I JORNADA STIC

CAPÍTULO COLOMBIA

Defensa contra el ransomware

Caso de éxito

En colaboración con:

cn-cert centro criptológico nacional

incibe_

ean universidad

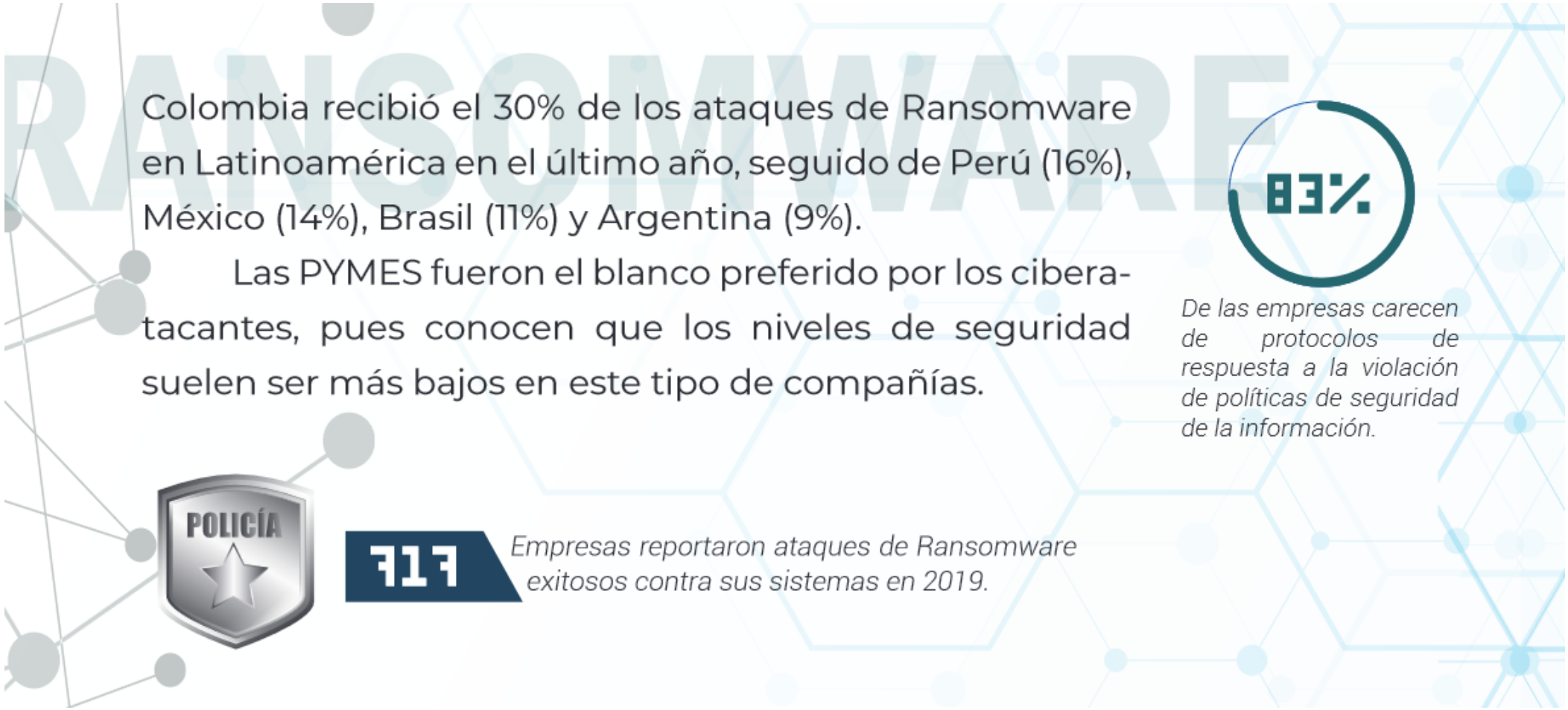
fundación in-n-va

- Antonio Sanz
- Analista senior de ciberseguridad / S2 Grupo
- asanz/@/s2grupo(.)es
  @antoniosanzalc

Ransomware = Enemigo Nº1

Evolución del ransomware

- 1º fase: cifrado de **equipos individuales**
- 2º fase: cifrado de **todos los equipos** de una organización (Human Operated Ransomware)
- 3º fase: eliminación de las **copias de seguridad**
- 4º fase: **exfiltración** de información y amenaza de venta o **publicación**



Fuente: Tendencias Cibercrimen Colombia 2019-2020

https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

1.

