RANSOMWARE as a Service

SEGU.INFO
SEGURIDAD DE LA INFORMACION

SIGESTIC'23

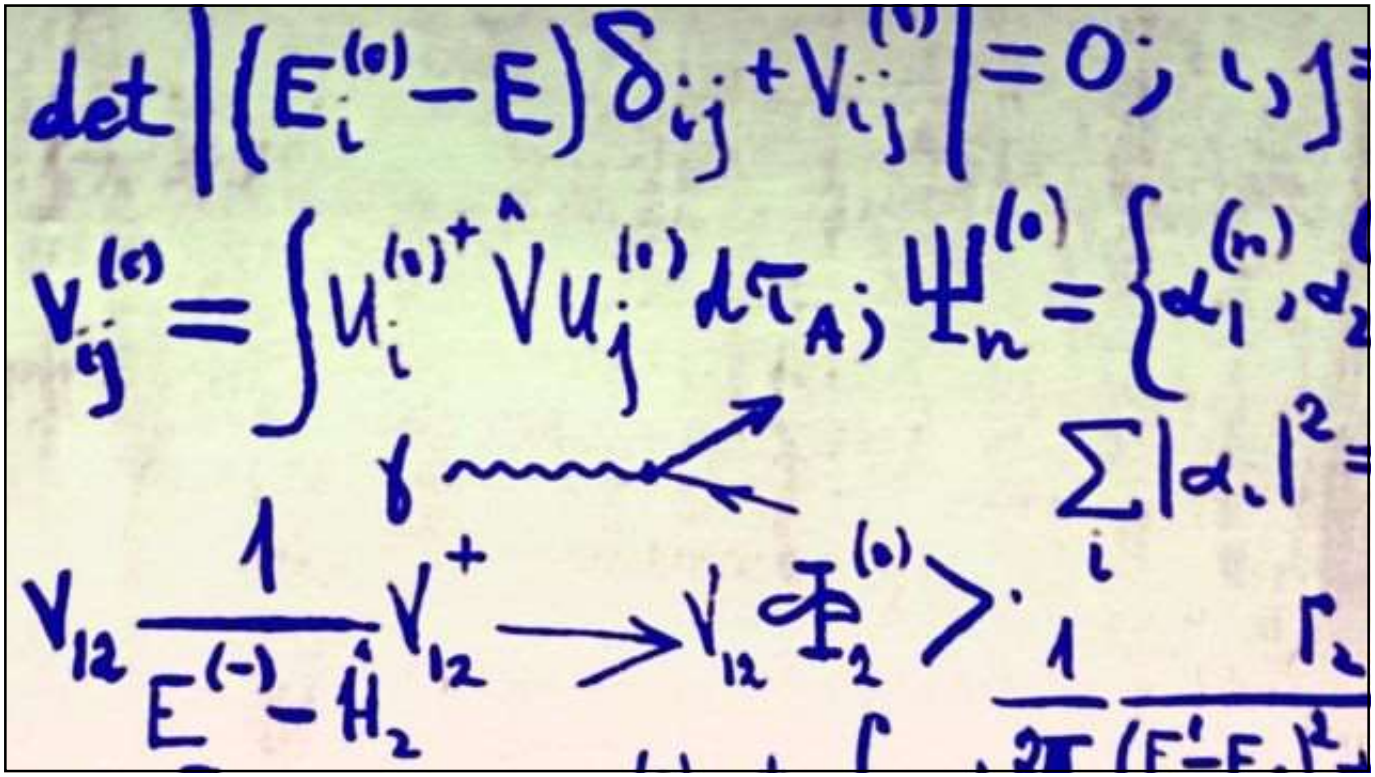
Lic. Cristian Borghello
CISSP – CCSK – CSFPC
www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo

Sobre Cristian Borghello (AR)

- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP *(Certified Information Systems Security Professional)*
- Microsoft MVP Security durante 10 años
- CCSK *(Certificate Cloud Security Knowledge)*
- CSFPC *(Certification Cyber Security Foundation)*
- Certificado en Ciberseguridad en Corea del Sur
- Profesor Universitario de Grado y Posgrado
- Entrenador en Ciberseguridad para la ONU
- Creador de Segu-Info, Segu-Kids, ODILA y Antiphishing.LA

El “poder”de las IPs ☺

El “poder”de las IPs ☺



Cibercrimen

- **Primera era:** ataques y creación de malware amateur *"por hobby"*
- **Segunda era:** fusión entre el crimen organizado e Internet
- **Tercera era:** combinación de las dos anteriores, con injerencias geopolíticas
- **Contra las personas:** pornografía, violación a la privacidad, suplantación de identidad, etc.
- **Contra las propiedades:** bandalismo, ataques de malware, robo de información, CaaS, etc.
- **Auspiciado por los Estados y bien financiados**

Servicios delictivos

- **CyberCrime as a Service (CaaS):** modelo de negocio para recolectar, comprar y vender información obtenida en forma fraudulenta.
- **Criminal to Criminal (CtC):** servicios y negocios criminales realizados en Internet.
- **Hacking as a Service (HaaS):** *cracking* de cuentas que permite obtener datos que, posteriormente, serán utilizados para cometer otros delitos.
- **Malware as a Service (MaaS):** modelo para difundir e instalar malware a medida y bajo el modelo *Pay-per-Install*.

Crecimiento del Cibercrimen

Modelo de organizaciones criminales centradas en el malware y distribuidas en Internet para generar ingresos rápidos

Segmentación de los servicios

- **Data as a Service (DaaS):** almacenamiento y control de datos sensibles robados a terceros, como cuentas en perfiles sociales, datos personales, datos médicos, números de cuenta, etc.
- **Translation as a Service (TaaS):** servicios de traducción y localización para campañas de *phishing* y fraude multi-idioma y/o multi-región.
- **BulletProof Services:** alojamiento web (IaaS) que permite cualquier tipo de contenido y asegura resiliencia.
- **Money Laundering as-a-service (MLaaS):** servicio de mulas para blanquear dinero mediante transferencias internacionales (mueve dinero FIAT y Cripto).

Malware

Malicious Software

Cualquier programa potencialmente dañino para el sistema

Remote Access Trojan

RAT

Gusano

Troyano

Backdoors

Adware

MALWARE

Spyware

Rootkit

VIRUS

Keylogger

Ransomware

Botnet

Ransomware

Tipo de troyano que “secuestra” (cifra) archivos y pide un rescate económico por los mismos

Ransomware as a Service (RaaS)

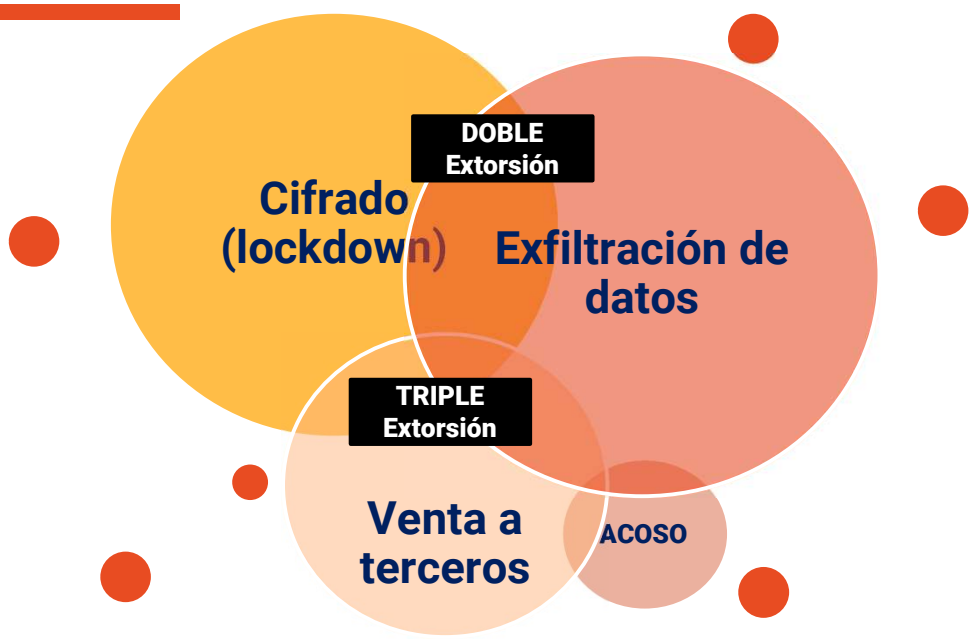
Modelo de negocio entre el **desarrollador** o el **operador** del *ransomware* y **afiliados**

- El ransomware es desarrollado por los operadores (habilidad “alta”)
- Los afiliados infectan y lanzan los ataques de *ransomware* a las víctimas (habilidad “baja”)

