BOLETÍN INFORMATIVO

002-2022

CONCIBER

Comité Nacional de Seguridad Cibernética

Limitación de Responsabilidad

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Comité Nacional de Seguridad Cibernética - CONCIBER puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

Aviso Legal

Contenido

Comité Nacional de Seguridad Cibernética – CONCIBER:

Por medio de este boletín informativo destacamos las noticias más relevantes en el ámbito de la ciberseguridad a nivel nacional y regional (Centroamérica y el Caribe) de forma quincenal.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes cibernéticos y amenazas cibernéticas, así como recomendaciones específicas de mitigación.

La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas. A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

Vulnerabilidades Tecnológicas

Vulnerabilidad en el protocolo Server Message Block SMB

Descripción:

La explotación de la vulnerabilidad en el protocolo Server Message Block - SMB podría permitir a un ciberdelincuente la ejecución arbitraria de código que puede propagarse rápidamente por redes de computadoras que utilicen una versión vulnerable del protocolo.

La capacidad de desencadenar la ejecución de código arbitrario a través de una red, le dará al atacante la capacidad de ejecutar código remoto (RCE) creando así una conexión remota hacia el sistema objetivo.

Recomendaciones:

Se recomienda realizar las siguientes acciones recomendadas por el fabricante samba.org

1. Si utiliza la versión 4.16, actualice a la versión 4.16.4
2. Si utiliza la versión 4.15, actualice a la versión 4.15.9
3. Si utiliza la versión 4.14, actualice a la versión 4.14.14

Fuente de referencia:

1. https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/11979-vulnerabilidades-criticas-en-samba.html
2. CVE-2022-2031: https://www.samba.org/samba/security/CVE-2022-2031.html
3. CVE-2022-32744: https://www.samba.org/samba/security/CVE-2022-32744.html
4. CVE-2022-32745: https://www.samba.org/samba/security/CVE-2022-32745.html
5. CVE-2022-32746: https://www.samba.org/samba/security/CVE-2022-32746.html
6. CVE-2022-32742: https://www.samba.org/samba/security/CVE-2022-32742.html

Vulnerabilidad Use-After-Free (UAF) en productos Adobe Acrobat & Reader

Descripción:

La explotación de la vulnerabilidad permite el uso de memoria previamente liberada la cual puede desencadenar una serie de consecuencias adversas, que van desde la corrupción de datos válidos hasta la ejecución de código arbitrario por lo que:

- Si el área de memoria en cuestión se ha asignado y utilizado correctamente en otro lugar.
- Si la consolidación de fragmentos se produce después del uso de datos previamente liberados, el proceso puede bloquearse cuando se utilizan datos no válidos como información de fragmentos.
- Si se ingresan datos maliciosos antes de que pueda llevarse a cabo la consolidación de fragmentos, es posible aprovechar una primitiva de escribir qué y dónde para ejecutar código arbitrario.

Recomendaciones:

La empresa Adobe Systems Incorporated recomienda a sus usuarios que actualicen sus instalaciones de software a las últimas versiones siguiendo las recomendaciones para cada caso.

Fuente de referencia:

1. https://helpx.adobe.com/security/products/acrobat/apsb22-32.html
2. https://nvd.nist.gov/vuln/detail/CVE-2022-34233#vulnCurrentDescriptionTitle
3. https://www.zscaler.es/blogs/security-research/analysis-adobe-acrobat-reader-javascript-docprint-use-after-free
4. https://cwe.mitre.org/data/definitions/416

Campañas de fraude cibernético

Campaña de fraude cibernético a contribuyentes

Descripción:

Ciberdelincuentes fingen ser empleados de la Superintendencia de Administración Tributaria – SAT y envían falsos requerimientos de pago o solicitudes de depósito a cuentas bancarias personales de terceros. Los contribuyentes son contactados por medio de correo electrónico, plataformas de redes sociales y de mensajería instantánea para comunicarles sobre un falso requerimiento de pago a nombre de la Superintendencia de Administración Tributaria y/o de empresas privadas.

Figura 1 alerta emitida por Superintendencia de Administración Tributaria

Recomendaciones:

1. No proporcione información personal por ningún medio digital que pueda comprometer su confidencialidad
2. Verifique información de multas u omisos directamente desde el portal web oficial de la Superintendencia de Administración Tributaria – SAT
3. No realice depósitos a cuentas bancarias de terceros

Fuente de Referencia

1. https://twitter.com/SATGT/status/1551631935767826442/photo/1
2. https://portal.sat.gob.gt/portal/

Campaña masiva de phishing dirigida a usuarios del servicio de correo electrónico de Microsoft Outlook

Descripción:

El grupo de ciberseguridad “Zscaler ThreatLabz” alerta sobre la campaña masiva de phishing dirigida a los usuarios empresariales del servicio de correo electrónico de Microsoft Outlook.
Los ciberdelincuentes pueden intentar posicionarse entre dos o más dispositivos en red utilizando una técnica de adversario en el medio AiTM Adversary-in-the-middle para respaldar comportamientos de seguimiento como Network Sniffing o Transmitted Data Manipulation . Al abusar de las características de los protocolos de red comunes que pueden determinar el flujo del tráfico de la red, los ciberdelincuentes pueden obligar a un dispositivo a comunicarse a través de un sistema controlado por el adversario para que puedan recopilar información o realizar acciones adicionales.

Los ciberdelincuentes pueden configurar una posición similar a AiTM para evitar que el tráfico fluya hacia el destino apropiado, potencialmente para perjudicar las defensas y/o en apoyo de una denegación de servicio de red .

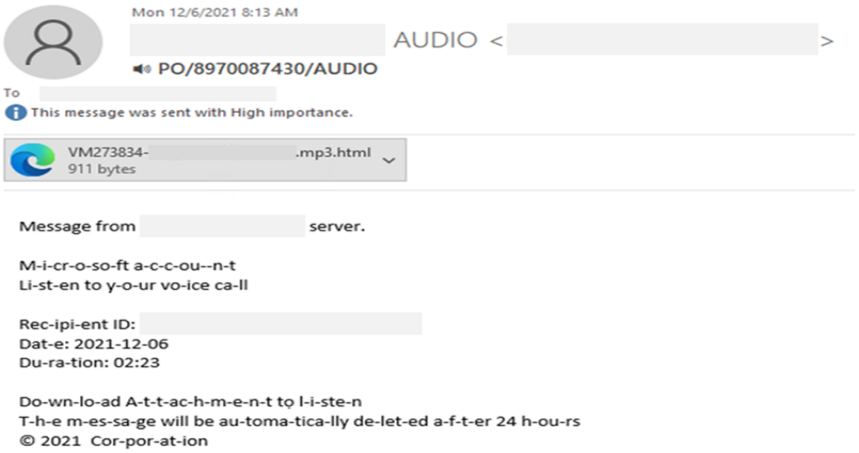

Figura 2 correo recibido de referencia

Recomendaciones:

Ante esta alerta se dan las siguientes recomendaciones para mitigar este tipo de ataques:

1. Deshabilite los protocolos de red heredados que pueden usarse para interceptar el tráfico de red
2. Asegúrese de que todo el tráfico cableado y/o inalámbrico esté encriptado adecuadamente. Utilice las mejores prácticas para los protocolos de autenticación, como Kerberos, y asegúrese de que el tráfico web que pueda contener credenciales esté protegido por SSL/TLS.
3. Utilice dispositivos de red y software de seguridad basado en host para bloquear el tráfico de red que no es necesario dentro del entorno
4. Limite el acceso a la infraestructura de red y los recursos que se pueden usar para remodelar el tráfico o producir condiciones AiTM.
5. Los sistemas de detección y prevención de intrusiones en la red que pueden identificar patrones de tráfico indicativos de actividad AiTM

6. La segmentación de la red se puede utilizar para aislar los componentes de la infraestructura que no requieren un amplio acceso a la red.

Fuente de Referencia:

1. https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/
2. https://www.zscaler.com/blogs/security-research/large-scale-aitm-attack-targeting-enterprise-users-microsoft-email-services
3. https://attack.mitre.org/techniques/T1557/

Campaña de fraude "Gasolina Gratis"

Descripción

Chevron Guatemala-Texaco hace saber a la población en general sobre la campaña de estafa realizada en medios sociales y plataformas de mensajería instantánea, ofreciendo gasolina gratis en su nombre.

Ciberdelincuentes atraen a su víctima por medio de redes sociales y plataformas de mensajería instantánea, facilitándoles una invitación que contiene una URL maliciosa que redirige hacia un sitio web que suplanta la identidad de Chevron Guatemala-Texaco, donde se le pide a la víctima el llenado de un formulario que requiere información personal.

Figura 3 comunicado Chevron Guatemala – Texaco

Recomendaciones:

1. Verificar en plataformas oficiales promociones y /o regalos que se ofrezcan en medios digitales para validar su veracidad.
2. No brindar por ningún medio digital información personal que pueda comprometer su confidencialidad.

Fuentes de Referencia:

1. https://www.facebook.com/texaco.gt/photos/a.168174288212828 7/2886778951624668/
2. https://www.virustotal.com/gui/url/75bc1b82f6f46f2ecd2df00ccbc6473870a63e845c0e09ca4c1e391964f341f5?nocache=1

Amenazas Cibernéticas

Aumento exponencial de tipo Ransomware en la región guatemalteca

Descripción:

El crecimiento exponencial de Ransomware continúa expandiéndose durante la última semana por una amplia variedad de los mismos sobre el territorio nacional.

De acuerdo a las estadísticas reportadas por los distintos fabricantes de soluciones de ciberseguridad, a continuación, se muestra el listado de las versiones de Ransomware empleadas en ciberataques en la región guatemalteca.

A continuación, se muestra el listado de las diez (10) principales amenazas que pueden poner en riesgo la Integridad, Disponibilidad y Confidencialidad de un sistema de información.

1.	Trojan-ransom.win32.Crypmod.gen	30%
2.	Trojan-Ransom.Win32.Crypren.afmu	13.33%
3.	Trojan-Ransom.Win32.Stop.gen	13.33%
4.	Trojan-Ransom.Win32.Crypmodng.gen	10%
5.	Trojan-Ransom.Win32.Phobos.vho	6.67%
6.	Trojan-Ransom.Win32.Blocker.gen	6.67%
7.	Trojan-Ransom.MSIL.Blocker.gen	3.33%
8.	Trojan-Ransom.Win32.Blocker.pef	3.33%
9.	Trojan-Ransom.Win32.Gen.kmi	3.33%
10.	Trojan-Ransom.Win32.Zerber.vho	3.33%

Recomendaciones:

1. Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de datos que se pueden usar para restaurar datos de la organización.
2. Implementar servicios de Antivirus/Antimalware.
3. Implementar herramientas de Prevención de intrusiones en la red (IDS)
4. Restringir contenido basado en la web
5. Utilice mecanismos de autenticación de correo electrónico y contra la suplantación de identidad
6. Capacitar a sus usuarios para identificar técnicas de ingeniería social y correos electrónicos de phishing.

Fuente de referencia:

1. Reporte de amenazas https://cybermap.kaspersky.com/es
2. Reporte de amenazas https://www.fireeye.com/cyber-map/threat-map.html
3. Reporte de amenazas https://threatmap.fortiguard.com/
4. Mitigación https://attack.mitre.org/techniques/T1486/
5. Mitigación https://attack.mitre.org/techniques/T1566/

Crecimiento exponencial de Malware en Guatemala

Descripción:

De acuerdo al reporte de amenazas emitido por ESET compañía de software especializada en ciberseguridad durante las últimas semanas del mes de agosto de 2022, se visualizó un crecimiento exponencial de amenazas cibernéticas de Malware en la región.

Estas amenazas de tipo malware generalmente la infección se lleva a cabo debido a que un ciberdelincuente puede aprovecharse de las vulnerabilidades o fallas de software encontradas. Posteriormente a su explotación los ciberdelincuentes pueden escalar privilegios y tomar el control del dispositivo, acceder a la información e incluso cifrar la misma.

A continuación, se muestra el listado de las diez (10) principales amenazas que pueden poner en riesgo la Integridad, Disponibilidad y Confidencialidad de un sistema de información.

1.	SMB.Attack.Bruteforce	9.28 %
2.	JS/Adware.TerraClicks	7.68 %
3.	JS/Adware.Adport	6.56 %
4.	RDP.Attack.Bruteforce	6.22 %
5.	JS/Packed.Agent.K	5.52 %
6.	JS/Adware.Sculinst	5.27 %
7.	JS/Packed.Agent.L	4.34 %
8.	HTML/ScrInject	4.1 %
9.	EK-Mozi	3.35 %
10.	HTTP/Exploit.CVE-2021-41773	3.09 %

Recomendaciones:

Considere implementar:

1. Servicios de Antivirus/Antimalware.
2. Herramientas de Prevención de Intrusiones en la red (IDS)
3. Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)
4. Herramientas de Detección y Respuesta Extendidas (XDR)

Es importante:

1. Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
2. Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos y programas ofimáticos.
3. Implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de datos que se pueden usar para restaurar datos de la organización.

