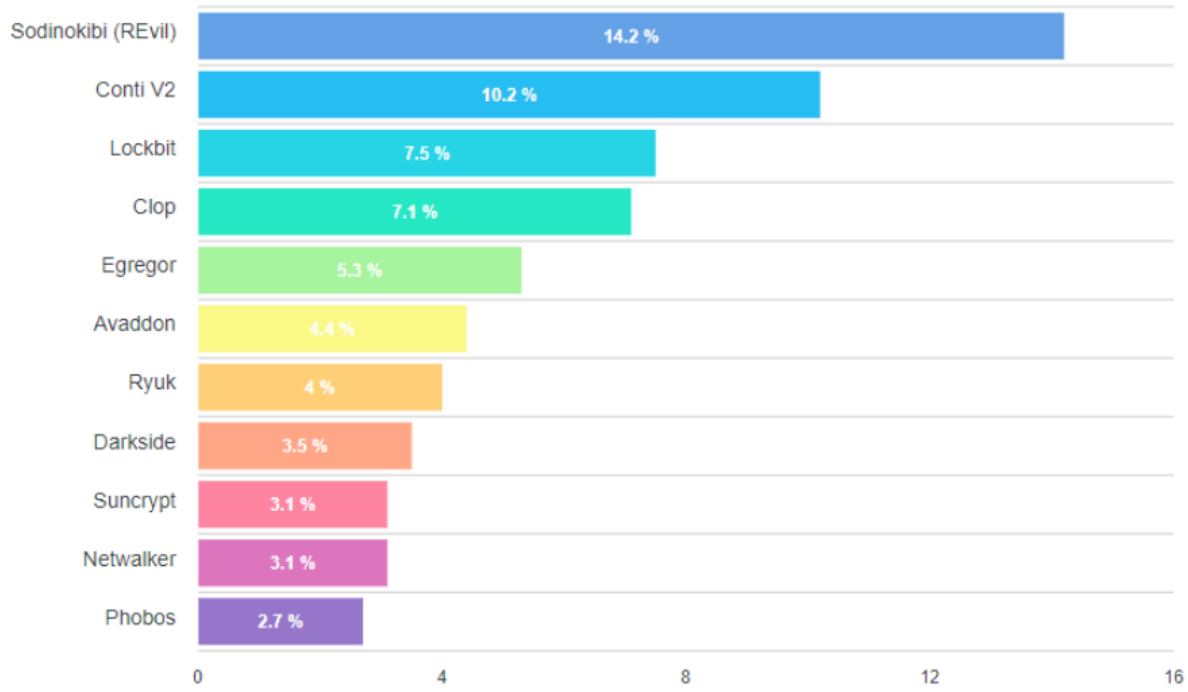
BOLETÍN DE ALERTA

Boletín Nro.: 2022-48
Fecha de publicación: 11/11/2022
Tema: Principales vulnerabilidades críticas explotadas por grupos de ransomware

Descripción:

Recientemente se han reportado múltiples ataques de ransomware contra sistemas informáticos, especialmente en la región de Latinoamérica, en donde los atacantes explotan vulnerabilidades en softwares ampliamente utilizados. Actualmente existe una gran cantidad de tipos de ataques de ransomware, entre los más reportados se detallan los siguientes:



Fuente: https://www.cloudwards.net/ransomware-statistics/

Otra modalidad delictiva es lo que se conoce como ransomware como servicio (*RaaS*), que consiste en un modelo de negocio en el que actores maliciosos contratan los servicios de un ransomware a través de un programa de afiliados y se encargan de llevar adelante los ataques. En todos los aspectos, cualquier *RaaS* puede considerarse un *SaaS* (*Software as a Service*).

Algunas de las principales vulnerabilidades explotadas se detallan a continuación:

Zimbra:

- CVE-2022-27925, de severidad “alta”, con puntuación asignada de 7.2. Esta se debe a la falla en la función *mboximport* del servidor Zimbra, que recibe un archivo ZIP y extrae los archivos encontrados en él. Un atacante sin credenciales administrativas podría aprovechar esta vulnerabilidad para realizar ejecución remota de código (RCE). Existen reportes de que está siendo explotada masivamente. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

- CVE-2022-27924, de severidad “alta” y puntuación de 7.5. Esta vulnerabilidad se debe a una falla encontrada en Zimbra Collaboration (también conocido como *ZCS*). Esto permite a un atacante inyectar comandos arbitrarios de *memcache* en una instancia específica del sistema. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace

- CVE-2022-30333, de severidad “alta” y puntuación de 7.5. Esta vulnerabilidad se debe a la extracción realizada por la herramienta *UnRar* incluida en el servicio Amavisd utilizado por Zimbra, de un archivo creado con fines malintencionados fuera del directorio predeterminado, logrando una escritura de archivos en una ubicación especificada. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

- CVE-2022-41352, de severidad de severidad “crítica”, con puntuación asignada de 9.8. Esta se debe a la falla en el método de control *cpio* del servicio de antivirus Amavis utilizado por Zimbra. Esto permitiría a un atacante enviar un archivo especialmente diseñado para realizar ejecución remota de código (*RCE*) en el sistema afectado, así también la misma permitiría introducir *webshells* en carpetas públicas para obtener una línea de comandos remoto. Actualmente para esta vulnerabilidad existen *PoCs* publicados en internet. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

Citrix:

- CVE-2019-11634 de severidad “crítica” y con puntuación asignada de 9.8. Esta vulnerabilidad se debe falla en el control de acceso de *Citrix Workspace.* Un atacante podría aprovechar esta vulnerabilidad realizar ejecución remota de código (*RCE*) en los dispositivos afectados.

- CVE-2019-19781 de severidad “crítica” y con puntuación asignada de 9.8. Esta vulnerabilidad se debe falla en la validación de datos de entrada en *Citrix Application Delivery Controller (ADC) and Citrix Gateway.* Un atacante remoto podría aprovechar esta vulnerabilidad ejecutar código arbitrario en los dispositivos afectados.

- CVE-2020-8195 y CVE-2020-8196 ambas de severidad “media” y con puntuación asignada de 6.5 y 4.3 respectivamente. Estas vulnerabilidades se deben a fallas en la validación de datos de entrada de *Citrix ADC y Citrix Gateway*. Un atacante remoto podría aprovechar estas vulnerabilidades para enviar una solicitud *HTTP* especialmente diseñada, y acceder a información sensible del dispositivo, como archivos de configuración. Actualmente para esta vulnerabilidad existen *PoCs* publicados en internet.

Fortinet:

CVE-2018-13374 de severidad “alta” y con puntuación asignada de 8.8. Esta vulnerabilidad se debe a una falla en el control de acceso del servidor *LDAP* de FortiGate. Un atacante podría obtener las credenciales de inicio de sesión e información confidencial en el sistema afectado. Actualmente para esta vulnerabilidad existen *PoCs* publicados en internet.

- CVE-2018-13379 de severidad “critica” y con puntuación asignada de 9.8. Esta vulnerabilidad de *directory traversal* se debe a la validación incorrecta de datos de entrada en FortiOs. Un atacante remoto podría aprovechar esta vulnerabilidad para enviar solicitudes *HTTP* especialmente diseñadas y acceder a archivos confidenciales

del sistema. Actualmente para esta vulnerabilidad existen *PoCs* publicados en internet.

- CVE-2020-0688 de severidad "alta" y con puntuación de 8.8. Esta vulnerabilidad se debe a la validación incorrecta de datos de entrada en la interfaz OCP de Microsoft Exchange. Un atacante remoto podría aprovechar esta vulnerabilidad para realizar ejecución remota de código (RCE) en el sistema afectado. Actualmente para esta vulnerabilidad existen PoCs publicados en internet.

- CVE-2021-36166, de severidad "crítica", con una puntuación de 9.8. Esta vulnerabilidad se debe a una falla en el proceso de autenticación de FortiMail, que permite a través de la observación de ciertas propiedades del sistema adivinar el token de autenticación de una cuenta de administración. Un atacante remoto podría aprovechar esta situación para obtener acceso completo al sistema afectado con dicho token. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

- CVE-2021-32586, de severidad "alta", con una puntuación de 7.7. Esta vulnerabilidad se debe a una validación incorrecta de un input de la *CGI* del servidor web de FortiMail. Un atacante no autenticado podría enviar peticiones *HTTP* especialmente diseñadas para alterar el entorno del intérprete de scripts del sistema y así comprometer el sistema afectado. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

- CVE-2021-43077 de severidad Alta, con una puntuación de 8.8. Esta vulnerabilidad se debe a un error en el componente *AP Monitor Handler*, que no valida correctamente la entrada de datos que realiza el usuario. Un atacante podría enviar una petición maliciosa con el objetivo de ejecutar código SQL arbitrario. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

- CVE-2022-40684, de severidad "crítica", con una puntuación asignada de 9.6. Esta vulnerabilidad se debe a una falla en el componente Administrative Interface. Esto permitiría a un atacante no autenticado realizar operaciones arbitrarias en la interfaz

administrativa. Actualmente para esta vulnerabilidad existe *un* PoC publicado en Internet. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

Microsoft Exchange:

- CVE-2020-0688 de severidad "alta" y con puntuación de 8.8. Esta vulnerabilidad se debe a la validación incorrecta de datos de entrada en la interfaz OCP de Microsoft Exchange. Un atacante remoto podría aprovechar esta vulnerabilidad para realizar ejecución remota de código (*RCE*) en el sistema afectado. Actualmente para esta vulnerabilidad existen *PoCs* publicados en internet.

- CVE-2021-26855 de severidad "crítica" y con puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla de control en Microsoft Exchange Server. Un atacante podría realizar ejecución remota de código (*RCE*) afectando al sistema.

- CVE-2022-41040, de severidad "alta" y con puntuación de 8.8. Esta vulnerabilidad de día cero (*0-day*) se debe a un problema en el Microsoft Exchange Server. Un atacante podría obtener escalamientos de privilegios en el sistema. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

- CVE-2022-41082, de severidad "alta" y con puntuación de 8.8. Esta vulnerabilidad de día cero (*0-day*) se debe a un problema en el Microsoft Exchange Server. Un atacante podría realizar ejecución remota de código (*RCE*) afectando al sistema. Hemos emitido un boletín al respecto con los detalles en el siguiente enlace.

Microsoft Office:

- CVE-2017-0199 de severidad "alta" y con puntuación asignada de 7.8. Esta vulnerabilidad se debe a una falla en la validación de archivos de Microsoft Office y WordPad. Un atacante podría aprovechar esta vulnerabilidad y realizar ejecución remota de código (*RCE*) en el sistema afectado.

- CVE-2017-11882 de severidad “alta” y con puntuación asignada de 7.8. Esta vulnerabilidad se debe a un problema relacionada con Microsoft Office al no tratar correctamente los objetos en la memoria. Un atacante podría iniciar sesión con derechos de usuario administrativos y ejecutar código arbitrario en el sistema.

Microsoft Azure:

- CVE-2021-38647 de severidad “critica” y con puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla en el *Open Management Infrastructure*. Un atacante no autenticado podría realizar ejecución remota de código (*RCE*) en el sistema afectado. Actualmente para esta vulnerabilidad existen *PoCs* publicados en internet.

Atlassian:

- CVE-2021-26084 de severidad “critica” y con puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla en la validación de datos de entrada en *Confluence Server and Data Center*. Un atacante no autenticado podría realizar ejecución remota de código (*RCE*) en el sistema.

Microsoft Windows:

- CVE-2019-0543 de severidad "alta" y puntuación asignada de 7.8. Esta vulnerabilidad se debe a una falla en el control de elevación de privilegios de Windows. Esto permitiría a un atacante realizar escalamiento de privilegios.

- CVE-2021–31166 de severidad “crítica” y con puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla en la pila de protocolos *HTTP*. Un atacante podría realizar ejecución remota de código (*RCE*). Actualmente para esta vulnerabilidad existen *PoCs* publicados en internet.

- CVE-2022-37986 y CVE-2022-38050 ambas de severidad "alta" y con puntuación asignada de 7.8. Estas vulnerabilidades se deben a una falla en el Win32k en Windows. Esto permitiría a un atacante realizar escalamiento de privilegios.

Se puede acceder al listado completo de vulnerabilidades aquí

Impacto:

Un atacante podría aprovechar todas estas vulnerabilidades críticas y dependiendo del tipo de ataque de ransomware obtener información confidencial, escalar privilegios, realizar ejecución remota de código (*RCE*), cifrar datos de la víctima, realizar denegación de servicio (DoS), entre otros.

Solución:

Existen varias medidas que pueden proporcionar una buena defensa contra una amplia gama de incidentes de seguridad relacionadas a ataques de ransomware. Algunas de ellas se detallan a continuación:

- Utilizar contraseñas con complejidad avanzada en los sistemas.
- Habilitar la autenticación de dos factores (2FA), en caso de que sea posible.
- Mantener actualizados todos los sistemas operativos y aplicaciones.
- Mantener el *firewall* de Internet habilitado y actualizado.
- Mantener un software de seguridad *Endpoint Detection and Response* (EDR) actualizado.
- Mantener copias de seguridad (Backups) y pruebas de restauración de datos.
- Activar la protección contra ransomware a través de la seguridad de Windows.

Información adicional:

- https://socradar.io/top-critical-vulnerabilities-used-by-ransomware-groups/
- https://socradar.io/what-is-ransomware-as-a-service-raas/
- BOL-CERT-PY-2022-38-Vulnerabilidades-de-dia-cero-en-Microsoft-Exchange-Server.pdf
- BOL-CERT-PY-2022-41-Vulnerabilidad-de-omision-de-autenticacion-en-FortiGate-y-FortiProxy.pdf
- BOL-CERT-PY-2022-14_Multiples_vulnerabilidades_en_productos_de_Fortinet.pdf
- BOL-CERT-PY-2022-40-Explotacion-masiva-de-vulnerabilidad-RCE-0-day-en-Zimbra-Actualizacion.pdf
- BOL-CERT-PY-2022-35-Vulnerabilidad-RCE-explotada-masivamente-en-Zimbra.pdf
- BOL-CERT-PY-2022-29_Vulnerabilidad_de_Unrar_Path_Traversal_afecta_en_Zimbra_Mail.pdf

- BOL-CERT-PY-2022-26_Vulnerabilidad_critica_en_Zimbra.pdf
- https://nvd.nist.gov/vuln/detail/CVE-2022-41352
- https://nvd.nist.gov/vuln/detail/CVE-2022-27925
- https://nvd.nist.gov/vuln/detail/CVE-2022-30333
- https://nvd.nist.gov/vuln/detail/CVE-2022-27924
- https://nvd.nist.gov/vuln/detail/cve-2019-19781
- https://nvd.nist.gov/vuln/detail/cve-2020-8195
- https://nvd.nist.gov/vuln/detail/CVE-2020-8196
- https://nvd.nist.gov/vuln/detail/cve-2019-11634
- https://nvd.nist.gov/vuln/detail/CVE-2018-13379
- https://nvd.nist.gov/vuln/detail/CVE-2018-13374
- https://nvd.nist.gov/vuln/detail/CVE-2021-26855
- https://nvd.nist.gov/vuln/detail/CVE-2020-0688
- https://nvd.nist.gov/vuln/detail/cve-2017-0199
- https://nvd.nist.gov/vuln/detail/CVE-2017-11882
- https://nvd.nist.gov/vuln/detail/CVE-2021-38647
- https://nvd.nist.gov/vuln/detail/CVE-2021-26084
- https://nvd.nist.gov/vuln/detail/CVE-2022-37986
- https://nvd.nist.gov/vuln/detail/CVE-2022-38050
- https://nvd.nist.gov/vuln/detail/CVE-2021-31166
- https://nvd.nist.gov/vuln/detail/CVE-2019-0543
- https://support.microsoft.com/es-es/windows/proteger-el-pc-contra-el-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3