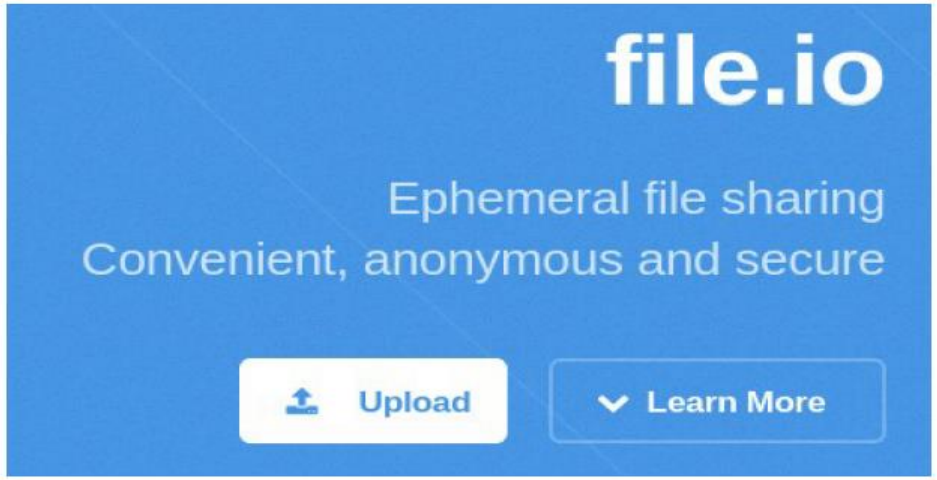
Detección

Lunes: Alertas de monitorización

- Alerta1 (Bro) analizador de **conexiones directas** a IP
  - *hxxp://194.xxx.xxx.199/a y dll.txt*
- Alerta2 (Bro) descargas HTTP sospechosas (reglas YARA de tipos de fichero **sospechosos**)
  - *IP: 194.xxx.xxx.199*
- Alerta3 (cortafuegos perimetral) - descarga de **VBS ofuscado**
  - *IP: 194.xxx.xxx.199*

Primer análisis

- Se revisan los logs de navegación del equipo
- Viernes noche: múltiples conexiones contra **file.io** (servicio efímero para compartir ficheros)



- Se declara **incidente de seguridad**

2.

Respuesta

Vector de entrada

- Se revisa en el proxy la **navegación** del usuario
- Se revisan los correos recibidos (**metadatos**)
- **Sysmon** + envío de eventos a un sistema centralizado (anterior a **CLAUDIA**)
- Se revisan los eventos → Acceso vía Citrix Cloud (**acceso remoto**) a las 00:05

Triaje y volcado de RAM

- Se ordena un **volcado de la RAM** del equipo con winpmem y un **triage** con CyLR
- Se recupera el perfil del usuario → varios de los **ficheros** vistos con Sysmon
- Comienza el **análisis forense** con los datos disponibles

Análisis de eventos

- Edición con notepad y ejecución de **a.bat**
- Ejecuciones de **Powershell**
- Ejecución de **hhupd.exe**
- Ejecución de **so.exe**
- Ejecución de un **Excel** malicioso
- Intento de descarga y registro de una DLL con **certutil.exe** + **regsvr32.exe**

Análisis forense

- **Prefetch**: confirmamos las ejecuciones ya vistas
- **MFT**: se observa la apertura de Chrome, y la descarga del fichero **WinPwn.ps1** (script de post-explotación basado en Powershell)
- Esta descarga correla con accesos a **file.io**
- Se observan varias descargas, así como de **ObfusWinPwn y Obfus_SecurePS_WinPwn**

