Ransomware en la banca

Ing. Demian García

DISC 2020

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Descargo de responsabilidad

Los comentarios, opiniones y otras aseveraciones expresadas en ésta plática se realizan a título personal y no representan, ni buscan representar, una postura oficial de mi empleador actual o de algún empleador previo.

La información presentada a continuación es de carácter público y no pretende violar ningún acuerdo de confidencialidad, tiene por objetivo único servir como material de divulgación sin fines de lucro.

$ whoami

Demian García

- Responsable de la función de Inteligencia de Ciberamenazas en Banco Santander México.
- Durante los últimos 7 años he sido parte de equipos de Respuesta a Incidentes realizando tareas de gestión, análisis forense e inteligencia de ciberamenazas.
- Orgulloso ex colaborador de UNAM-CERT.

Ransomware en la banca

DISC
2020

Ransomware

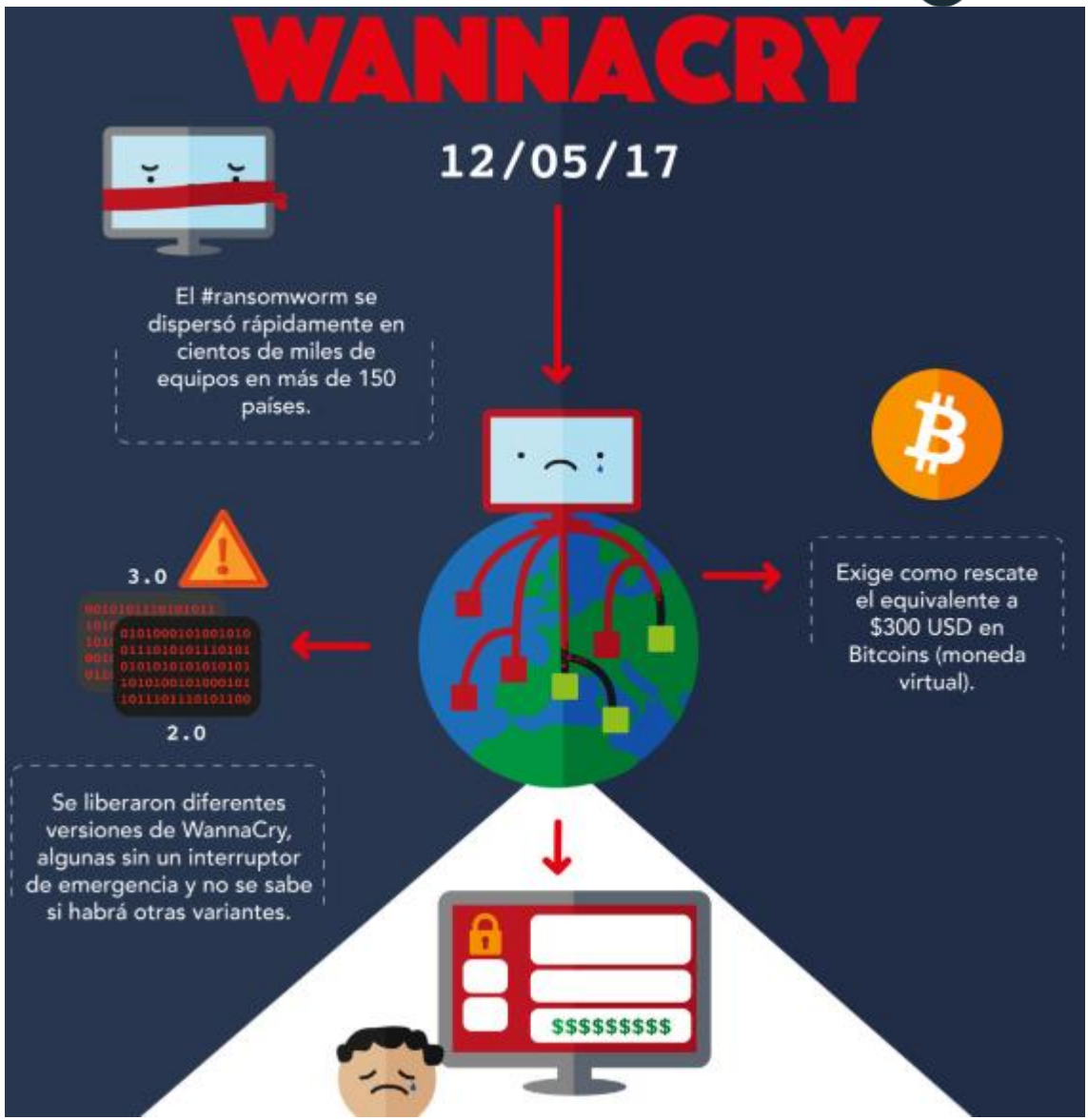
Ransom + Software

(Rescate)

Ransomware: Código malicioso que secuestra la información de un equipo de cómputo y exige un rescate para liberar los datos.

¡Ataque! WannaCry

En mayo de 2017 el mundo entero fue afectado por un ataque masivo de ransomware, hospitales, compañias de telefonía, universidades, ciudadanos de internet, entre otros sufrieron el secuestro de sus datos por wannacy.



Fuente:

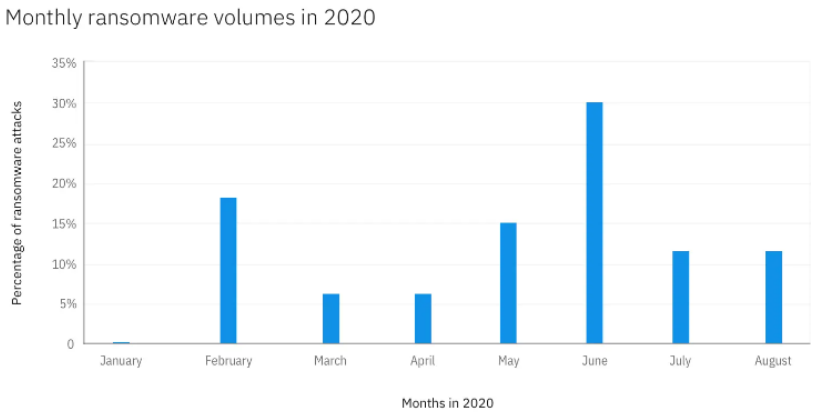
https://www.cert.org.mx/ataque-wannacry

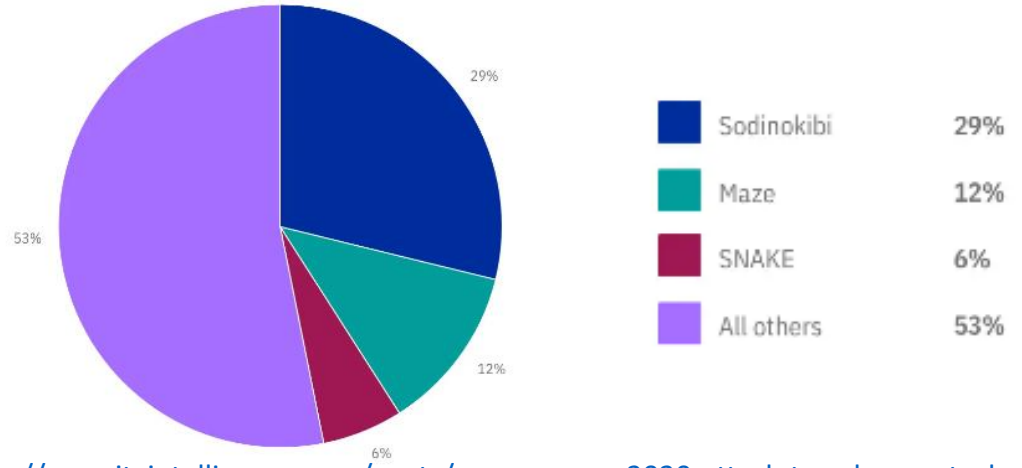
$ Ransomware, una tendencia

Los ataques de ransomware continúan en aumento y son una de las principales amenazas para las organizaciones y gobiernos. En 2020 se ha convertido en un grave problema para organizaciones en todo el mundo.

Ransomware 2020: Attack Trends Affecting Organizations Worldwide

September 28, 2020 | By **Camille Singleton** co-authored by **Christopher Kiefer, Ole Villadsen** | 9 min read



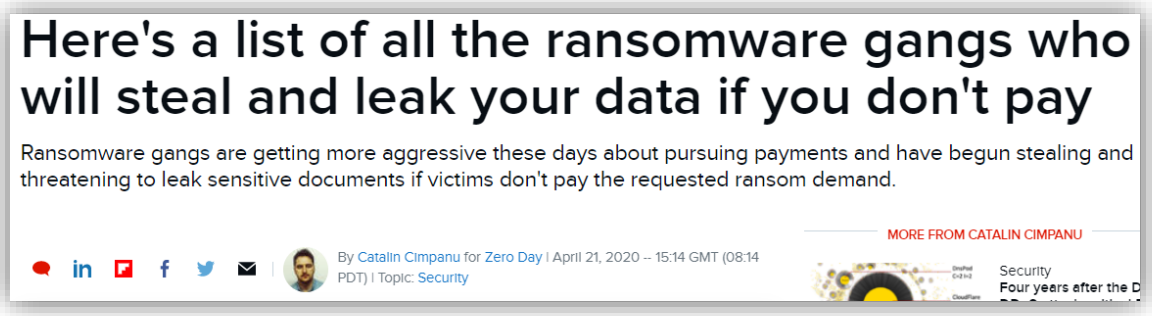


https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

¿Por qué?

Los grupos criminales detrás de los ataques de ransomware tienen una fuerte **motivación económica.**

¿Quién?


Here's a list of all the ransomware gangs who will steal and leak your data if you don't pay

Ransomware gangs are getting more aggressive these days about pursuing payments and have begun stealing and threatening to leak sensitive documents if victims don't pay the requested ransom demand.

By Catalin Cimpanu for Zero Day | April 21, 2020 -- 15:14 GMT (08:14 PDT) | Topic: Security

MORE FROM CATALIN CIMPANU

Security

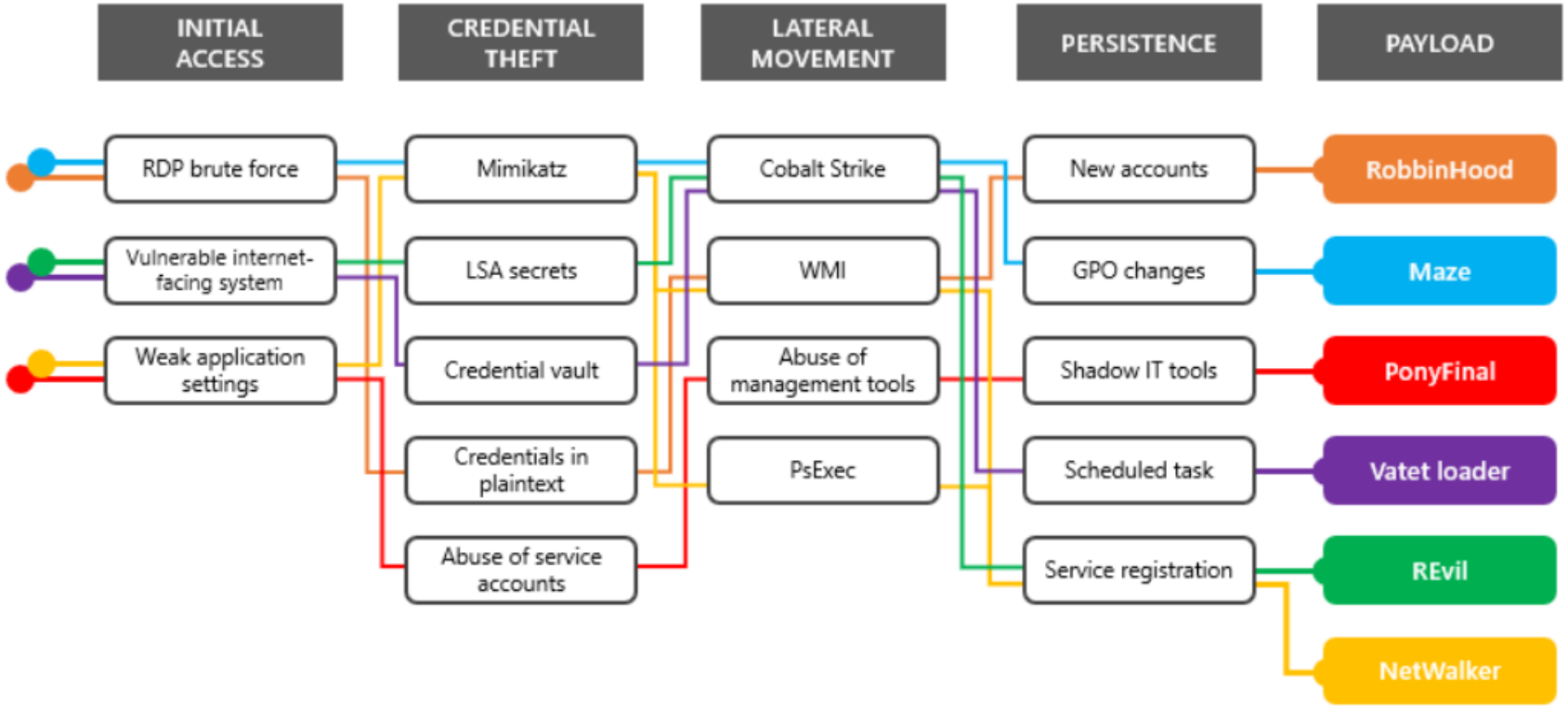
Four years after the D

AKO (REBRANDED AS RANZY)
AVADDON
CLOP
CONTI
DARKSIDE
DOPPELPAYMER
EGREGOR
LOCKBIT
MAZE
MESPINOZA (PYSA)
MOUNT LOCKER
NEFILIM
NEMTY
NETWALKER
RAGNARLOCKER
REVIL (SODINOKIBI)
SEKHMET
SNATCH
SUNCRYPT

https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/

¿Cómo? – TTPs

Los grupos de cibercriminales utilizan diferentes **T**ácticas, **T**écnicas y **P**rocedimientos para lograr su objetivo: secuestrar la información de las organizaciones.



https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

Las víctimas

Diferentes organizaciones, independientemente del sector al que pertenezcan, han sufrido afectaciones por este tipo de ataque. La afectación al sector energético, financiero y entidades de gobierno se convierten rápidamente en noticia

EL ECONOMISTA

RANSOMWARE

El rescate por el hackeo a Pemex es el segundo mayor por ransomware

El monto promedio de los rescates exigidos a través de un ataque de ransomware ha crecido 589.62% desde el tercer trimestre del 2018.

Rodrigo Riquelme
15 de noviembre de 2019, 07:13

Reporte Indigo

Portada Reporte Opinión La

ECONOMÍA

SUFRE BANCO BASE CIBERATAQUE; NO SE COMPROMETIERON DATOS LOS CLIENTES, ASEGURA

Indigo Staff

A través de un comunicado, enviado a la Bolsa Mexicana de Valores, Banco BASE informó acerca del taque cibernético del que fue víctima

Nov 12, 2020 Lectura 2 min

MILENIO 2020 AÑOS

Ante intento de ciberataque, información de clientes está a salvo, afirma CIBanco

Comparte esta noticia

La institución financiera aclaró que se trató de un intento de intrusión en sus servidores sin que los ciberdelincuentes lograran liquidar la extorsión.

Banco Estado, Chile

En septiembre se reportó un ataque a uno de los bancos más importantes de Chile: Banco Estado.

De acuerdo con la información disponible, el ataque interrumpió las operaciones de varias sucursales en diferentes regiones ocasionando problemas y dificultades s sus clientes.

El restablecimiento de operaciones en sucursal se realizó de marea gradual.

Respuesta al incidente

El Equipo de Respuesta ante incidentes de Seguridad Informática de Chile, CSIRT GOB publicó un comunicado en relación a este ataque, en el que se lee:

“El atacante analizado fue el **Ransomware Sodinokibi**, el cual es un programa distribuido con un modelo de negocio Ransomware-as-a-Service, detectado por primera vez en una campaña en el 2019.”

Respuesta al incidente (cont.)

DISC 2020

CSIRT sugiere implementar las siguientes recomendaciones a la brevedad posible:

CSIRT

Aumentar el monitoreo de tráfico no usual,
Mantener los equipos actualizados, tanto sistemas operativos como otros software instalados.
No abrir documentos de fuentes desconocidas.
Tener precaución en abrir documentos y seleccionar enlaces de correos electrónicos.
Verificar y controlar los servicios de escritorio remoto (RDP).
Bloqueo de script o servicios remotos no permitidos en la instrucción.
Monitorear servicios SMB de forma horizontal en la red
Mantener actualizados las protecciones perimetrales de las instituciones
Aumentar los niveles de protección en los equipos que cumplan las funciones de AntiSpam, WebFilter y Antivirus.
Verificar el funcionamiento, y si no es necesario, bloquear las herramientas como PsExec y Powershell.
Mantener especial atención sobre el tráfico sospechoso que tengan conexiones a los puertos 135TCP/UDP y 445TCP/UDP
Verificar periódicamente los indicadores de compromisos entregados por Csirt en los informes 2CMV20.
Segmentar las redes en base a las necesidades de sus activos, permitiendo solamente los puertos necesarios.

Gracias

DISC
2020

Ing. Demian García

@demgv

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN