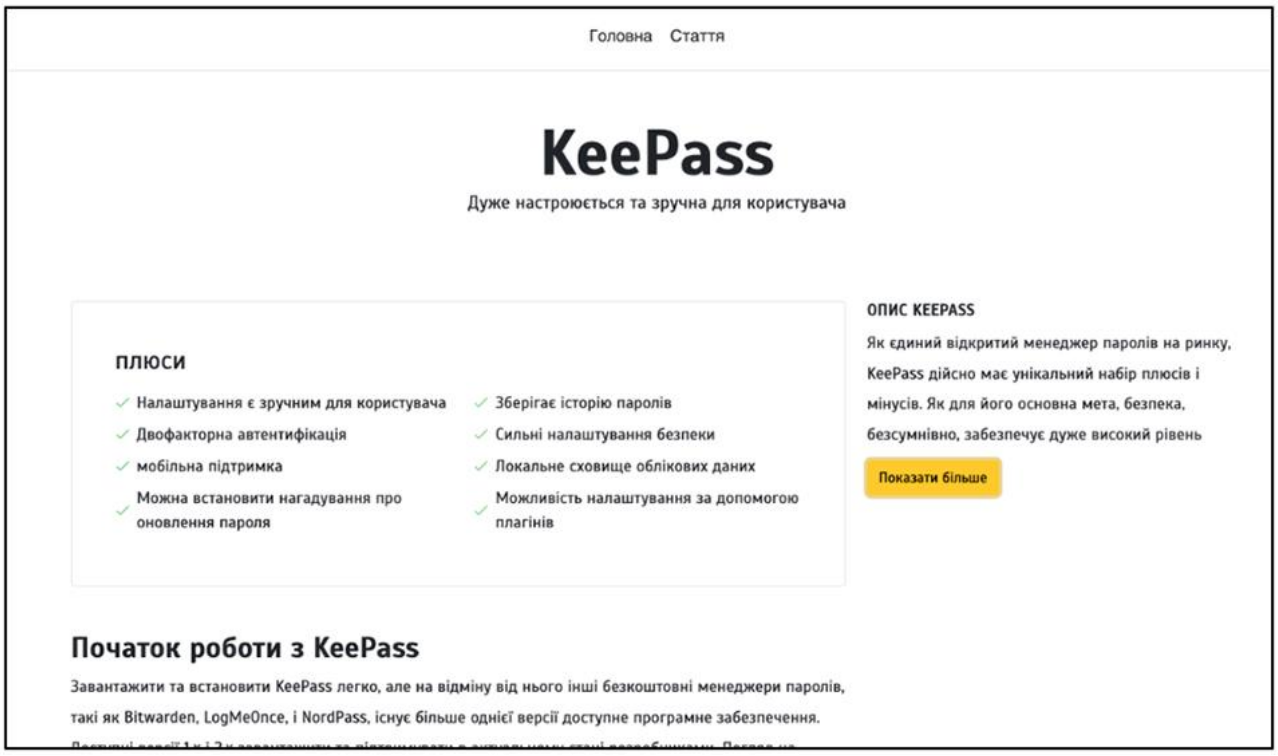
Sitio web falso de KeePass que promociona RomCom RAT (BlackBerry)

El archivo ZIP contiene varios archivos, incluido "hlpr.dat", que es el cuentagotas de RomCom RAT, y "setup.exe", que inicia el cuentagotas. Setup.exe es lo que se espera que el usuario ejecute manualmente después de descargar el archivo.



Contenido del archivo ZIP descargado (BlackBerry)

Los investigadores de BlackBerry también localizaron un segundo sitio KeePass falsificado y un sitio PDF Reader Pro, ambos en ucraniano.



Otro sitio falso de KeePass dirigido a ucranianos (BlackBerry)

Esto indica que, si bien RomCom todavía está apuntando a Ucrania, también han cambiado los objetivos para incluir a los usuarios de habla inglesa.

No está claro en este momento cómo los actores de amenazas están atrayendo a las víctimas potenciales a los sitios, pero podría ser a través de phishing, envenenamiento de SEO o publicaciones en foros/redes sociales.

Sin atribución

En agosto de 2022, la Unidad 42 de Palo Alto Networks asoció RomCom RAT con un afiliado de Cuba Ransomware llamado 'Tropical Scorpius', ya que este fue el primer actor en emplearlo.

RomCom RAT era un malware entonces desconocido que admitía comunicaciones basadas en ICMP y ofrecía a los operadores diez comandos para acciones de archivos, generación y falsificación de procesos, exfiltración de datos y lanzamiento de un shell inverso.

El informe anterior de BlackBerry sobre RomCom RAT argumentó que no había evidencia concreta que apuntara la operación a ningún actor de amenazas conocido.

El nuevo informe menciona Cuba Ransomware e Industrial Spy como potencialmente conectados a esta operación; sin embargo, la motivación detrás de los operadores de RomCom aún no está clara.

Recomendaciones

- Agregar los Indicadores de compromiso en sus consolas AV, Firewall, Proxy. Para garantizar una cobertura adecuada ante esta amenaza.

- Validar que solo las cuentas con nivel de administrador en dominio puedan instalar software en sus equipos.

- Se recomienda de forma periódica hacer un escaneo profundo con su Antivirus a todos sus equipos.

Indicadores de Compromiso

https://github.com/develgroup/SOC_IOCs/tree/main/20221104_01_RomCom

Noticia Completa

https://devel.group/blog/romcom-se-distribuye-mediante-aplicaciones-popularmente-conocidas/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente