Nro. Alerta:	EC-2022-20	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	03-febrero-2022	**Ransomware PYSA y Lockbit.**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Contenido dañino
Tipo de incidente: Malware
Nivel de riesgo: Alta

II. ALERTA

Analistas de seguridad NCC Group, ESET Latinoamérica dan a conocer características de funcionamiento de PYSA y Lockbit, actores de amenazas que dominan el panorama del ransomware.

Figura 1.- Ilustración asociada a Ransonware
Fuente: INCIBE

III. INTRODUCCIÓN

Ransomware es un malware diseñado para cifrar archivos en un dispositivo, una particularidad es que los actores malintencionados exigen un rescate a cambio del descifrado. En los últimos años, los incidentes de ransomware se han vuelto cada vez más frecuentes entre las entidades gubernamentales estatales, locales.

En este sentido, se mencionaran características de PYSA y Lockbit; que son los ataques con mayor incidencia.

Ransomware PYSA (Protect Your System Amigo))

- Opera desde el 2019.
- Malware de tipo Ransomware-as-a-Service (RaaS); es decir, implica que los desarrolladores de este ransomware reclutan afiliados que se encargan de la distribución de la amenaza .
- Secuestra, cifra y pide rescate por los datos.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-20	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	03-febrero-2022	**Ransomware PYSA y Lockbit.**	Versión 1.0

- Si no pagas cold-calling (llamadas telefónicas presionando a las compañías).
- Tanto el FBI como la agencia de ciberseguridad de Francia le siguen el rastro a este malware debido a las víctimas de alto calibre que fueron afectadas.
- PYSA cuentan con un sitio en la Dark web, a diciembre del 2021 indicaron que tenía 307 víctimas.

LockBit

- Se tiene registro de actividades desde el 2019.
- Es una de las familias de ransomware más prolíficas en el ámbito de amenazas.
- Se enfoca en el cifrado de máquinas virtuales VMware y ESXi.
- Malware de tipo Ransomware-as-a-Service (RaaS).
- Utiliza una combinación de algoritmos de cifrado AES y criptografía de curva elíptica para el cifrado de datos
- Los creadores han desarrollado sus tácticas para crear cifrados de Linux.
- LockBit tiene capacidades de registro y puede almacenar la siguiente información: información del procesador, Volúmenes en el sistema, Máquinas virtuales (VM) para omitir, Archivos totales, Máquinas virtuales totales, Archivos cifrados, Máquinas virtuales cifradas, Tamaño cifrado total y Tiempo dedicado al cifrado.
- Contiene instrucciones para cifrar imágenes de VM alojadas en servidores ESXi.

IV. VECTOR DE ATAQUE:

A continuación, se describen los vectores de ataque de PYSA y Lockbit.

PYSA

Previo al ataque:

Realizan tareas de reconocimiento dentro de los sistemas para recolectar otras credenciales, escalar privilegios, moverse lateralmente dentro de la red comprometida, etc.

Para obtener acceso:

1. Correos electrónicos con phishing elaborados a medida del objetivo (spearphishing).
2. Ataques de fuerza bruta contra sistemas desprotegidos con el protocolo RDP expuestos públicamente.

Ejecución

1. Crea un mutex para asegurarse que no haya otras instancias del ransomware corriendo en

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

el mismo equipo.

2. Crea hilos de ejecución que se encargarán del mecanismo de cifrado.
3. Modifica de los registros del sistema para que la nota de rescate que se muestra a la víctima se abra cada vez que el equipo inicia.
4. Prepara un script, llamado update.bat, para luego remover cualquier rastro de la amenaza en materia de archivos.
5. Examina el sistema de archivos del equipo y genera dos listas, llamadas:
6. Allowlist: incluyen archivos con extensiones:.doc, .db, .zip, entre otros, y sean de mayor tamaño a 1 KB.
7. Blacklist. Se incluyen directorios críticos para el funcionamiento del sistema (como “C:\Windows”), ya que cifrarlos dificultaría el posible descifrado por parte de los atacantes. Al finalizar, todo archivo o directorio que no esté incluido en ninguna de las dos listas es marcado como “Allow”.
8. Cifra el contenido de la lista “Allowlist” y no modifica aquellos archivos en la blacklist.
9. Los archivos robados se utilizan en las negociaciones de rescate, donde los atacantes amenazan con divulgar públicamente los datos si no se paga el rescate.

En la siguiente figura, se observa una imagen asociada a PYSA.

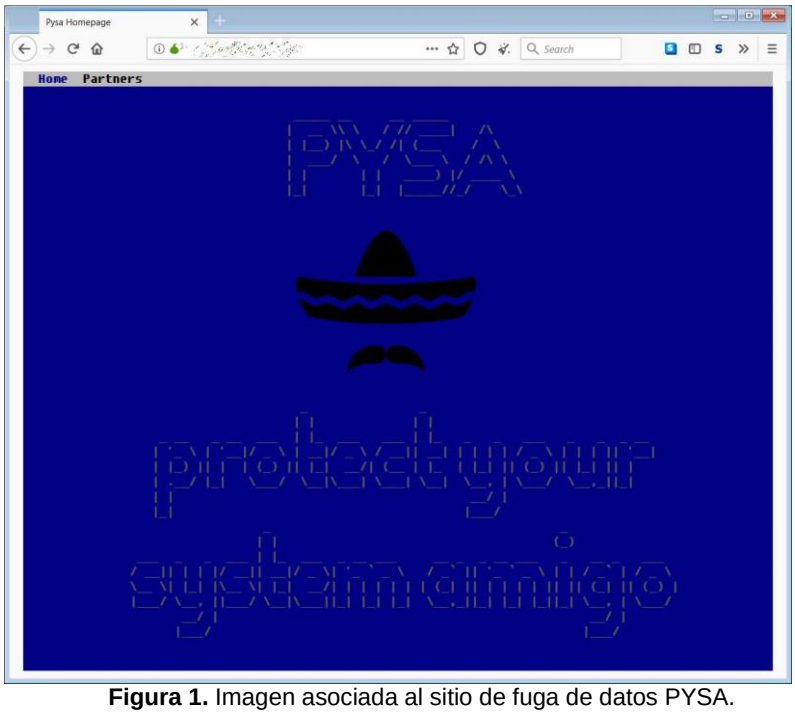

Figura 1. Imagen asociada al sitio de fuga de datos PYSA.

Nro. Alerta:	EC-2022-20	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	03-febrero-2022	**Ransomware PYSA y Lockbit.**	Versión 1.0

LockBit

1. Proporciona una interfaz de línea de comandos que permite a los afiliados habilitar y deshabilitar varias funciones para adaptar sus ataques; por ejemplo se puede especificar el tamaño de un archivo y cuántos bytes cifrar, si dejar de ejecutar máquinas virtuales o borrar el espacio libre después. En la siguiente figura se indica la interfaz de línea de comandos.

```
Usage: %s [OPTION]... -i '/path/to/crypt'
Recursively crypts files in a path or by extention.

Mandatory arguments to long options are mandatory for short options too.
  -i, --indir         path to crypt
  -m, --minfile       minimal size of a crypted file, no less than 4096
  -r, --remove        self remove this file after work
  -l, --log           prints the log to the console
  -n, --nolog         do not print the log to the file /tmp/locker.log
  -d, --daemonize     runs a program as Unix daemon
  -w, --wholefile     encrypts whole file
  -b, --beginfile     encrypts first N bytes
  -e, --extentions    encrypts files by extentions
  -o, --nostop        prevent to stop working VM
  -p, --wipe          wipe free space
  -s, --spot          upper bound limitation value of spot in Mb
```

Figura 2. Imagen asociada a los argumentos de la línea de comandos del cifrador LockBit.

2. Una característica particular del cifrador de Linux LockBit es el amplio uso de las utilidades de línea de comandos VMware ESXI y VMware vCenter para verificar qué máquinas virtuales se están ejecutando y apagarlas limpiamente para que no se dañen mientras se cifran.
3. Una vez que los datos han sido cifrados por LockBit aparece la nota de rescate; como se indica en la siguiente figura.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-20	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	03-febrero-2022	**Ransomware PYSA y Lockbit.**	Versión 1.0

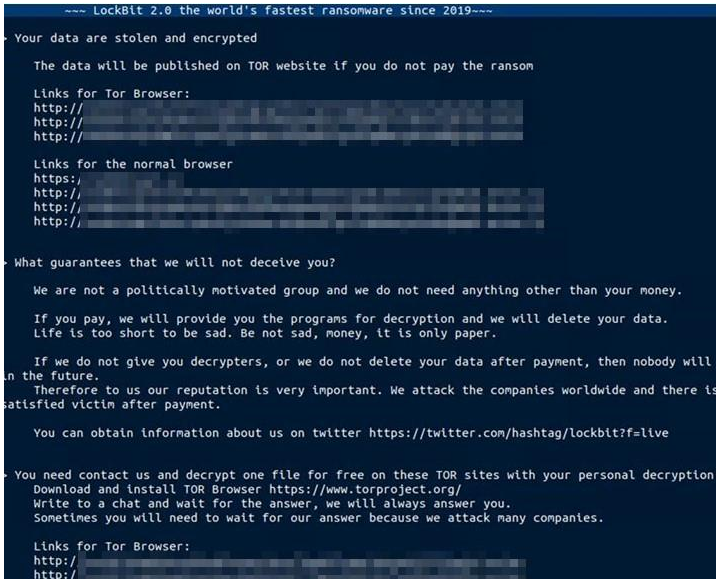

Figura 3. Imagen asociada a la nota de rescate de LockBit.

V. INDICADORES DE COMPROMISO:

A continuación, se mencionan indicadores de compromiso asociado a PYSA.

Indicador	Detalle	
File Extension of encrypted files:	.pysa	
Observed malware filename:	\Users\%username%\Downloads\svchost.exe	
SHA1 Hashes:	Unknown	07cb2a3fe86414b054e2b002f283935bb0cb993c
	svchost.exe	52b2fc13ec0dbf8a0250c066cd3486b635a27827
	svchost.exe	728CB56F98EDBADA697FE66FBF7D367215271F10
	17535.pyz	c74378a93806628b62276195f9657487310a96fd
	Step2.ps1	24c592ad9b21df380cb4f39a85d4375b6a8a6175
Tor URLs:	pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad.onion na47pldl5eoqxt42.onion	

Tabla 1. IOC de PYSA

Continuando con los indicadores de compromiso, en la siguiente tabla se mencionan indicadores de compromiso asociado a Lockbit.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-20	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	03-febrero-2022	**Ransomware PYSA y Lockbit.**	Versión 1.0

Indicador	Detalle
SHA256	• f3a1576837ed56bcf79ff486aadf36e78d624853e9409ec1823a6f46fd0143ea • 67df6effa1d1d0690c0a7580598f6d05057c99014fcbfe9c225faae59b9a3224 • ee3e03f4510a1a325a06a17060a89da7ae5f9b805e4fe3a8c78327b9ecae84df

Tabla 2. IOC de Lockbit

Regla YARA:

```
regla Linux_Lockbit_Jan2022 {
  meta:
    description = "Detecta una versión de Linux del ransomware Lockbit"
    autor = "Investigación de TrendMicro"
    fecha = "2022-01-24"
    hash1 =
"038ff8b2fef16f8ee9d70e6c219c5f380afe1a21761791e8cbda21fa4d09fdb4"
   instrumentos de cuerda:
     $xor_string_1 = "LockBit Linux/ESXi casillero V:" xor(0x01-0xff)
     $xor_string_2 = "LockBit 2.0, el ransomware más rápido del mundo
desde 2019" xor(0x01-0xff)
     $xor_string_3 = "ID de tóxicos LockBitSupp" xor(0x01-0xff)
  condición:
    uint16(0) == 0x457f y tamaño de archivo < 300KB y
    tamaño de archivo > 200KB y cualquiera de ellos

}
```

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- No abrir, manipular, o interactuar con comunicaciones altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Implementar contraseñas fuertes y el doble factor de autenticación para evitar ataques de fuerza bruta.
- Descargar programas y archivos de fuentes oficiales.
- Mantener actualizado el sistema de seguridad implementado.
- Configurar correctamente los protocolos de escritorio remoto (RDP), e inhabilitar aquellos que no sean necesarios.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de información.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

- Mantener los sistemas actualizados con los últimos parches de seguridad para evitar intrusiones.
- En el caso de que la Organización/Institución se vea afectada por un ransomware, lo más importante es NO PAGAR nunca el rescate.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VII. REFERENCIAS:

Abrams, L. (26 de 01 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/linux-version-of-lockbit-ransomware-targets-vmware-esxi-servers/

Ciberseguridadlatam. (03 de 02 de 2022). *Ciberseguridadlatam*. Obtenido de Ciberseguridadlatam: https://www.ciberseguridadlatam.com/2022/02/02/ransomware-pysa-caracteristicas-de-uno-de-los-grupos-mas-activos-de-2021/

CISA. (s.f.). *CISA*. Obtenido de CISA: https://www.cisa.gov/stopransomware/ransomware-guide

Dela Cruz, J. (24 de 02 de 2022). *Trendmicro*. Obtenido de Trendmicro: https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0122_ImpactofLockbit

Federal Bureau of Investigation, C. D. (s.f.). *Federal Bureau of Investigation, Cyber Division*. Obtenido de https://www.ic3.gov/Media/News/2021/210316.pdf

GROUP, N. (s.f.). *NCC GROUP*. Obtenido de NCC GROUP: https://newsroom.nccgroup.com/news/ncc-group-monthly-threat-pulse-november-2021-439934

INCIBE. (s.f.). *INCIBE*. Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

Segu-Info. (27 de 01 de 2022). *Segu-Info*. Obtenido de Segu-Info: https://blog.segu-info.com.ar/2022/01/lockbit-nuevo-ransomware-para-linux-y.html

Toulas, B. (s.f.). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/pysa-ransomware-behind-most-double-extortion-attacks-in-november/