bafing

BOLETÍN
De Inteligencia de Ciberseguridad

Grupo NCC: Los ataques DDoS aumentaron en octubre mientras que los ataques de ransomware cayeron

El último informe de NCC Group muestra un aumento en los ataques de denegación de servicio distribuido (DDoS) el mes pasado. Mientras tanto, los ataques de ransomware se redujeron ligeramente.

Octubre vio la mayor cantidad de ataques DDoS este año, con un aumento del 14 % desde septiembre, a 2090 ataques. El crecimiento monumental advierte que la amenaza de DDoS va en aumento. Los ataques de ransomware disminuyeron un 7 % en octubre con respecto al mes anterior.

La industria (34 %) y los productos cíclicos de consumo (18 %) siguen siendo los sectores más atacados por piratas informáticos malintencionados. El cuidado de la salud (10%) reemplazó a la tecnología (8,5%) como el tercer sector más objetivo.

Actores de amenazas más frecuentes

Lockbit 3.0, Black Basta y BlackCat siguen siendo los actores de amenazas más frecuentes. Octubre fue el décimo mes en el que Lockbit (Lockbit 2.0/Lockbit 3.0) ha sido el más activo. Las cifras de ataques de ransomware de este mes son la mitad de las registradas en octubre del año pasado. Por lo tanto, es poco probable que el número total de ataques este año alcance las mismas alturas que en 2021.

Muchas motivaciones para los ataques DDoS

Los actores de amenazas pueden usar ataques DDoS para satisfacer varias motivaciones, dijo Hirst. Esos incluyen ganancias financieras para los grupos del

crimen organizado y actos de protesta para los hacktivistas. Además, ocasionalmente se trata de sabotaje cibernético a través de la interrupción operativa de los estados-nación.

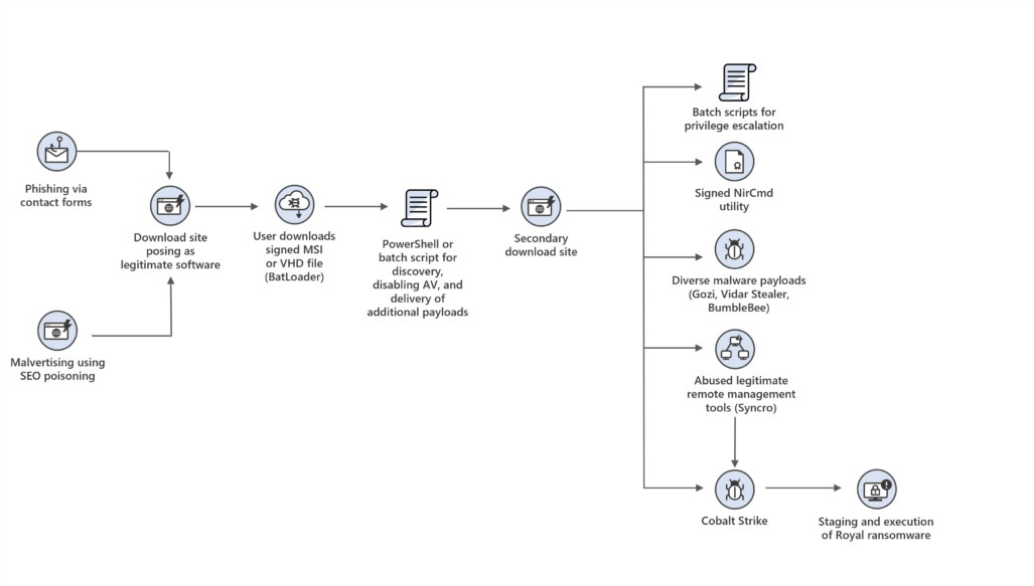
“Es posible que el aumento de los ataques DDoS esté relacionado con el cambio de suerte de las fuerzas rusas en Ucrania”, dijo Jack Hirst es consultor de inteligencia de amenazas en NCC Group. “Los ataques DDoS se utilizan como una herramienta eficaz de interrupción y, a menudo, se utilizan junto con los objetivos rusos/contra organizaciones y naciones que se oponen a los esfuerzos de Rusia por conquistar Ucrania. El monitoreo continuo de los números de DDoS combinado con el análisis a través de la lente del panorama cibernético en su conjunto (ransomware, fugas de datos, ataques de malware de limpieza) será necesario para proporcionar una evaluación más confiable”.

Continúa leyendo aquí

Fuente: ChannerFutures

DEV-0569 encuentra nuevas formas de entregar Royal ransomware, varias cargas útiles

La actividad reciente del actor de amenazas que Microsoft rastrea como DEV-0569, conocida por distribuir varias cargas útiles, ha llevado al uso del ransomware Royal, que surgió por primera vez en septiembre de 2022 y está siendo distribuida por múltiples actores de amenazas.



DEV-0569 se basa ciertamente en publicidad maliciosa, enlaces de phishing que apuntan a un descargador de malware que se hace pasar por instaladores de software o actualizaciones incrustadas en correos electrónicos no deseados, páginas de foros falsos y comentarios de blogs. En los últimos meses, los investigadores de seguridad de Microsoft observaron los siguientes ajustes en los métodos de entrega del grupo:

1. Uso de formularios de contacto en sitios

2. Alojar archivos de instalación falsos en sitios de descarga de

3. Expansión de su técnica de publicidad maliciosa

web de organizaciones objetivo para intentar entregar enlaces de phishing.

software de aspecto legítimo y repositorios legítimos para que las descargas maliciosas parezcan auténticas.

mediante Google Ads en una de sus campañas, mezclándose efectivamente con el tráfico publicitario normal.

Es probable que DEV-0569 continúe dependiendo de la publicidad maliciosa y el phishing para entregar cargas útiles de malware. Soluciones como la protección de red y Microsoft Defender SmartScreen pueden ayudar a frustrar el acceso a enlaces maliciosos. Microsoft Defender para Office 365 ayuda a protegerse contra el phishing al inspeccionar el cuerpo del correo electrónico y la URL en busca de patrones conocidos.

Dado que el esquema de phishing de DEV-0569 abusa de los servicios legítimos, las organizaciones también pueden aprovechar las reglas de flujo de correo para capturar palabras clave sospechosas o revisar amplias excepciones, como aquellas relacionadas con rangos de IP y listas permitidas en cuanto a dominio. Habilitar vínculos seguros para correos electrónicos, equipos de Microsoft y aplicaciones de Office también puede ayudar a abordar esta amenaza.

Continúa leyendo aquí

Fuente: Microsoft

Vulnerabilidad de Path Traversal (CVE-2022-0902) en controladores remotos y computadores de caudal ABB

FortiGuard Labs tiene conocimiento de una vulnerabilidad de cruce de ruta (CVE-2022-0902) que afecta a los controladores remotos y a las computadoras de flujo ABB Totalflow, ampliamente utilizados por las empresas de servicios públicos de petróleo y gas.

Esto es importante porque la nueva vulnerabilidad (CVE-2022-0902) afecta a los controladores remotos y a las computadoras de flujo TotalFlow de ABB, ampliamente utilizados por las empresas de servicios públicos de petróleo y gas. ABB TotalFlow se utiliza para calcular el volumen y los caudales de petróleo y gas, y también se utiliza para la facturación y otros fines.

Al explotar con éxito la vulnerabilidad, un atacante puede obstaculizar la capacidad de las compañías de petróleo y gas afectadas para medir correctamente el flujo de petróleo y gas, lo que puede generar problemas de seguridad e interrupción del negocio.

CVE-2022-0902 es una vulnerabilidad de cruce de ruta (CVE-2022-0902) en las computadoras de flujo y controladores remotos ABB TotalFlow. La vulnerabilidad permite que un atacante obtenga acceso a directorios restringidos en las computadoras de flujo de ABB, lo que lleva a la ejecución de código arbitrario en

un nodo del sistema afectado.

Según el aviso emitido por ABB, los siguientes productos se ven afectados por la vulnerabilidad:

• RMC-100
• RMC100L ITE
• XIO
• XFCG5
• XRCG5
• uFLOG5
• UDC

Continúa leyendo aquí

Fuente: FortiGuard

NanoCore: un malware del tipo RAT muy utilizado espiar a las víctimas

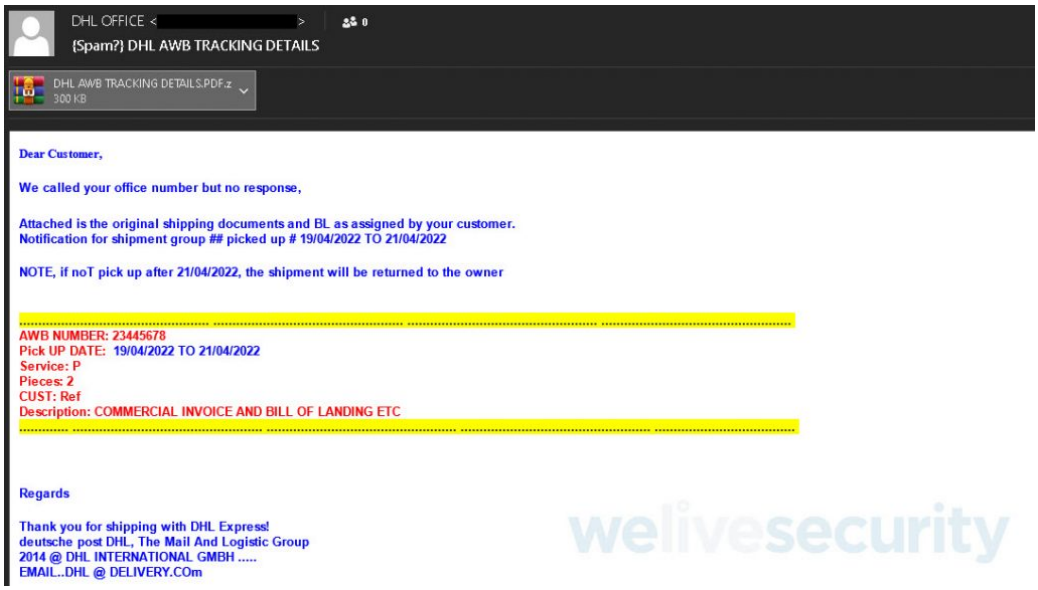
Se analizaron las principales características de NanoCore, un troyano de acceso remoto activo desde 2013 que sigue siendo muy utilizado por cibercriminales en la actualidad.

NanoCore es un malware perteneciente a la familia de los RAT (Remote Access Trojan), activo desde el 2013, que cuenta con diferentes características que le permiten a un cibercriminal realizar distintas acciones maliciosas sobre la máquina víctima. Principalmente, espiar en su equipo y robar información. Según un informe la Agencia Nacional de Ciberseguridad de los Estados Unidos (CISA, por sus siglas en inglés), NanoCore es una de las variantes de malware qué más actividad registró en 2021.

> Escrito con el framework Microsoft .NET, NanoCore solía ser comercializado en foros clandestinos a partir de los 25 dólares. Las principales características de este malware son su capacidad para robar archivos de la máquina de la víctima, registrar las pulsaciones del teclado, robar credenciales, grabar audio y video, entre otras.

A pesar de que hoy en día es más amplia la oferta de códigos maliciosos que son

comercializadas en foros clandestinos, NanoCore sigue siendo un malware con mucha actividad. En parte esto se debe a su bajo costo, las capacidades que ofrece, así como también a la circulación de versiones crackeadas, lo que permitió que cibercriminales con pocos o ningún conocimiento en el desarrollo de códigos maliciosos tengan acceso a un malware para llevar adelante sus actividades delictivas.



NanoCore suele propagarse por medio de correos electrónicos de phishing. Generalmente oculto como un archivo adjunto o una URL que lleva a la víctima a la descarga de este malware.

Para aumentar la probabilidad de que una víctima abra y ejecute el contenido de alguno de estos correos, los cibercriminales utilizan distintas temáticas. Algunas de estas están relacionadas con facturas de órdenes de compra falsas, solicitudes de presupuesto falsas, entre otras. En algunos casos, se hacen pasar por empresas legítimas de logística o de envío de paquetería utilizando incluso imágenes de estas empresas en los correos.

Continúa leyendo aquí

Fuente: WeLiveSecurity by ESET

Vulnerabilidad sin doble atributo de clase de Microsoft Office

Cisco Talos descubrió recientemente una vulnerabilidad sin doble atributo de clase en Microsoft Office.

Microsoft Office es un conjunto de herramientas utilizadas para la productividad tanto en un entorno corporativo como por parte de los usuarios finales. Ofrece una gama de herramientas que se pueden utilizar para diversos fines. Como Excel para hojas de cálculo, Word para edición de documentos, Outlook para correo electrónico, PowerPoint para presentaciones, etc.

Talos ha identificado una vulnerabilidad doblemente libre en Microsoft Office Excel. TALOS-2022-1591 (CVE-2022-41106) permite a un atacante proporcionar un archivo malicioso para desencadenar una posible ejecución de código arbitrario.
Cisco Talos trabajó con Microsoft para garantizar que este problema se resolviera y que hubiera una actualización disponible para los clientes afectados, todo en cumplimiento de la política de divulgación de vulnerabilidades de Cisco.

Se recomienda a los usuarios que actualicen estos productos afectados lo antes posible: Microsoft Office Excel 2019 x86, versión 2207 compilación 15427.20210 y versión 2202 compilación 14931.20660. Talos probó y confirmó que estas versiones de Office podrían ser explotadas por estas vulnerabilidades.

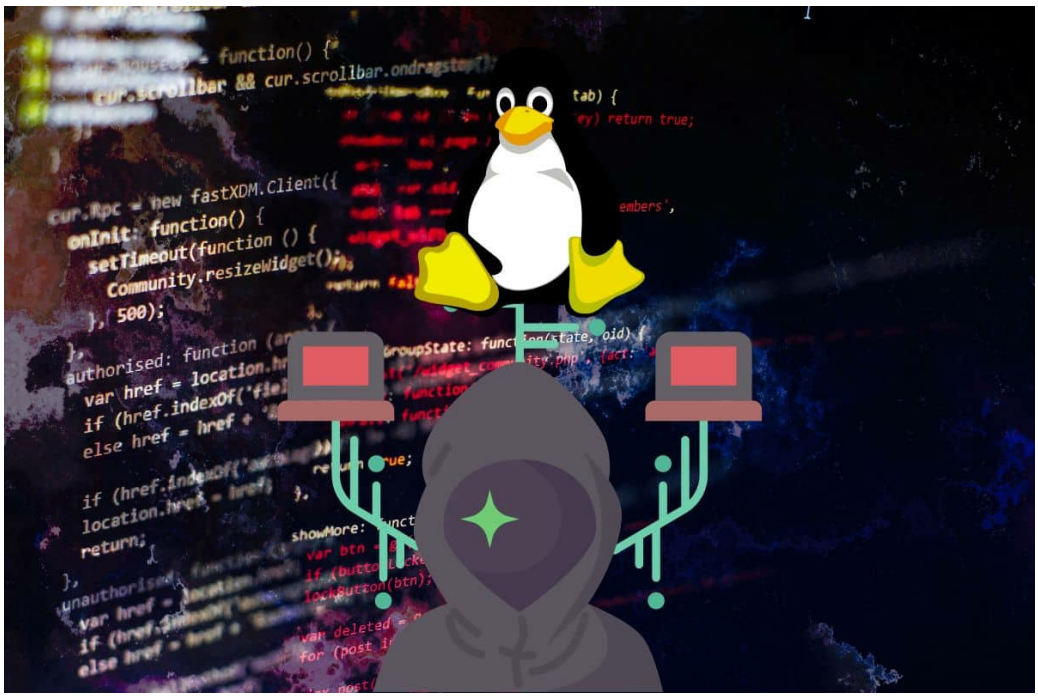
Las siguientes reglas de Snort detectarán intentos de explotación contra estas vulnerabilidades: 60500-60501. Es posible que se publiquen reglas adicionales en el futuro y las reglas actuales están sujetas a cambios, en espera de información adicional sobre vulnerabilidades. Para obtener la información más actualizada sobre las reglas, consulte su Firepower Management Center o Snort.org.

Continúa leyendo aquí

Fuente: Talos by Cisco

Nueva campaña de RapperBot: Fortinet investiga su nuevo propósito

Este artículo analiza las diferencias observadas en esta campaña y su relación con el RapperBot anterior y campañas similares en el pasado.



FortiGuard Labs se encontró con esta campaña buscando muestras utilizando la ID de bot única utilizada por RapperBot para comunicarse con su servidor de comando y control (C2), como se informó en el artículo anterior.

Pero una vez que analizamos estas nuevas muestras, observamos una diferencia significativa entre ellas y la campaña anterior. De hecho, resulta que esta campaña se

parece menos a RapperBot que a una campaña anterior que apareció en febrero y luego desapareció misteriosamente a mediados de abril. Otras campañas relacionadas descubiertas durante esta investigación se detallan más adelante en este artículo.

> Según las similitudes innegables entre esta nueva campaña y la campaña RapperBot informada anteriormente, es muy probable que estén siendo operadas por un solo actor de amenazas o por diferentes actores de amenazas con acceso a un código fuente base compartido de forma privada.
>
> A diferencia de la campaña anterior de RapperBot, esta nueva campaña tiene una clara motivación para comprometer tantos dispositivos IoT como sea posible para construir una botnet DDoS.
>
> Aunque esta nueva campaña ha evolucionado significativamente con respecto a las campañas anteriores, la mitigación sigue siendo la misma: establecer contraseñas seguras para todos los dispositivos conectados a Internet.
> FortiGuard Labs continuará monitoreando el desarrollo de RapperBot.

Continúa leyendo aquí

Fuente: Fortinet

Contáctenos

Central: +511 2259900 anexo 110
Equipo de Marketing: igrandez@bafing.com o al +51 969454618
Command Center y SOC: helpdesk@bafing.com o al +51 971500877

www.bafing.com

Facebook **Twitter** **LinkedIn**

Síguenos Síguenos Síguenos

Acerca de Bafing

Somos una empresa con más de 27 años de experiencia en el mercado de Tecnologías que ofrece soluciones muy especializadas en Ciberseguridad, eHealth y Smart Buildings.

El presente documento es una comunicación de carácter general hecha exclusivamente con propósitos informativos. Usted recibe este newsletter tras haberse suscrito al mismo. Si no desea continuar recibiéndolo, por favor escribir a bdigital@bafing.com

Bafing S.A.C. | Av. Del Parque Sur 560, San Borja, Lima, LIMA 15036 Perú

Cancelar suscripción pbisso@bafing.com

Aviso de datos de Constant Contact

Enviado porbdigital@bafing.comalimentado por

Constant Contact

Try email marketing for free today!