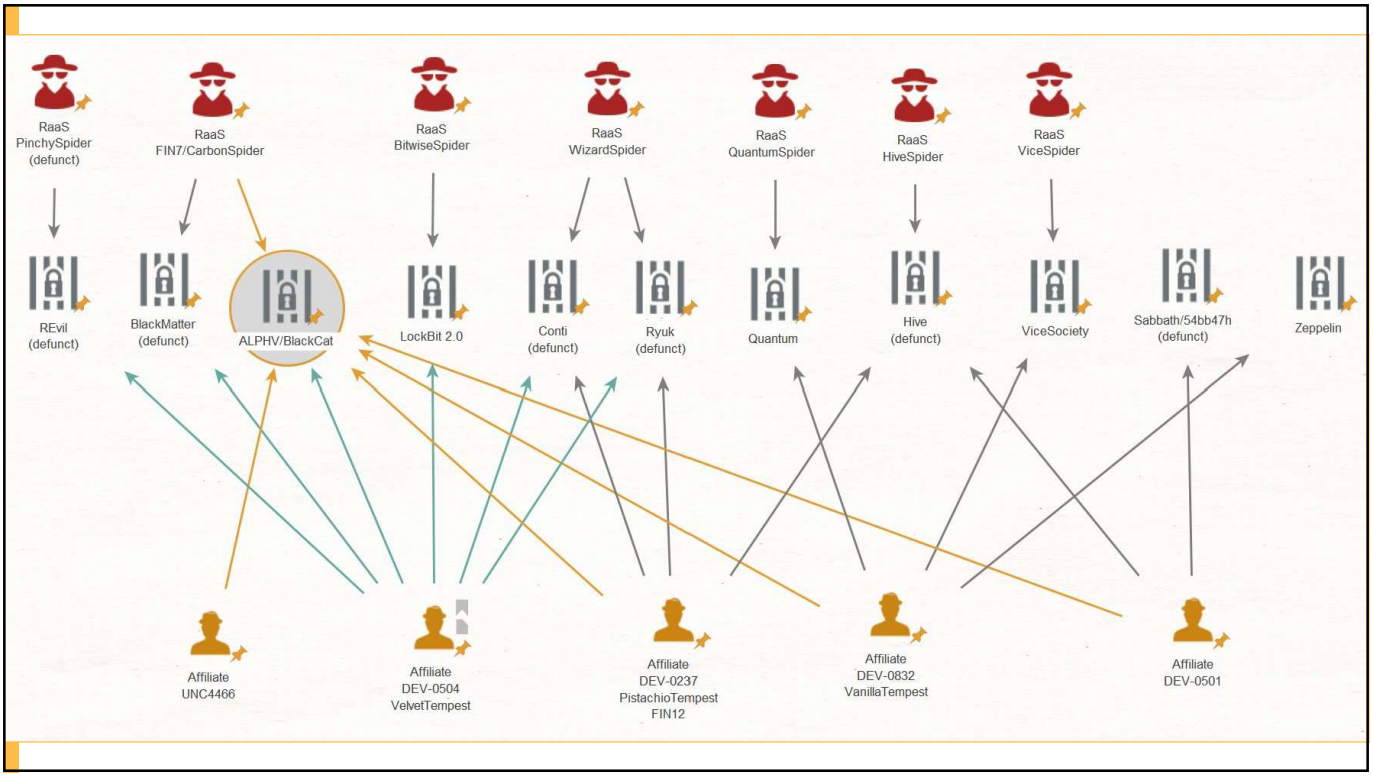
Modelos de negocio RaaS

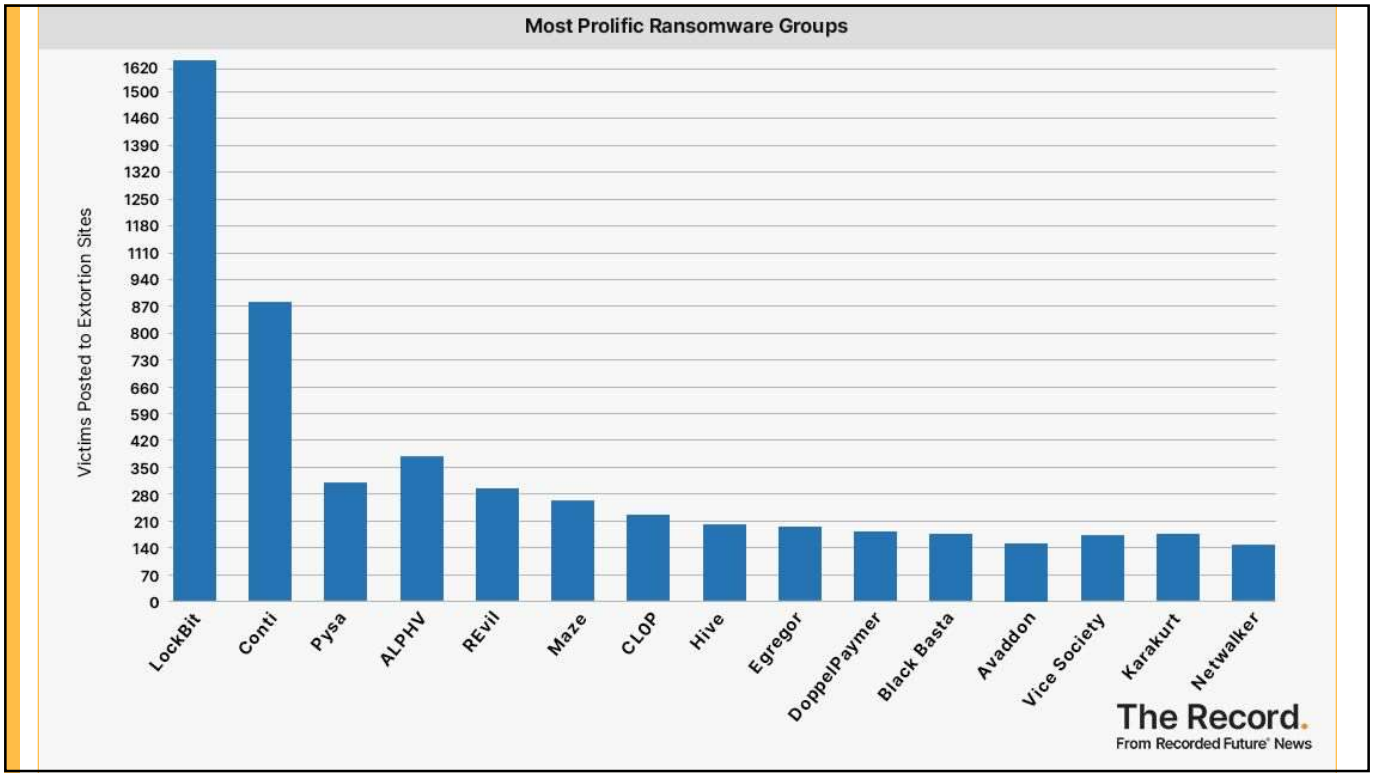
1. Suscripción mensual por una tarifa plana
2. Tarifa de licencia única sin participación en las ganancias
3. Programas de afiliados con un porcentaje de las ganancias (20-30%) para el desarrollador del *ransomware*
4. …

Extorsiones

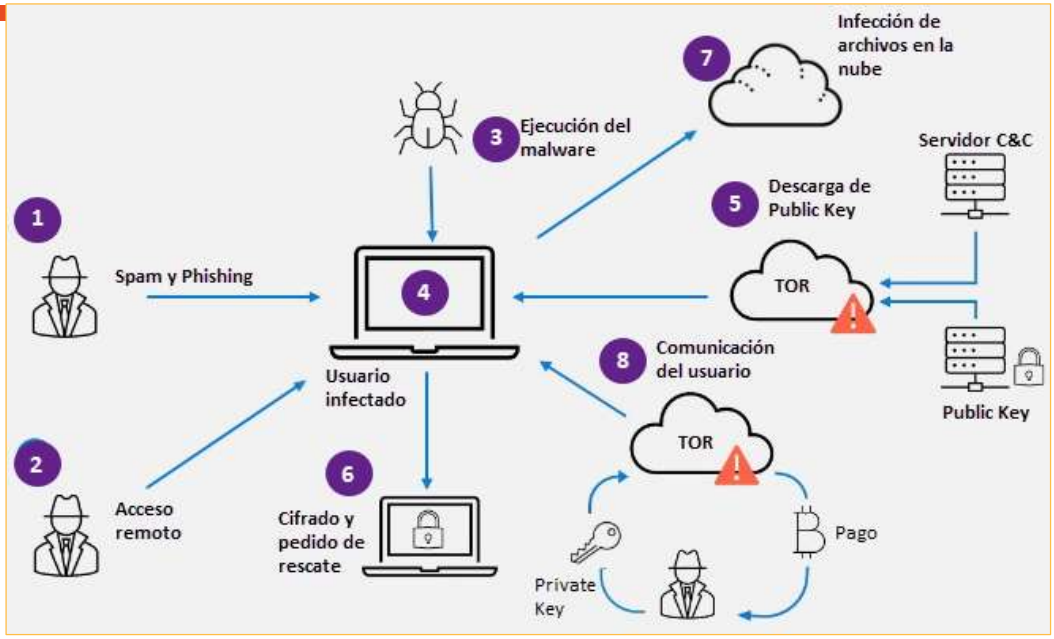


Panorama Internacional y Cibercrimen



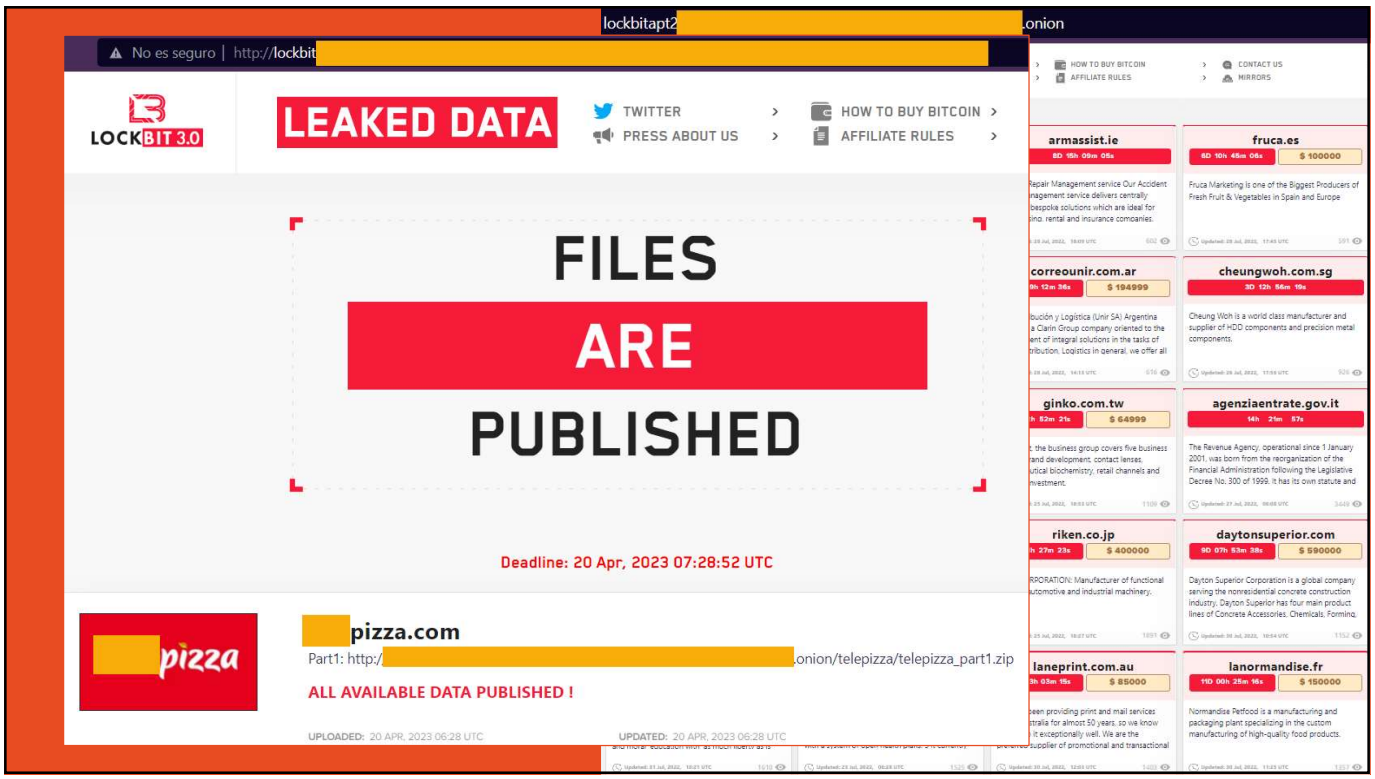


Anatomía de un ataque de ransomware



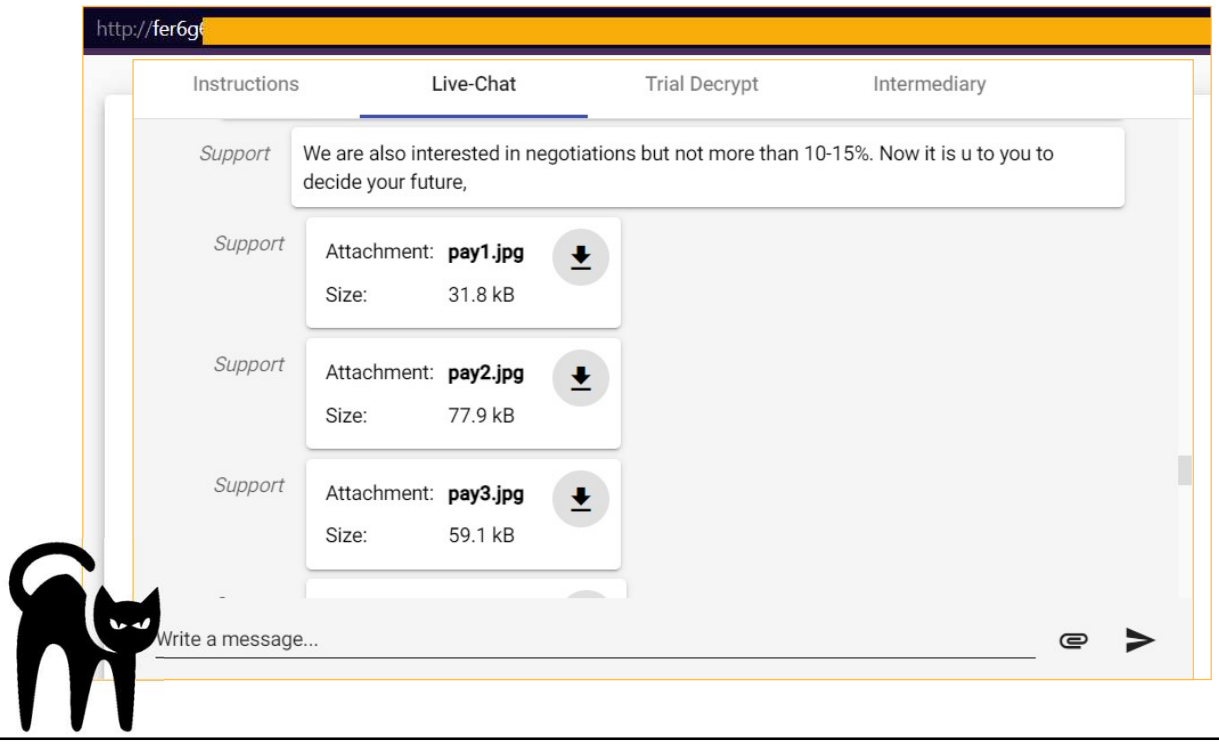
Lockbit

- Disponible desde 2019
- Similar a Revil y Sodinokibi
- Se anuncia como el *"software de cifrado más rápido del mundo"*. Algunas estimaciones sugieren que está detrás del 40% de todos los ataques de ransomware.
- Existen versiones (*in-progress*) para Win, macOS, ARM, FreeBSD, MIPS, SPARC y VMware ESXi



Alphv / BlackCat y Babuk

- **Alphv / BlackCat:** basado en el lenguaje Rust
- Formado por ex-miembros de REvil y conectado a los grupos BlackMatter y DarkSide
- Explota fallas de seguridad conocidas o credenciales de cuentas vulnerables; puede lanzar ataques DDoS para presionar a la víctima
- **Babuk:** especializado en VMware ESXi
- Existen decenas de variantes desde su código filtrado en 09/2021



Malware “benéfico”

Somos malas... podemos ser peores Releases RSS

Defaulters

We offer simple deal, you pay you get decrypter, we forget about you and your problems are solved. Ignoring🙈🙈 a problem doesn’t solve it. Restoring from your backups without decrypter doesn’t solve it either. Unless you want your data sold or published, and journalists and your clients finding you not fulfilling your obligations.

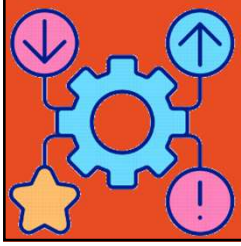
```
find /opt/zimbra/ -name README.txt

/opt/zimbra/common/lib/policyd-2.1/cbp/modules/README.txt
/opt/zimbra/jetty_base/webapps/zimbra/downloads/README.txt
/opt/zimbra/backup/README.txt
/opt/zimbra/extensions-extra/openidconsumer/README.txt
/opt/zimbra/store/0/1/msg/0/README.txt
/opt/zimbra/store/0/1/msg/README.txt
/opt/zimbra/store/0/1/README.txt
/opt/zimbra/store/0/7/msg/0/README.txt
/opt/zimbra/store/0/7/msg/README.txt
/opt/zimbra/store/0/7/README.txt
/opt/zimbra/store/0/8/msg/0/README.txt
/opt/zimbra/store/0/8/msg/1/README.txt
/opt/zimbra/store/0/8/msg/README.txt
/opt/zimbra/store/0/8/README.txt
/opt/zimbra/store/0/9/msg/0/README.txt
/opt/zimbra/store/0/9/msg/README.txt
/opt/zimbra/store/0/9/README.txt
/opt/zimbra/store/0/10/msg/0/README.txt
/opt/zimbra/store/0/10/msg/1/README.txt
/opt/zimbra/store/0/10/msg/2/README.txt
/opt/zimbra/store/0/10/msg/3/README.txt
/opt/zimbra/store/0/10/msg/4/README.txt
/opt/zimbra/store/0/10/msg/5/README.txt
/opt/zimbra/store/0/10/msg/6/README.txt
/opt/zimbra/store/0/10/msg/7/README.txt
/opt/zimbra/store/0/10/msg/8/README.txt
/opt/zimbra/store/0/10/msg/9/README.txt
/opt/zimbra/store/0/10/msg/10/README.txt
/opt/zimbra/store/0/10/msg/README.txt
/opt/zimbra/store/0/10/README.txt
/opt/zimbra/store/0/12/msg/0/README.txt
/opt/zimbra/store/0/12/msg/README.txt
/opt/zimbra/store/0/12/README.txt
/opt/zimbra/store/0/15/msg/0/README.txt
/opt/zimbra/store/0/15/msg/README.txt
/opt/zimbra/store/0/15/README.txt
/opt/zimbra/store/0/13/msg/0/README.txt
/opt/zimbra/store/0/13/msg/README.txt
/opt/zimbra/store/0/13/README.txt
/opt/zimbra/store/0/16/msg/0/README.txt
/opt/zimbra/store/0/16/msg/README.txt
/opt/zimbra/store/0/16/README.txt
/opt/zimbra/store/0/17/msg/0/README.txt
/opt/zimbra/store/0/17/msg/README.txt
/opt/zimbra/store/0/17/README.txt
/opt/zimbra/store/0/19/msg/0/README.txt
/opt/zimbra/store/0/19/msg/README.txt
/opt/zimbra/store/0/19/README.txt
```

Medidas de Protección

Personas

- Definir una Política de Seguridad de la Información relacionada a incidentes de ransomware
- Capacitación, Concientización y Educación de **todos** los empleados de forma regular
- Segregación de funciones, roles y permisos
- Administración de los riesgos en la cadena de suministro

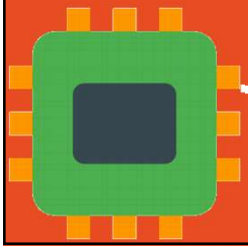
Medidas de Protección



Procesos

- Desarrollar e implementar una estrategia de ciberseguridad con roles y responsabilidades claros
- Desarrollar las medidas de mitigación de riesgos
- Implementar estándares de seguridad (ISO 27001, PCI, NIST,CSA, etc.)
- Realizar evaluaciones de vulnerabilidades periódicas

Medidas de Protección



Tecnología

- Redundancia de datos (backup + restore)
- Cifrado de datos sensibles
- Hardening de aplicaciones en nubes y sistemas
- Actualizaciones de seguridad regulares
- Desinstalar aplicaciones innecesarias e implementar control cambios
- Segmentación de red
- MFA (sin excepción)
- Herramientas de detección bloqueo proactivo

¿PREGUNTAS?

GRACIAS!

SEGU.INFO
SEGURIDAD DE LA INFORMACION

SIGESTIC'23

Lic. Cristian Borghello
CISSP – CCSK – CSFPC
www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo