HOJA DE INVESTIGACIÓN

FEBRERO 2021

EL MALWARE, MUTANDO JUNTO AL COVID-19

IMPACTO A NIVEL CRIPTOGRÁFICO

INVESTIGADORES: MSC. Arelis Guzmán/ Ing. Yakson Verenzuela

CONTACTO: aguzman@suscerte.gob.ve/ yverenzuela@suscerte.gob.ve

www.suscerte.gob.ve

DIRECCIÓN DE INVESTIGACIÓN, FORMACIÓN Y DESARROLLO

EFEMÉRIDES:

- ✓29 de febrero (1860) nace el “primer informático”, Herman Hollerith
- ✓28 de febrero (1989) México, el primer país Latinoamericano en tener acceso a Internet
- ✓27 de febrero (2008) Microsoft es la 1ra empresa multada por la ley antimonopolio
- ✓25 de febrero (2002) Kimberly Vanvaeck “Gigabyte” crea el primer virus en C#
- ✓24 de febrero (1955) Nace el genio de la manzana, nace Steve Jobs
- ✓23 de febrero (1998) Netscape anuncia el proyecto de código abierto “mozilla.org”
- ✓22 de febrero (2008) Hackers del cDc (Culto a la Vaca Muerta) lanzan "Goolag Scanner" [4]

FORMACIÓN:

- ✓Hacking Ético
- ✓CyberSeguridad IoT
- ✓Introducción a la Informática Forense
- ✓Seguridad de la Información y Teletrabajo
- ✓Programa Nacional de Protección de Niñas, Niños y Adolescentes en línea. NAEL

HOJA DE INVESTIGACIÓN

FEBRERO 2021

EL MALWARE, MUTANDO JUNTO AL COVID-19

IMPACTO A NIVEL CRIPTOGRÁFICO

INVESTIGADORES: MSC. Arelis Guzmán/ Ing. Yakson Verenzuela

CONTACTO: aguzman@suscerte.gob.ve/ yverenzuela@suscerte.gob.ve

www.suscerte.gob.ve

DIRECCIÓN DE INVESTIGACIÓN, FORMACIÓN Y DESARROLLO

1.INTRODUCCIÓN

Como es de conocimiento público, todos los años las instituciones de Salud Pública hacen campañas para que todo el mundo se vacune contra la gripe. Esto se debe a que los brotes de gripe se producen en una estación determinada del año en la que empiezan a extenderse y a contagiar a la gente, lo que se conoce como una nueva cepa o cepa anual.

Por el contrario, no hay epidemias estacionales previsibles para los PC, teléfonos inteligentes, tabletas y redes empresariales. En este caso, siempre es temporada de gripe. Pero en lugar de tener fiebre, malestar y dolor por todo el cuerpo, los usuarios pueden padecer una especie de enfermedad de las máquinas: el malware.

Las infecciones por malware nos llegan como el caudal de agua de una manguera contra incendios, cada una con sus propios métodos de ataque, que pueden ser sigilosos y solapados o nada sutiles, como un batazo. Pero si el conocimiento es poder, es importante formarse, a modo de inoculación preventiva contra la infección, sobre el malware, qué es, sus síntomas, cómo se contagia, cómo tratarlo y cómo evitarlo en el futuro.

2.MALWARE

Malware o “software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas

El malware hostil, intrusivo e intencionadamente desagradable intenta invadir, dañar o deshabilitar computadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo. Al igual que la gripe, interfiere en el funcionamiento normal.

HOJA DE INVESTIGACIÓN

FEBRERO 2021

EL MALWARE, MUTANDO JUNTO AL COVID-19

IMPACTO A NIVEL CRIPTOGRÁFICO

INVESTIGADORES: MSC. Arelis Guzmán/ Ing. Yakson Verenzuela

CONTACTO: aguzman@suscerte.gob.ve/ yverenzuela@suscerte.gob.ve

www.suscerte.gob.ve

DIRECCIÓN DE INVESTIGACIÓN, FORMACIÓN Y DESARROLLO

La intención del malware no es siempre sacarle dinero al usuario ilícitamente. Existen Malwares que dañan el Sistema de Archivo, incluso algunos simplemente espían. Aunque el malware no puede dañar el hardware de los sistemas o el equipo de red. Sí puede robar, cifrar o borrar sus datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en los computadores sin su conocimiento o permiso. [1].

