PARASITE HTTP RAT

2 de Agosto del 2018
CONFIDENCIAL

MALWARE PARASITE HTTP RAT

NIVEL DE ALERTA

Crítica
Sin CVE asociado a la fecha

PRODUCTOS AFECTADOS

A continuación, se relacionan los sistemas operativos que posiblemente son vulnerables:

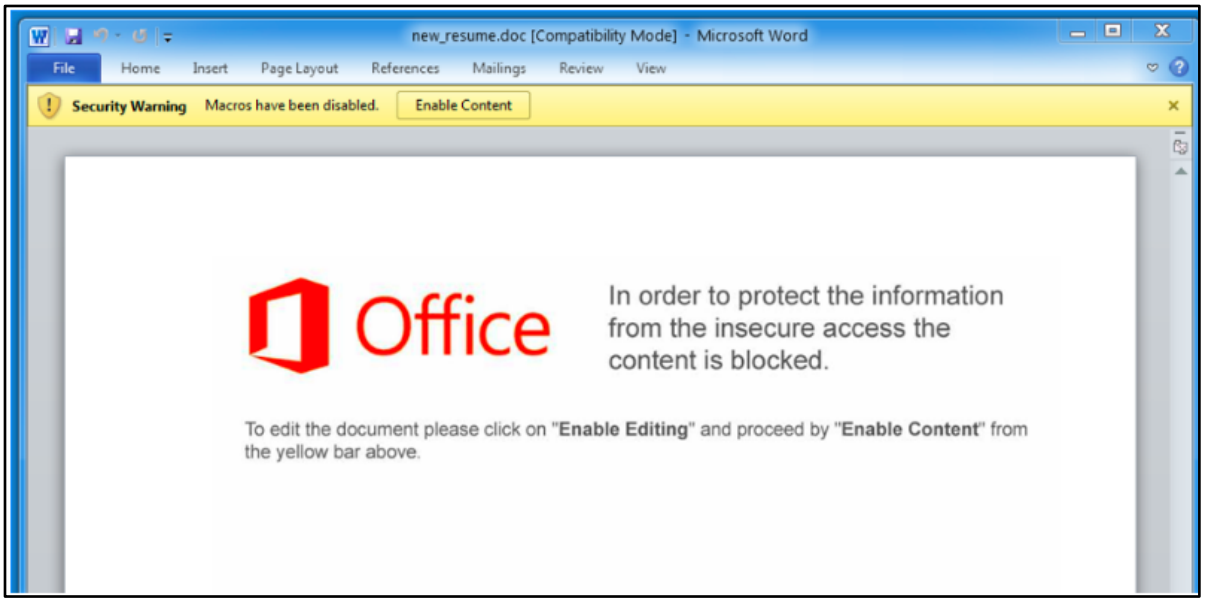
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

DESCRIPCIÓN DEL MALWARE

En 16 de Julio, se observó una pequeña campaña que parecía aprovechar las listas de distribución de recursos humanos para la propagación del malware. El cuerpo del mensaje de los correos electrónicos contenían curriculums y temas relacionados con aplicación a ofertas laborales; dentro de estos, se encontraban archivos adjuntos de Microsoft Word con nombres como los siguientes:

- my_cv.doc
- resume_.doc
- cvnew.doc
- cv.doc
- new_resume.doc

Los documentos contenían macros que, de estar habilitados, descargarían el malware Parasite HTTP desde un sitio remoto.



Parasite HTTP es una herramienta de administración remota modular codificada escrita en C que no tiene dependencias, excepto el sistema operativo en sí; esta tiene la habilidad de controlar una gran cantidad de computadoras desde una ubicación remota.

El malware al ser de naturaleza modular, permite a los atacantes agregar nuevas capacidades a medida que estén disponibles o descargar módulos adicionales después de la infección.

Hasta la fecha, solo se ha observado Parasite HTTP en una campaña pequeña de correo electrónico con destinatarios previstos principalmente en las industrias de tecnología de la información, atención médica y venta al por menor.

Características del Malware

- Sin dependencias (codificado en C)
- Pequeño tamaño de stub (~ 49kb sin comprimir, ~ 23kb comprimido)
- Cadenas cifradas
- Anular los ganchos Ring3
- Panel seguro de C&C escrito en PHP
- Cortafuegos
- Admite sistemas operativos Windows x86 y x64 (desde XP a 10)
- Constructor en línea vinculado a su dominio ó dominios (Build bot bin en cualquier momento con la configuración que desee)

- Comunicación cifrada con el panel C&C (Opcional: SSL con certificado autofirmado)
- Múltiples dominios de copia de seguridad
- Persistencia en todo el sistema (solo procesadores x86)
- Inyección al proceso del sistema en la lista blanca
- Inicio oculto
- Anti emulación
- Anti-depuración
- Bajo uso de recursos
- Descargar y ejecutar (admite enlaces HTTP y HTTPS)

Parasite HTTP proporciona numerosas técnicas avanzadas utilizadas para evitar la detección en entornos aislados y sistemas antimalware. Para los consumidores y organizaciones esto representa la última escalada en una carrera de armamentos de malware en curso que se extiende incluso a productos de malware como Parasite. Si bien actualmente solo se ha observado Parasite HTTP en una campaña pequeña, se espera ver que las características como las que se usan en Parasite continúen propagándose a través de otras variantes de malware.

INDICADORES DE COMPROMISO (IoC)

A continuación, se relacionan los indicadores de compromiso que a la fecha se han identificado:

Archivo (SHA256)	b52706530d7b56599834615357e8bbc1f5bed669001c06830029784eb4669518
	6479a901a17830de31153cb0c9f0f7e8bb9a6c00747423adc4d5ca1b347268dc
Dominios	befrodet.top
	dboxhost.tk
	jekoslo.space
	xetrodep.top
URL	http://dboxhost.tk/moz/bza.exe

RECOMENDACIONES

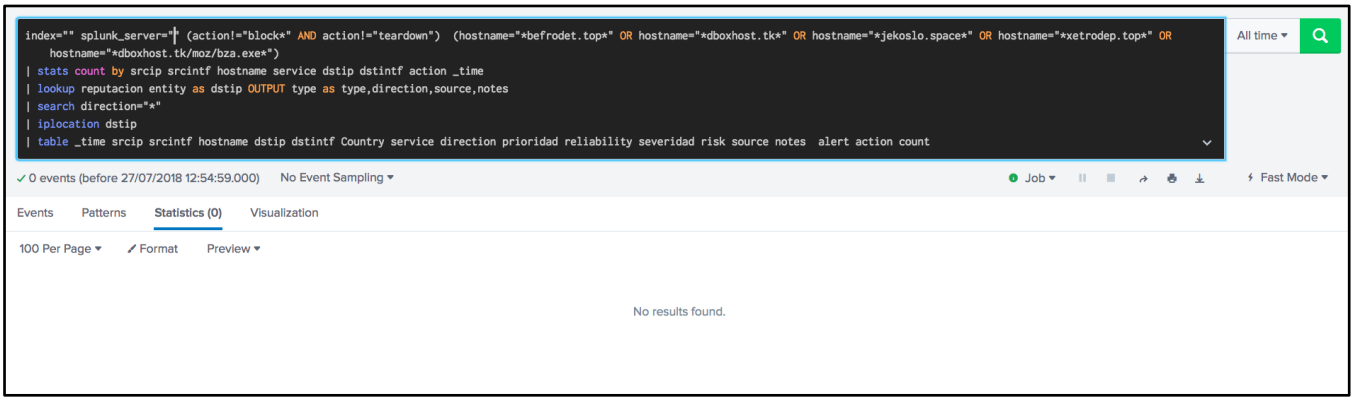
Desde el Centro de Seguridad y Vigilancia Digital, se realizan las siguientes recomendaciones:

1. Se recomienda generar el bloqueo de los dominios mencionados en los indicadores de compromiso en el Firewall; esto como contención para cerrar la comunicación entre el atacante y su objetivo (en caso de que la estación de trabajo se encuentre infectada y la organización aún no tenga conocimiento de esto).

2. Por otra parte, adjunto a este documento se comparte el listado de otros dominios, direcciones IP y hash de archivos identificados como maliciosos; agregue las direcciones IP y dominios mencionados del archivo adjunto a su lista de control de acceso de Botnets y Sitios maliciosos.

3. Generar fullscan periodico a las estaciones de trabajo de la organización; en la actualidad muchas de las casas de antivirus ya tienen identificado el malware con su respectiva firma.

Desde el CSVD (Centro de Seguridad y Vigilancia Digital), se realizó la creación de una alerta que se dispare cuando se identifique tráfico permitido a los dominios utilizados para la comunicación entre el atacante y el dispositivo.



REFERENCIAS

https://otx.alienvault.com/pulse/5b598f6e8440e04aaee17ac3

https://www.proofpoint.com/us/threat-insight/post/parasite-http-rat-cooks-stew-stealthy-tricks

https://twitter.com/search?q=Parasite%20HTTP%20RAT&src=typd&lang=es&lang=es&lang=es

A3SEC. ESPAÑA C/ Aravaca, 6 2º Piso 28040 Madrid, España T.+34 915330978	**A3SEC S.A.S** Carrera 49A # 94-76 Oficina 304 Edificio Empresarial Castellana Bogotá, COLOMBIA **T.**+57 1 3099533	**A3SEC USA** 1401 Brickell Ave #320 Miami, FL 33131, USA T. +1 786 556 90 32	**A3SEC. México** **Gral. Mariano Escobedo, 748 Piso 9 C.P. 11590 México D.F.** **T. +52 (55) 5980-3547**