# BOLETÍN DE ALERTA

**Boletín Nro.**: 2017-05
**Fecha de publicación**: 17/05/2017
**Tema**: Distribución de ransomware mediante ataques de fuerza bruta a RDP

**Descripción**:

En los últimos días se observó un aumento en los casos de una familia de ransomware llamada Dharma, que ha afectado a personas y empresas de nuestro país. Se trata de una variante del ransomware Wallet, cuya proliferación se observó en el país en el mes de diciembre, marzo y nuevamente ahora. El ransomware es implantado en los equipos explotando servicios RDP expuestos a Internet de forma insegura. También se ha observado un aumento de otras familias de ransomware tales como CrySIS (familia relacionada a Dharma), CryptoMix, ACCDFISA, entre otras, las cuales igualmente se implantan mediante la explotación de RDP.

**¿Qué es el Ransomware?**
Ransomware es un tipo de software malicioso (malware) que infecta un dispositivo y restringe el acceso al mismo, en la mayoría de los casos, encriptando documentos personales hasta que la víctima pague un "rescate" exigido por el malware para desencriptarlos.

**¿Cómo se transmite?**
Si bien, el Ransomware se puede transmitir de diversas formas (correos electrónicos con archivos adjuntos, sitios infectados, etc.), en el caso particular de la campaña de distribución de Dharma que se ha observado en nuestro país, se ha observado que se ha realizado ataques de fuerza bruta a equipos que cuentan con el servicio de Escritorio remoto (RDP - Remote Desktop Protocol) expuesto a Internet, con contraseñas débiles.



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py

**¿Cómo funciona Dharma?**

Al igual que la mayoría de las familias de ransomware, al quedar infectado, el ransomware se ejecuta e inmediatamente cifra la gran mayoría de los archivos y le añade una extensión característica. En el caso de Dharma, por ejemplo, la extensión añadida es filename.ID[VICTIM_16_CHAR_ID].[<email>].wallet

El ransomware encripta archivos con una gran cantidad de extensiones: desde las más comunes (.doc, .docx, .xlsx, .pdf, .png, .zip, etc.) hasta las más específicas, ya sea correspondientes a archivos de correo, de bases de datos, de código, máquinas virtuales, de diseño, etc.

Algo muy común en muchas de estas variantes es que además encriptan los directorios compartidos en red a los que el equipo tiene acceso, afectando así a un amplio número de usuarios.

Por lo general, el ransomware borra todas las instantáneas de recuperación (*Shadow Volume Copies*), de manera que no se pueden utilizar para restaurar los archivos de la víctima.

En algunos casos, al finalizar, el ransomware se auto-elimina del equipo, aunque en otros casos permanece latente en el sistema, de modo a seguir encriptando los nuevos archivos que se crean en la máquina. Luego, el ransomware despliega un mensaje en pantalla y/o como fondo de pantalla, como una "nota de rescate" en la que proporcionan las instrucciones para el pago del rescate y la recuperación de los archivos.


Figura 1: Mensaje de alerta desplegado por una de las versiones de Dharma



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py

El pago exigido es en bitcoins, y los montos pueden variar entre 500 a 1500 USD. En muchas de las variantes observadas, los cibercriminales exigen a la víctima que ésta contacte por correo electrónico, a través del cual le proporcionan las instrucciones específicas del pago, incluido el monto.

**¿Qué sistemas operativos afecta?**

Si bien, existen variantes de ransomware para casi cualquier sistema operativo, las familias observadas recientemente, tales como Dharma, CryptoMix, CrySIS, entre otras, afectan a equipos con sistema operativo Windows. Aquellos equipos y redes que cuentan con equipos con RDP habilitado, expuesto a Internet y con una contraseña débil son especialmente propensos a ser víctimas de estas familias de ransomware.

**Impacto**:

El ransomware encripta los archivos usando estándares de encriptación robusta (por lo general, RSA + AES-128), la cual no es reversible, por lo tanto lleva a una pérdida de los archivos.

Esto genera enormes daños, entre ellos:

- Pérdida temporal o permanente de información confidencial o de propiedad;
- La interrupción de las operaciones regulares, principalmente en los negocios o empresas;
- Las pérdidas financieras contraídas para restaurar los sistemas y archivos; y
- Daño potencial a la reputación de una organización.

En el caso que se cuente con copias de seguridad actualizadas de los archivos, el impacto puede ser significativamente menor.

**Solución:**

En la gran mayoría de los casos, no existen mecanismos para desencriptar los archivos sin la clave que está en poder de los atacantes. Sin embargo, en ocasiones, es posible que después de un tiempo se descubra una solución. Esto normalmente se puede dar de dos formas:

1. Se descubre una falla de seguridad en el propio ransomware, que puede ser explotada y permite recuperar los archivos
2. Una investigación del grupo criminal lleva a la recuperación de las claves de las víctimas.

Es posible que en un futuro se diera una de estas situaciones, encontrándose así una solución. Es por eso que se recomienda guardar los archivos encriptados, no eliminarlos.



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py

En el caso de la última variante de Dharma/Wallet/CrySIS, los cibercriminales han publicado las claves de descifrado en PasteBin, por lo que es posible que las víctimas puedan descifrar sus archivos de esta manera. La banda cibercriminal de esta familia de ransomware ya ha hecho esto en el pasado: en noviembre del año pasado han publicado las claves de CrySIS (http://www.cert.gov.py/application/files/2714/7930/0272/Boletin_20161116_CrySIS.pdf), en marzo hay publicado las claves de una variante de Dharma y días atrás han publicado las claves de Wallet/Dharma.
Varias empresas de seguridad han publicado herramientas que sirven para descifrar archivos cifrados por estas familias de ransomware y otras:

- Avast Decryptors: varias herramientas para familias de ransomware, entre ellas CrySIS/Dharma, incluida la última versión, cuya clave se liberó días atrás
  https://www.avast.com/ransomware-decryption-tools
- Kaspersky Decryptors: varias herramientas para varias familias de ranomsware, entre ellas Crysis/Dharma
  https://noransom.kaspersky.com/
- ESET CrySIS Decryptor: Herramienta para algunas variantes de CrySIS
  https://download.eset.com/com/eset/tools/decryptors/crysis/latest/esetcrysisdecryptor.exe

Debe tenerse en cuenta que, aunque ocasionalmente se da a conocer una manera de descifrar los archivos, esto normalmente suele coincidir con el inicio de la distribución de otras familias de ransomware.

**Mitigación y Prevención:**
Teniendo en cuenta que en la gran mayoría de las familias de ransomware no es posible recuperar los archivos cifrados, es fundamental tomar las medidas preventivas, como ser:

- Verificar los accesos de RDP (Escritorio remoto) expuestos a Internet y asegurar que las contraseñas de todos los usuarios sean robustas (10 a 12 caracteres como mínimo, evitar palabras comunes, combinar minúsculas, mayúsculas, números, símbolos, etc.). Verificar además otros mecanismos de acceso remoto, tales como SSH, TeamViewer y otros. En caso de tener habilitado RDP u otros mecanismos de acceso remoto, deshabilitarlo en caso de que no sea estrictamente necesario.
- No abrir nunca correos sospechosos, tanto si vienen de usuarios conocidos como desconocidos. Asegurarse siempre de que la persona que le ha enviado el correo realmente le quería remitir ese adjunto.



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py

- Evitar abrir los archivos adjuntos sospechosos. Incluso los archivos aparentemente inofensivos, como los documentos de Microsoft Word o Excel, pueden contener un virus, por lo que es mejor ser precavido.
- No ingresar a enlaces dudosos que le son enviados a través de correo electrónico, servicios de mensajería, redes sociales, etc.
- Realizar copias de seguridad (backup) de toda la información crítica para limitar el impacto de la pérdida de datos o del sistema y para facilitar el proceso de recuperación. Idealmente, estas copias deben hacerse de forma regular y deben mantenerse en un dispositivo independiente (disco duro externo, o servicios en la nube como OneDrive, Dropbox, etc.)
- Contar con soluciones de antivirus/firewall y mantenerlo actualizado, de modo a prevenir la infección.
- Mantener su sistema operativo y el software siempre actualizado, con los últimos parches.
- No acceder nunca a ningún pago u acción exigida por el atacante. Además de no existir ninguna garantía por parte de los cibercriminales, en muchas ocasiones, víctimas que han pagado el rescate no han podido recuperar sus archivos.

En caso de víctima de ransomware se recomienda realizar la denuncia a los organismos correspondientes; puede reportarlo al Centro de respuestas ante Incidentes Cibernéticos (CERT-PY).

**Información adicional:**

https://www.bleepingcomputer.com/news/security/new-version-of-the-cryptomix-ransomware-using-the-wallet-extension/

https://bestsecuritysearch.com/new-campaign-crysis-ransomware-rdp-brute-force-attacks/

https://blog.barkly.com/blocking-dharma-ransomware-before-it-encrypts-files

https://www.bleepingcomputer.com/news/security/wallet-ransomware-master-keys-released-on-bleepingcomputer-avast-releases-free-decryptor/

https://www.bleepingcomputer.com/news/security/alleged-master-keys-for-the-dharma-ransomware-released-on-bleepingcomputer-com/



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py