Fuentes de referencia

1. Reporte de amenazas https://www.virusradar.com/en/statistics/10
2. Reporte de amenazas https://www.welivesecurity.com/la-es/
3. Mitigación https://attack.mitre.org/techniques/T1486/
4. Mitigación https://attack.mitre.org/techniques/T1566/

Crecimiento exponencial del Ransomware “VICE SOCIETY - Neshta”.

Descripción:

Con base al reporte de amenazas emitido por el Centro Criptológico Nacional - CCN de España, institución especializada en ciberseguridad, se alerta sobre el crecimiento exponencial de amenazas de tipo Malware identificado como Código Dañino “VICE SOCIETY - Neshta”.

La investigación realizada por el Centro Estratégico de Monitoreo-CEM, esta amenaza de tipo malware posee la siguiente particularidad.

Neshta es un código dañino del tipo “file infector” con capacidad de autorreplicarse en otros ejecutables del sistema. El código que se inyecta se ejecuta cada vez que se abre un archivo “exe” y se copia en otros ficheros del mismo tipo. En otros casos, también pueden añadir algún código dañino que puede ser utilizado para otros fines como el robo de datos o credenciales.

Por su parte VICE SOCIETY, también conocido como VICE SPIDER, es un actor malicioso que utiliza diferentes familias de ransomware como Zeppelin, Spider, Death Kitty para versión de Linux y Hive como RaaS (Ransomware as a service) para cifrar los archivos de sus víctimas. El vector de entrada que suele utilizar son las credenciales legítimas comprometidas de servicios de VPN o RDP para así acceder a la red de las víctimas.

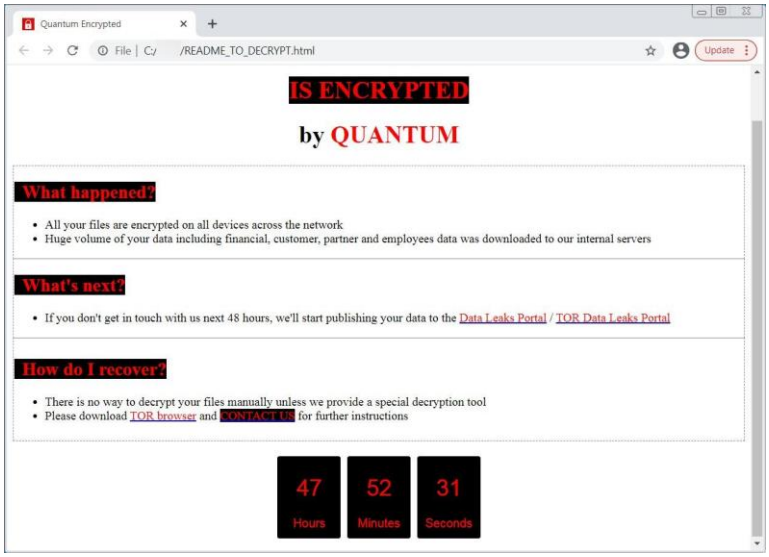

Figura 4 alerta emitida por el Centro Criptológico Nacional de España

Recomendaciones:

Considere implementar:

1. Servicios de Antivirus/Antimalware.
2. Herramientas de Prevención de Intrusiones en la red (IDS)
3. Herramientas de Detección y Respuesta de Amenazas de Puntos Finales (EDR)
4. Herramientas de Detección y Respuesta Extendidas (XDR)

Es importante:

1. Actualizar regularmente los sistemas operativos, el hardware y el software de los dispositivos.
2. Llevar a cabo una rutina periódica de actualización y parcheo de los sistemas operativos y programas ofimáticos.
3. Implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar y probar regularmente copias de seguridad de datos que se pueden usar para restaurar datos de la organización.

Fuente de referencia:

1. Publicación código dañino Neshta https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/12012-publicado-el-nuevo-informe-de-codigo-danino-id-09-22-sobre-el-ransomware-neshta.html
2. Informe Técnico del código dañino ID-09/22 sobre el ransomware Neshta https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6690-ccn-cert-id-09-22-vice-society-neshta-1/file.html