SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 02 EDICIÓN 2.27

WWW.COREONEIT.COM
@COREONEIT

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

¿QUÉ ES EL SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]?

Es una combinación de información de amenazas existentes en la red con el análisis e inteligencia del grupo de especialistas de CORE ONE IT, quienes analizan exhaustivamente todo tipo de amenazas informáticas y desarrollan una serie de recomendaciones adaptadas a cada tipo de cliente.

ALCANCE

Se personaliza de acuerdo al tipo de infraestructura y entorno de red del cliente basado en los tipos de dispositivos, modelos y fabricantes, con el fin de recibir solo información relevante y que pudiera afectar de manera directa o indirecta, la continuidad del negocio.

DEFINICIONES

•Riesgo: Probabilidad que una amenaza particular explote una vulnerabilidad particular de un sistema.

•Amenaza: Es la causa potencial de un incidente no deseado, el cual puede resultar en un daño a un sistema de información u organización.

•Ataque: Acción de tratar de traspasar controles de seguridad en un sistema. Un ataque puede ser activo, resultando en la modificación de datos, o pasivo, resultando en la divulgación de información. El hecho de que un ataque sea realizado no significa que será exitoso, el grado de éxito depende de la vulnerabilidad del sistema o actividad y de la eficiencia de las medidas existentes.

•Vulnerabilidad: Debilidad en los procedimientos de seguridad de un sistema, en el diseño del sistema, en la implementación, en los controles internos, y que puede ser explotada para violar la política de seguridad del sistema.

•DoS: Denegación de servicio, ataque a equipo o aplicación con el fin de que el servicio no esté disponible para los usuarios legítimos.

•Malware: también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

•Ransomware. Es un tipo especial de malware que amenaza con destruir los documentos y otros archivos de las víctimas.

•Troyano. -Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo.

•Backdating: Backdating es un término utilizado cuando se archiva cualquier clase de documento con una fecha anterior a la cual éste fue originalmente creado.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

EL HACKEO DE YAHOO FUE MÁS ALLÁ, Y LES ROBARON TODAS LAS CUENTAS QUE TENÍAN EN 2013

La nueva herramienta predictiva de Mastercard permite a los bancos realizar acciones más rápidas ante un fraude.

En agosto de 2016, la conocida empresa de seguridad Yahoo! hacía público uno de los mayores robos de datos de la historia, confirmando así el robo de 200 millones de cuentas de usuarios, cuentas que entonces empezaron a circular por la Dark Web. En los meses siguientes, la compañía intentó ir quitando importancia a este ataque informático y, mentira tras mentira, ocultar lo que realmente pasó, y que muchos nos temíamos. Ahora, un año después de darse a conocer, y 4 después de tener lugar, finalmente Yahoo lo ha confirmado: el ataque informático supuso el robo de datos del 100% de los usuarios que la compañía tenía en 2013.

Si volvemos la vista atrás, la compañía (que en aquel entonces estaba en proceso de venta a Verizon, razón por la que, probablemente, ocultó la magnitud real del ataque) confirmó que el robo de datos había sido de 500 millones de usuarios, triplicando este número poco después hasta los 1500 millones de perfiles, siendo la mitad de todos los usuarios que la compañía tenía en 2013. Ahora, un año más tarde de haber descubierto este ataque informático, finalmente Yahoo se ha dado por vencida y la confirmado que el hackeo fue total, completo, y que se robaron absolutamente todos los usuarios que la compañía tenía en 20143, es decir, más de 3000 millones de usuarios expuestos por este ataque informático.

Esta información se ha descubierto y, por desgracia, confirmado durante la integración de los servicios de la compañía a la infraestructura de Verizon. Tras estudiar todo el impacto, finalmente esta compañía, ahora propietaria de Yahoo, finalmente ha confirmado lo que muchos temían, y es que el ataque informático fue mucho más grande de lo que se pensaba y, como hemos dicho, no afectó solo a 500 millones de usuarios, ni a 1500 millones, sino a toda la base de datos de la compañía, más de 3000 millones de usuarios.

Durante el ataque informático quedaron expuestos los datos personales de los usuarios, datos que van desde los nombres reales y fechas de nacimiento hasta los correos, chats, teléfonos e incluso contraseñas, además de algunas preguntas y respuestas secretas para la recuperación de las cuentas.

Verizon avisará a todos los usuarios afectados por el robo de datos de Yahoo y les ayudará a proteger sus cuentas.
Verizon ha asegurado que desde ahora va a empezar a contactar con todos los usuarios afectados a través del correo electrónico, informándoles del ataque y facilitándoles una serie de consejos para cambiar los datos de sus cuentas y volver a asegurarlas para evitar que, si alguien se hace con nuestros datos, estos puedan acceder a nuestra cuenta de Yahoo.

Verizon, además, asegura que va a seguir investigando el ataque informático e intentando localizar a los responsables del mismo, así como intentando averiguar con precisión qué datos tienen los piratas informáticos y qué están haciendo con ellos.

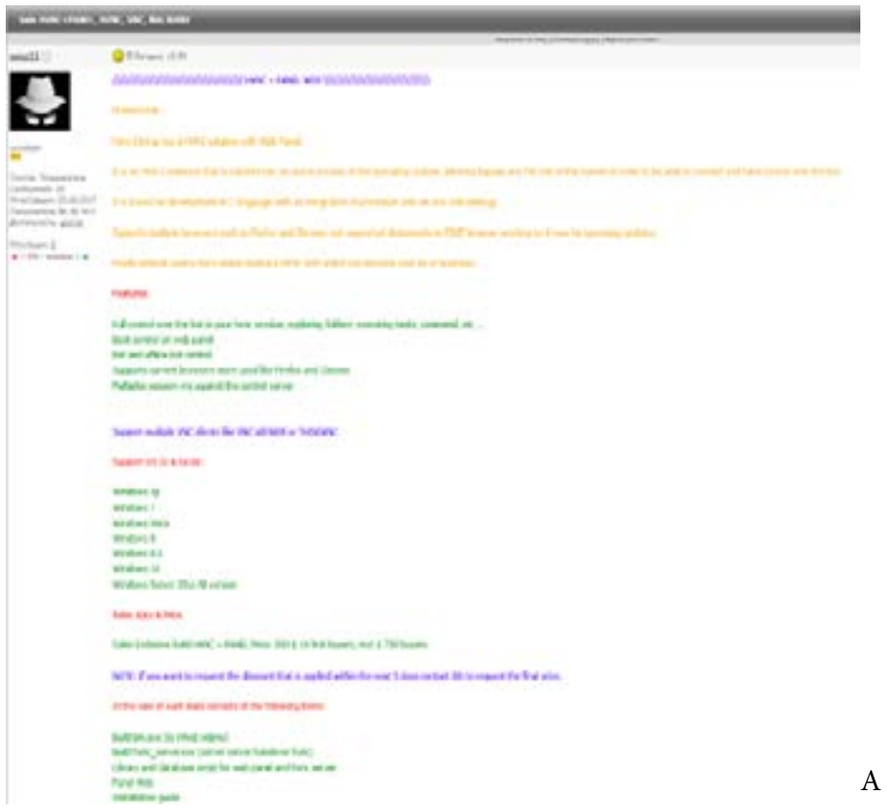
A

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Una cosa es segura, y es que, si hasta ahora el ataque a Yahoo ya era uno de los más grandes de la historia de la informática, ahora, tras los nuevos datos descubiertos sobre este nuevo robo de datos, su magnitud crece aún más, se hace aún más grande y puede que incluso llegue a ser inalcanzable.

VENTA DE VNC OCULTO CON PANEL ADMINISTRATIVO (AUTOR-NEOZ11)

El día de hoy se anunció sobre la venta de un malware - VNC oculto con panel administrativo - el cual fue publicado en un foro del mercado negro. El vendedor, actor de la amenaza, se encuentra con el apodo neoz11. Este malware está destinado para el acceso remoto a la PC de la víctima, funciona en todas las versiones de Windows.



A

FUENTES:

Tara Seals (2017). Uber, Facebook Messenger Top List of Riskiest Apps in the Enterprise, de Info-Security Magazine, Sitio web: https://www.infosecurity-magazine.com/news/uber-facebook-messenger-riskiest/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Se trata de un malware HVNC que se inyecta en un proceso activo del sistema operativo, lo que permite omitir cualquier regla del Firewall del sistema con el fin de poder conectarse y tener el control sobre el bot.

Su desarrollo está basado en el lenguaje de programación C con una integración de protección anti-vm y anti-debbug.

Soporta múltiples navegadores como Firefox y Chrome, no soporta Edge (en el proceso de trabajo).

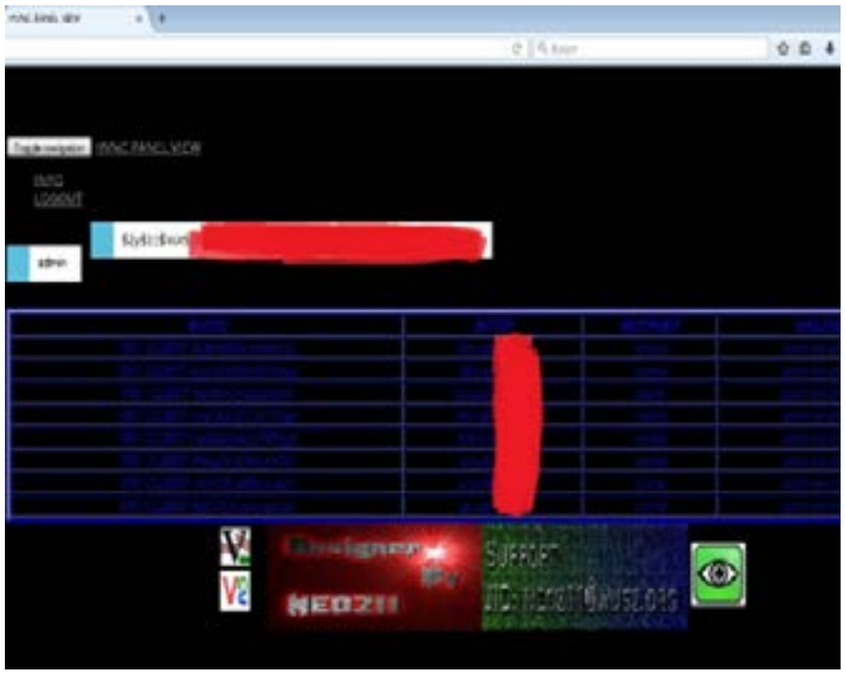
Características:
- *Control total sobre el bot en sesión HVNC, explorando carpetas, ejecutando tareas, comando, etc.*
- *Control de arranque en el panel de web*
- *Control del bot y en modo offline*
- *Compatible con los navegadores más usados como Firefox y Chrome*
- *Múltiples sesiones VNC contra el servidor de control*
- *Soporta múltiples clientes VNC como VNC Viewer o THINGVNC*

Soporta S.O. de 32 & 64 bits:
- *Windows Xp*
- *Windows 7*
- *Windows Vista*
- *Windows 8*
- *Windows 8.1*
- *Windows 10*
- *Windows Server 20xx Todas las versiones*

Precios:
- *Precio de la compilación HVNC + Panel HVNC: $550 10 primeros compradores, resto $750 compradores.*
- *Reconstruir paquete 2 bin.exe = $250*
- *Soporte mensual = $100*