Powershell + notepad

- a.bat = powershell.exe (técnica para lanzar una consola de Powershell en **entornos restringidos**)
- Los script son **loaders** → funcionalidades online: observamos accesos a raw.githubusercontent[.]com:443
- Accesos **denegados** por la lista de bloqueo del proxy ☺

hhupd.exe

- Binario **legítimo** de Windows
- … pero una versión antigua es vulnerable a una escalada de privilegios → CVE-2019-1388
- La Organización aplica **actualizaciones de seguridad** de forma estricta →el equipo no es vulnerable ☺

so.exe

- VirusTotal indica que puede ser una muestra de **Trickbot** (frecuente precursor de **ransomware**)
- Se detona en una **sandbox** y se comprueba que contacta contra la IP 213.xxx.xxx.213
- No se detectan contactos en el proxy (¿no es proxy-aware?) ☺
- La IP está relacionada con el ransomware **Sodinokibi**

Excel malicioso

- Se obtiene el fichero a.txt lanzado desde el Excel
- Macro maliciosa que contacta contra 194.xxx.xxx.199
- Posible beacon de **Cobalt Strike**
- Sin contactos exitosos → parado por el proxy ☺

Certutil.exe + regsvr32.exe

- Certutil.exe → Descarga de una dll
- Rundll32.exe → Registro de esa dll
- Se obtiene y detona en una sandbox → contacta contra http://194.xxx.xxx.199/pixel.gif (conocido terminador de Cobalt Strike)
- Se observa después un regsvr32.exe al mismo recurso → Ambos parados por el proxy ☺

Erradicación y recuperación

- Bloqueo de las **IP maliciosas**
- Plataformado del **equipo afectado**
- Cambio de las **credenciales** del usuario
- Revisión de **accesos** en Citrix Cloud
- Planificación de **2FA** en Citrix Cloud

3.

Lecciones aprendidas

Lecciones aprendidas

- Desplegar 2FA en todos los accesos remotos
- Obtener logs en el acceso remote
- Mejorar detección (NIDS no generó alertas)
- Desplegar microCLAUDIA
- Trabajar sobre el principio de mejora continua ☺

Guías CCN-STIC

- Guías de **configuración segura** de sistemas, servicios y aplicaciones
- Ofrece también **políticas, procedimientos y normas**
- Base ideal sobre la que basar una **estrategia de bastionado**

https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html


/claudia>

CLAUDIA + CARMEN

- Solución de vigilancia en el **endpoint**
- **Centraliza** y posibilita analizar la información
- CLAUDIA **requiere** CARMEN
- Múltiples capacidades de **respuesta ante incidentes, forense y threat hunting**

cn-cert

4.

Conclusiones

Bastiona lo mejor que puedas

Tim MalcomVetter ❤️
@malcomvetter

Reminder & reality check:

An opponent can successfully achieve objectives with trashy tactics if the window of time required to reach the objectives is shorter than defender's ability to detect & respond.

Sometimes it doesn't matter that the tactics are obviously bad.

Traducir Tweet

4:48 p. m. · 12 nov. 2020 · Twitter Web App

https://twitter.com/malcomvetter/status/1326914680783253505

- Bastionado = Ganar **TIEMPO** y obligar a hacer **RUIDO**
- Invertir en bastionado = ganancia **segura**
- Buen bastionado = No hay ransomware (recuerda, para ellos no es personal, solo es **€€€**)

Detectar y reaccionar es crítico

Victoria de todo el equipo

Agradecimientos especiales

@dgarcianet

#TrincheraTeam

Slides

http://bit.ly/NOransom

Email: asanz/@/s2grupo(.)es
Twitter: @antoniosanzalc

Canal de forense: t.me/forense

Blog: https://www.securityartwork.es

I JORNADA STIC

CAPÍTULO COLOMBIA

GRACIAS

En colaboración con:

ccn-cert centro criptológico nacional

incibe_

ean universidad

fundación in-nova