3.ANTECEDENTES DE ROCKE

Este Malware fue documentado por primera vez por CISCO Talos en 2018, donde luego de un prestigioso análisis y estudio se determina que: Rocke distribuye y ejecuta malware de minería criptográfica utilizando un conjunto de herramientas variado que incluye repositorios de Git y diferentes cargas útiles, como scripts de Shell, backdoors de JavaScript, además de archivos ejecutables portátiles. [2]

4.MUTANDO CON EL COVID-19

Aunque las versiones anteriores del malware confiaban en la capacidad de apuntar y eliminar productos de seguridad en la nube desarrollados por Tencent Cloud y Alibaba Cloud mediante la explotación de fallas en Apache Struts 2, Oracle WebLogic y Adobe ColdFusion, Pro-Ocean agrandó la amplitud de esos vectores de ataque apuntando a los servidores Apache ActiveMQ, Oracle WebLogic y Redis.

Además de sus características de propagación automática y mejores técnicas de ocultación que le permiten permanecer bajo el radar y propagarse a software sin parches en la red, el malware propone desinstalar agentes de monitoreo para esquivar la detección y eliminar otros malware y mineros de los sistemas infectados. [3]

5.DESTRUYENDO EL SISTEMA INMUNE DE SU PC

Para lograr esto, cual virus humano ataca por las debilidades del sistema, aprovecha una característica nativa de Linux llamada LD_PRELOAD, con el fin de enmascarar su actividad maliciosa, una biblioteca llamada “Libprocesshider”, para permanecer oculta y

HOJA DE INVESTIGACIÓN

FEBRERO 2021

EL MALWARE, MUTANDO JUNTO AL COVID-19

IMPACTO A NIVEL CRIPTOGRÁFICO

INVESTIGADORES: MSC. Arelis Guzmán/ Ing. Yakson Verenzuela

CONTACTO: aguzman@suscerte.gob.ve/ yverenzuela@suscerte.gob.ve

www.suscerte.gob.ve

DIRECCIÓN DE INVESTIGACIÓN, FORMACIÓN Y DESARROLLO

utiliza un script de infección de Python que toma la IP pública de la máquina para infectar todas las máquinas en la misma subred de 16 bits.

Aunado a esto Pro-Ocean no admite competencia, trabaja para eliminar otros malware y mineros, incluyendo Luoxk, BillGates, XMRig y Hashfish, que se ejecutan en el host comprometido.

Finalmente, cuenta con un módulo de vigilancia escrito en Bash, que asegura la persistencia y se encarga de terminar todos los procesos que utilizan más del 30% de la CPU con el objetivo de minar criptoactivos de forma eficiente.

«Este malware es un ejemplo que demuestra que las soluciones de seguridad basadas en agentes de los proveedores de la nube pueden no ser suficientes para prevenir el malware evasivo dirigido a la infraestructura de la nube pública. Esta muestra tiene la capacidad de eliminar los agentes de algunos proveedores de nube y evadir su detección», dijo Aviv Sasson. [3].