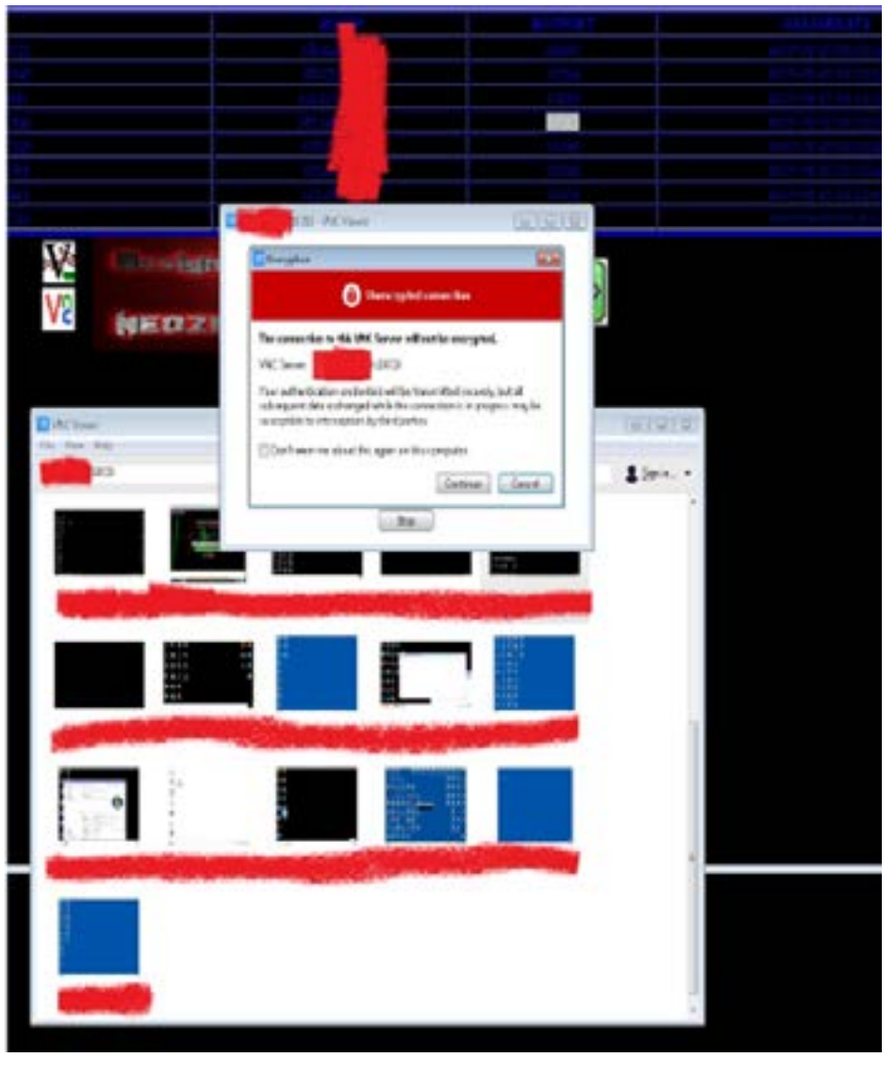
En la venta de cada compilación se compone de los siguientes elementos:
- *Build bin .exe (para infectar a las víctimas)*
- *Build hvnc Server. exe (servidor de entrega hvnc) Biblioteca y script de base de datos para panel web y hvnc servidor*
- *Panel Web*
- *Guía de instalación*

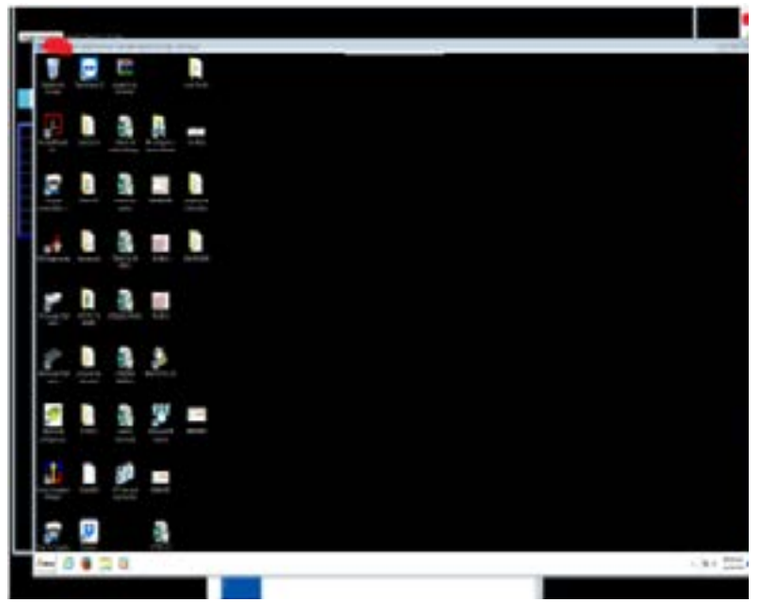
Capturas de Pantalla proporcionadas por neoz11:



A

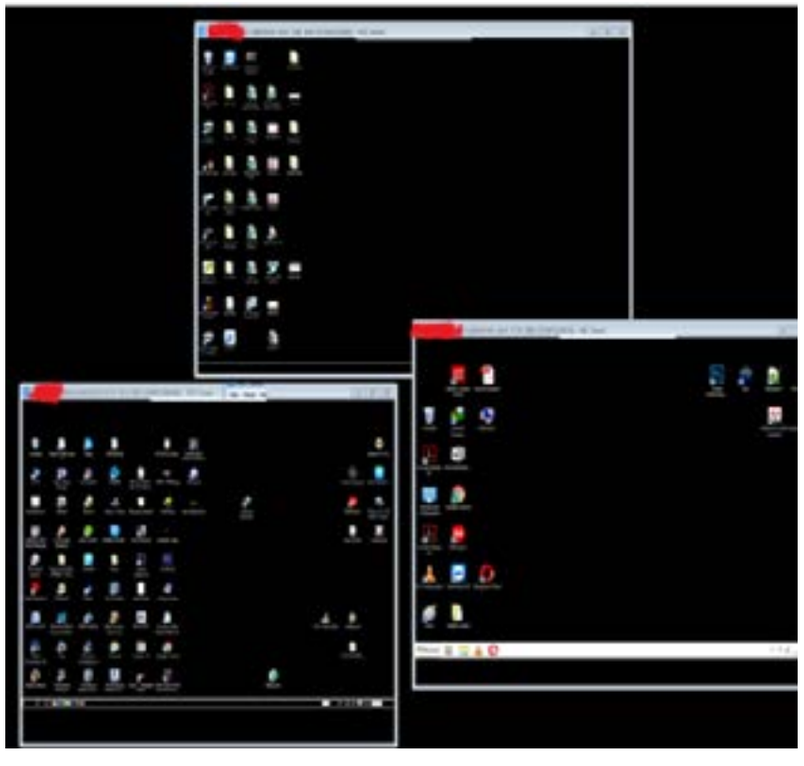
SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"



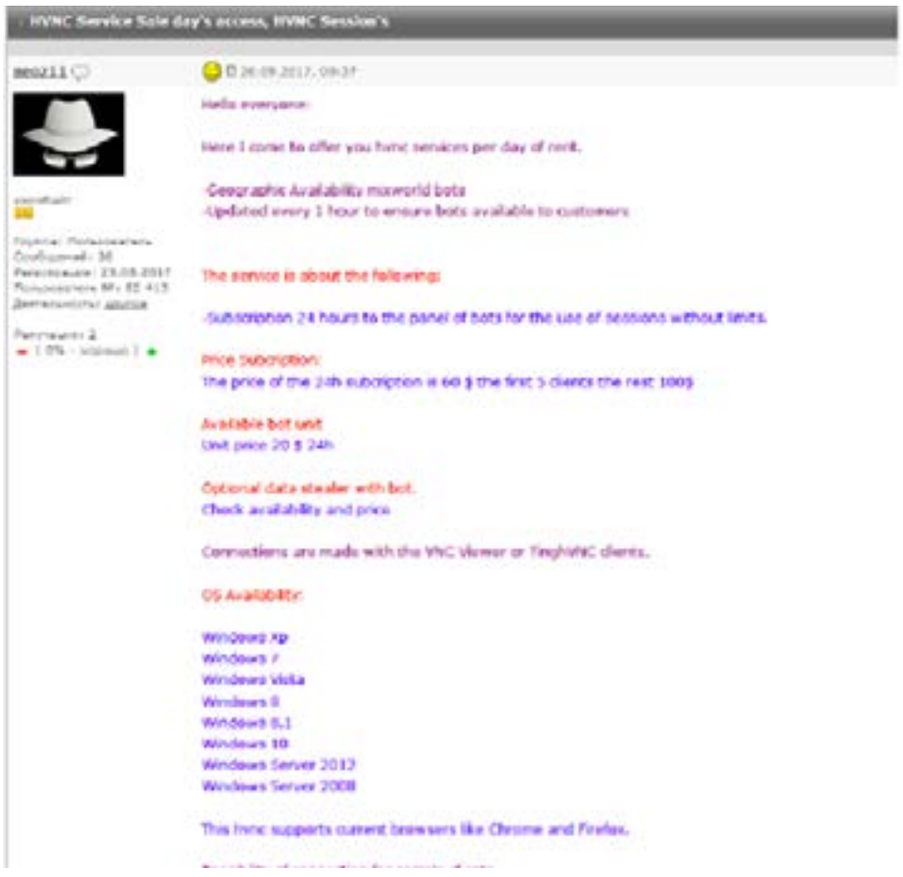


A

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"



Desde el 20 de septiembre del año en curso, neoz11 ha estado ofreciendo el programa para ser rentado por un precio de $20 por día. Existes reseñas positivas de otros usuarios en el siguiente tópico.



FUENTES:

Centro de Ciberinteligencia Group-IB

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

EL HACKEO DE YAHOO FUE MÁS ALLÁ, Y LES ROBARON TODAS LAS CUENTAS QUE TENÍAN EN 2013

Muchas empresas no están preparadas para lidiar con ataques DNS, y una cuarta parte de las que ya han sido afectadas reportaron pérdidas significativas, según una encuesta realizada por Dimensional Research en nombre de la empresa de seguridad de redes Infoblox.

Los ataques a los servicios del Sistema de Nombres de Dominio (DNS) pueden tener serias consecuencias, como lo demuestra el ataque a Dyn el año pasado. El ataque, impulsado por la botnet Mirai, llevó a interrupciones del servicio de varios sitios web importantes, incluyendo Twitter, GitHub, Etsy, Soundcloud, PagerDuty, Spotify y Airbnb.

El estudio de Dimensional Research e Infoblox, basado en una encuesta de más de 1,000 profesionales de TI y seguridad en todo el mundo, reveló que 3 de cada 10 empresas ya han experimentado ataques DNS y en la mayoría de los casos resultó en tiempo de inactividad.
Mientras que más de la mitad de los ataques resultaron en un tiempo de inactividad de menos de una hora, en el 6% de los casos el tiempo de inactividad duró entre 8 y 24 horas, y algunas víctimas incluso reportaron interrupciones del servicio que duraron más de un día.

En cuanto a las pérdidas financieras causadas por los ataques de DNS, el 3% de los encuestados dijo que había perdido más de un millón de dólares, y casi un cuarto reportó pérdidas superiores a los 100,000 dólares.

La investigación no ha encontrado ningún vínculo entre el tipo de servicio DNS utilizado y el riesgo de ataques. Las empresas que usaron un servicio de DNS en la nube, un servicio de terceros o su propio servicio fueron atacadas casi igual.

Según el informe, el 22% de las empresas no tienen un servicio DNS de respaldo, y el 63% de ellos no son capaces de defenderse contra todos los ataques DNS comu-

nes, tales como secuestro, explotaciones, envenenamiento de caché, anomalías de protocolo, reflexión, NXDomain y amplificación.

Casi un tercio de los 1,000 encuestados dijeron que no estaban seguros de que su compañía podría manejar un ataque DNS. Sin embargo, el incidente de Dyn ha tenido un impacto claro en cómo se ven los ataques DNS, lo que provoca que una tercera parte de las empresas cambie su estrategia de seguridad DNS.

La encuesta mostró que sólo el 11% de las empresas tienen equipos de seguridad que gestionan DNS, mientras que en la mayoría de los casos el servicio es manejado por la infraestructura de TI o los equipos de operaciones. Casi el 90% de los encuestados se quejaron de que sus soluciones de DNS no los habían alertado de un ataque de DNS que se estaba produciendo.

"Es probable que los ataques de DNS continúen y aumenten, dado que los ataques han sido extremadamente exitosos al afectar al negocio objetivo en un 93% por ciento del tiempo. Esta tasa de éxito revela que las empresas son vulnerables hoy en día con herramientas DNS de calidad inferior que son incapaces de defenderse frente a los ataques DNS comunes o alertar adecuadamente a los equipos cuando están bajo asedio".

FUENTES:

SGlobal Cybersec (2017). Compañías no están preparadas para los ataques de DNS, Octubre 2017, de sitio web: http://www.globalcybersec.com/reader.php?p=4112

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDADES CRÍTICAS DE SEGURIDAD PARA TOMAR LAS MEDIDAS PREVENTIVAS Y CORRECTIVAS FRENTE A LAS AMENAZAS TECNOLÓGICAS

VMWARE ESXI, VCENTER SERVER, FUSION Y WORKSTATION RESUELVEN MÚLTIPLES VULNERABILIDADES DE SEGURIDAD

Criticidad: Crítica
Impacto: Escalamiento de privilegios
Vulnerabilidad: -
Ejecución: Remota
Plataforma(s) afectada(s): VMware ESXi (ESXi), VMware vCenter Server, VMware Workstation Pro / Player (Estación de trabajo) y VMware Fusion Pro, Fusion (Fusion)
Referencia: CVE-2017-4924, CVE-2017-4925, CVE-2017-4926

Descripción:

Vulnerabilidad de escritura fuera de límites en SVGA
VMware ESXi, Workstation y Fusion contienen una vulnerabilidad de escritura fuera de límites en el dispositivo SVGA. Este problema puede permitir que un invitado ejecute código en el host.
El proyecto Common Vulnerabilities and Exposures (cve.mitre.org) ha asignado el identificador CVE-2017-4924 a este número.

Invitado RPC NULL puntero de referencia vulnerabilidad

VMware ESXi, Workstation y Fusion contienen una vulnerabilidad de desreferencia de puntero NULL. Este problema se produce al manejar solicitudes RPC invitado. La explotación exitosa de este problema puede permitir a los atacantes con privilegios de usuario normales bloquear sus máquinas virtuales.

El proyecto Common Vulnerabilities and Exposures (cve.mitre.org) ha asignado el identificador CVE-2017-4925 a este número.

XSS almacenado en el cliente H5

vCenter Server H5 Client contiene una vulnerabilidad que puede permitir el almacenamiento de scripts entre sitios (XSS). Un atacante con privilegios de usuario VC puede inyectar scripts java maliciosos que se ejecutarán cuando otros usuarios de VC accedan a la página.
El proyecto Common Vulnerabilities and Exposures (cve.mitre.org) ha asignado el identificador CVE-2017-4926 a este número.

Solución:

Revise las notas del parche / release de su producto y realice la actualización.

FUENTES:

VMWARE. (octubre 2017). VMware ESXi, vCenter Server, Fusion and Workstation updates resolve multiple security vulnerabilities. octubre 2017, de trend micro Sitio web: https://www.vmware.com/security/advisories/VMSA-2017-0015.html
https://www.cvedetails.com/cve/CVE-2017-4925/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

CISCO_VULNERABILIDAD DE DENEGACIÓN DE SERVICIO DEL CONSUMO DE MEMORIA DE DESCIFRADO SSL DEL MOTOR DE DETECCIÓN FIREPOWER DE CISCO

Criticidad: Alta
Impacto: Denegación de servicios
Vulnerabilidad: -
Ejecución: Remota
Plataforma(s) afectada(s): Cisco Firepower Threat Defense (FTD) 6.0.1
Referencia: CVE-2017-12245

Descripción:

Una vulnerabilidad en el descifrado del tráfico SSL para el software Cisco Firepower Threat Defense (FTD) podría permitir a un atacante remoto no autenticado causar agotamiento de la memoria del sistema. Si esta pérdida de memoria persiste en el tiempo, podría producirse una condición de denegación de servicio (DoS) porque el tráfico puede dejar de transmitirse a través del dispositivo.

La vulnerabilidad se debe a un error en la forma en que Firepower Detection Snort Engine gestiona el descifrado del tráfico SSL y las notificaciones desde y hacia el controlador ASA (Adaptive Security Appliance). Un atacante podría explotar esta vulnerabilidad enviando un flujo constante de tráfico malicioso de Secure Sockets Layer (SSL) a través del dispositivo. Un exploit podría permitir al atacante causar una condición DoS cuando el dispositivo se agota en la memoria del sistema.

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones provisionales que resuelvan esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Octubre 2017). Vulnerabilidad de denegación de servicio del consumo de memoria de descifrado SSL del motor de detección Firepower de Cisco. Octubre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-ftd

CISCO_VULNERABILIDAD DE DENEGACIÓN DE SERVICIO DE IPV6 DE CISCO FIREPOWER DETECTION ENGINE

Criticidad: Alta
Impacto: Denegación de servicio
Vulnerabilidad: -
Ejecución: Remota
Plataforma(s) afectada(s): Cisco Firepower System 6.0
Referencia: CVE-2017-12244

Descripción:

Una vulnerabilidad en el análisis del motor de detección de paquetes IPv6 para Cisco Firepower System Software podría permitir a un atacante remoto no autenticado causar una alta utilización de la CPU o provocar una condición de denegación de servicio porque el proceso de Snort se reinicia inesperadamente.

La vulnerabilidad se debe a la validación incorrecta de entrada de los campos en el paquete de encabezado de extensión IPv6. Un atacante podría explotar esta vulnerabilidad enviando un paquete malicioso IPv6 al motor de detección del dispositivo de destino. Un exploit podría permitir que el atacante causara una condición de DoS si el proceso de Snort se reinicia y se anula la inspección de tráfico o se baja el tráfico. Esta vulnerabilidad es específica para el tráfico IPv6 solamente.

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones provisionales que resuelvan esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Octubre 2017). Vulnerabilidad de denegación de servicio de IPv6 de Cisco Firepower Detection Engine. Octubre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-fpsnort

A

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

CISCO_VULNERABILIDAD DE DIVULGACIÓN DE INFORMACIÓN DE TRAVERSAL DEL DIRECTORIO DE LICENCIAS DE CISCO

Criticidad: Alta
Impacto: Divulgación de información
Vulnerabilidad: -
Ejecución: Remota
Plataforma(s) afectada(s): Cisco License Manager
Referencia: CVE-2017-12263

Descripción:

Una vulnerabilidad en la interfaz web del software Cisco License Manager podría permitir a un atacante remoto no autenticado descargar y ver archivos dentro de la aplicación que deberían estar restringidos.
El problema se debe a una desinfección inadecuada de la entrada suministrada por el usuario en los parámetros de solicitud HTTP que describen los nombres de archivo. Un atacante podría explotar esta vulnerabilidad mediante técnicas de recorrido de directorios para enviar una ruta a la ubicación del archivo deseada. Un exploit podría permitir al atacante ver archivos de aplicaciones que pueden contener información confidencial.

Cisco no ha lanzado y no lanzará una actualización de software para solucionar esta vulnerabilidad. No hay soluciones provisionales que resuelvan esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Octubre 2017). https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-clm. Octubre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-clm

CISCO_VULNERABILIDAD DE CROSS-SITE SCRIPTING DE HREF EN SOFTWARE DE CISCO ADAPTIVE SECURITY APPLIANCE

Criticidad: Media
Impacto: Cross Site Scripting
Vulnerabilidad: -
Ejecución: Remota
Plataforma(s) afectada(s): Cisco Adaptive Security Appliance (ASA)
Referencia: CVE-2017-12265

Descripción:

Una vulnerabilidad en la interfaz de administración basada en web del software ASA (Cisco Adaptive Security Appliance) podría permitir que un atacante remoto no autenticado lleve a cabo un ataque XSS (cross-site scripting) contra un usuario de la interfaz de administración basada en web de un dispositivo afectado.

La vulnerabilidad se debe a una validación insuficiente de la entrada suministrada por el usuario por la interfaz de administración basada en web de un dispositivo afectado. Un atacante podría explotar esta vulnerabilidad persuadiendo a un usuario de la interfaz para hacer clic en un vínculo creado. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz o permitir al atacante acceder a información sensible basada en navegador.

Puede encontrar más información sobre los ataques XSS y las posibles mitigaciones en: ***https://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20060922-understanding-xss***
https://www.owasp.org/index.php/Cross-site_Scripting_ (XSS)
No hay soluciones provisionales que resuelvan esta vulnerabilidad.

FUENTES:

Seguridad de cisco. (Octubre 2017). Vulnerabilidad de Cross Site Scripting de HREF en software de Cisco Adaptive Security Appliance. Octubre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-asa1

A

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

CISCO_VULNERABILIDAD DE CROSS-SITE SCRIPTING DE CISCO WEBEX MEETINGS SERVER

Criticidad: Media
Impacto: Cross Site Scripting
Vulnerabilidad: -
Ejecución: Remota
Plataforma(s) afectada(s): Cisco WebEx Meetings Server
Referencia: CVE-2017-12257

Descripción:

Una vulnerabilidad en el marco web de Cisco WebEx Meetings Server podría permitir que un atacante remoto no autenticado lleve a cabo un ataque XSS (cross-site scripting) contra un usuario de la interfaz web de un sistema afectado.
La vulnerabilidad se debe a la insuficiente validación de entrada de algunos parámetros que se pasan al servidor web del sistema afectado. Un atacante podría explotar esta vulnerabilidad convenciendo a un usuario para que siga un enlace malicioso o intercepte una solicitud de usuario e inyecte código malicioso en la solicitud. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz web afectada o permitir al atacante acceder a información sensible basada en navegador.

No hay soluciones provisionales que resuelvan esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Octubre 2017). https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-wms. Octubre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-wms

PARA MÁS INFORMACIÓN:

FORMULARIO@COREONEIT.COM
6387 88 87