HOJA DE INVESTIGACIÓN

FEBRERO 2021

EL MALWARE, MUTANDO JUNTO AL COVID-19

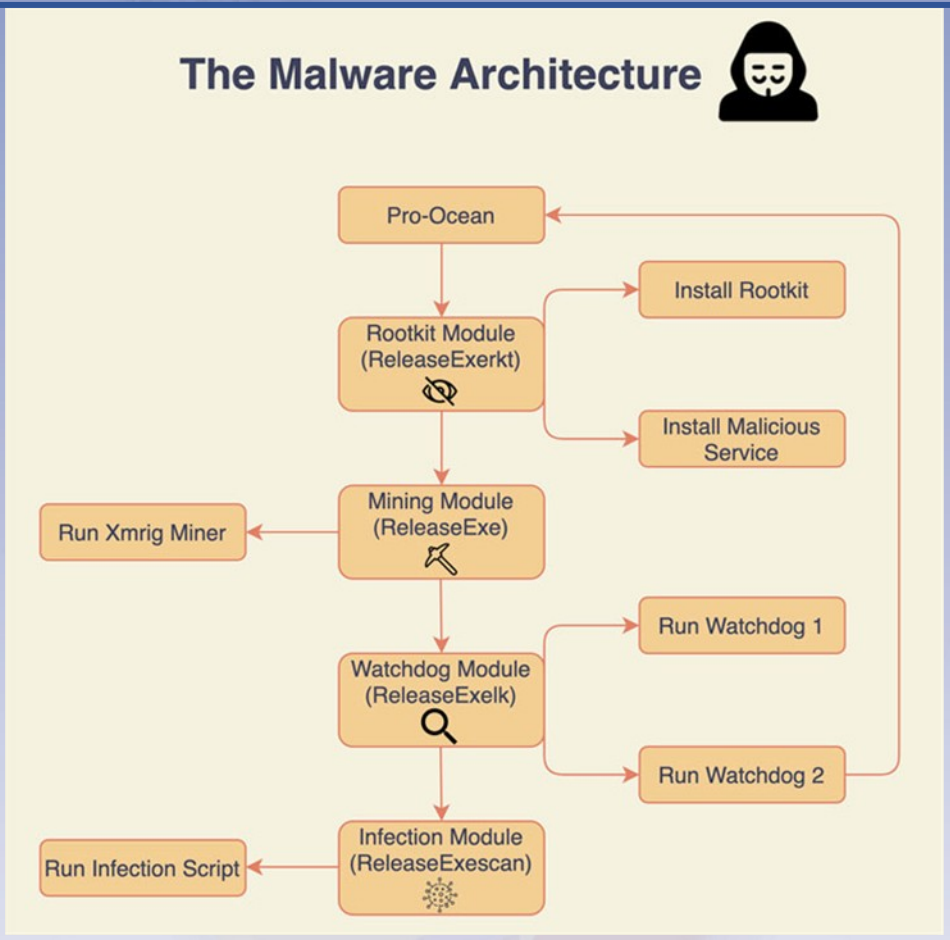
IMPACTO A NIVEL CRIPTOGRÁFICO

INVESTIGADORES: MSC. Arelis Guzmán/ Ing. Yakson Verenzuela

CONTACTO: aguzman@suscerte.gob.ve/ yverenzuela@suscerte.gob.ve

www.suscerte.gob.ve

DIRECCIÓN DE INVESTIGACIÓN, FORMACIÓN Y DESARROLLO



HOJA DE INVESTIGACIÓN

FEBRERO 2021

EL MALWARE, MUTANDO JUNTO AL COVID-19

IMPACTO A NIVEL CRIPTOGRÁFICO

INVESTIGADORES: MSC. Arelis Guzmán/ Ing. Yakson Verenzuela

CONTACTO: aguzman@suscerte.gob.ve/ yverenzuela@suscerte.gob.ve

www.suscerte.gob.ve

DIRECCIÓN DE INVESTIGACIÓN, FORMACIÓN Y DESARROLLO

6.¡ESTO NUNCA PASARÍA CON LINUX!

Existe una amplia variedad de **sistemas operativos alternativos** para uso corporativo y particular. Sin embargo, estas alternativas **no están libres de riesgos**, como algunos pueden pensar.

Tan pronto como se desvela o se informa sobre un nuevo troyano, aparece la famosa frase **"¡Eso nunca ocurriría en Linux!"**. Y esto no es cierto al 100 por ciento. Si ciertamente la mayoría de los programas maliciosos identificados hasta la fecha (más de dos millones) apuntan a Windows. Por otra parte, **Linux**, con apenas 1.898 programas maliciosos desarrollados para vulnerar este sistema operativo, parece gozar de relativa seguridad. Y hasta la fecha, sólo se han identificado 48 programas maliciosos para el sistema operativo Apple OS X.

Sistema operativo	**Total**	**Backdoors, Hacktools, Exploits & Rootkits**	**Virus y Gusanos**	**Troyanos**
Linux	1898	942 (50%)	136 (7%)	88 (5%)
FreeBSD	43	33 (77%)	10 (23%)	0 (0%)
Sun Solaris	119	99 (83%)	17 (15%)	3 (2%)
Unix	212	76 (36%)	118(56%)	3 (1%)
OSX	48	14 (29%)	9 (19%)	11 (23%)

HOJA DE INVESTIGACIÓN

FEBRERO 2021

EL MALWARE, MUTANDO JUNTO AL COVID-19

IMPACTO A NIVEL CRIPTOGRÁFICO

INVESTIGADORES: MSC. Arelis Guzmán/ Ing. Yakson Verenzuela

CONTACTO: aguzman@suscerte.gob.ve/ yverenzuela@suscerte.gob.ve

www.suscerte.gob.ve

DIRECCIÓN DE INVESTIGACIÓN, FORMACIÓN Y DESARROLLO

Windows	2247659	501515 (22%)	40188 (2%)	1232798(55%)
Fuente: [5]				

Vistas las cifras, algunos dirán ¡Solo es el 5% de riesgo! Cualquier otro sistema es más seguro comparado con Windows. Pero existe un pequeño pero gran detalle que debemos tener presente: los troyanos no necesitan privilegios en la raíz para acceder y espiar la información o para llamar a casa a través del puerto 80. Actualmente la expresión «¿No es Ubuntu?» se oye decir ligeramente a los principiantes en informática; no obstante, los usuarios de Linux tienen que estar preparados para cuando los ciberdelincuentes que tienen en la mira a los usuarios inexpertos irrumpan en sus equipos. [5]

7.CONCLUSIÓN

Lo que representa el mayor de los riesgos es la creencia de que un sistema sea impermeable. Incluso hoy en día, las computadoras vienen con una solución antivirus preinstalada, pero, a la vez, muchos usuarios de Linux son reacios a instalar hasta los análisis gratuitos como ClamAV, creyendo que simplemente no es necesario. Actualmente la comunidad ofrece una variedad de soluciones de alto rendimiento, con tecnologías como SELinux, AppArmor, y una serie de sistemas de detección de intrusiones. Quienes omitan el uso de estas soluciones, ya sea porque consideran que les toma mucho tiempo o esfuerzo, o porque piensan que no son necesarias, quizás no se den cuenta cuando su equipo caiga en manos de un pirata en busca de presas fáciles.

En oportunidades, los informáticos se refieren a Linux como si fuese un sistema operativo, cuando eso no es cierto, Linux es el Core, el núcleo, el kernel, pero él sólo, por sí mismo, no es operativo para un usuario. Es necesario un conjunto de paquetes, sistemas, librerías, etc. Este conjunto de aplicaciones que se engranan con el núcleo

HOJA DE INVESTIGACIÓN

FEBRERO 2021

EL MALWARE, MUTANDO JUNTO AL COVID-19

IMPACTO A NIVEL CRIPTOGRÁFICO

INVESTIGADORES: MSC. Arelis Guzmán/ Ing. Yakson Verenzuela

CONTACTO: aguzman@suscerte.gob.ve/ yverenzuela@suscerte.gob.ve

www.suscerte.gob.ve

DIRECCIÓN DE INVESTIGACIÓN, FORMACIÓN Y DESARROLLO

Linux es lo que conocemos como GNU/Linux. GNU/Linux si es un sistema operativo, o como diría el profesor Jorge Baralt, “es un sistema de operación base”.

8.REFERENCIA BIBLIOGRÁFICA

[1] es.malwarebytes.com. (2021, febrero 09). ¿Qué es el malware? | Malwarebytes. [On Line]. Available: https://es.malwarebytes.com/malware/

[2] D. Liebenberg. (2018, agosto 30). Rocke: The Champion of Monero Miners. [On Line] Available: https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html

[3] A. Sasson. (2021, enero 28). Pro-Ocean: Rocke Group’s New Cryptojacking Malware. [On Line]. Available: **https://unit42.paloaltonetworks.com/pro-ocean-rocke-groups-new-cryptojacking-malware/**

[4] H. Sulbaran. (2021, enero 26). Efemérides de Tecnología: Febrero. [On Line]. Available: https://helisulbaran.blogspot.com/p/feb.html

[5] M. Kalkuhl – M. Preuss. (2009, agosto 21). ¿Cuáles son las amenazas que atacan al software libre y alternativo? – RedUSERS. [On Line]. Available: http://www.redusers.com/noticias/%C2%BFcuales-son-las-amenazas-que-atacan-al-software-libre-y-alternativo/