Check Point®
SOFTWARE TECHNOLOGIES LTD

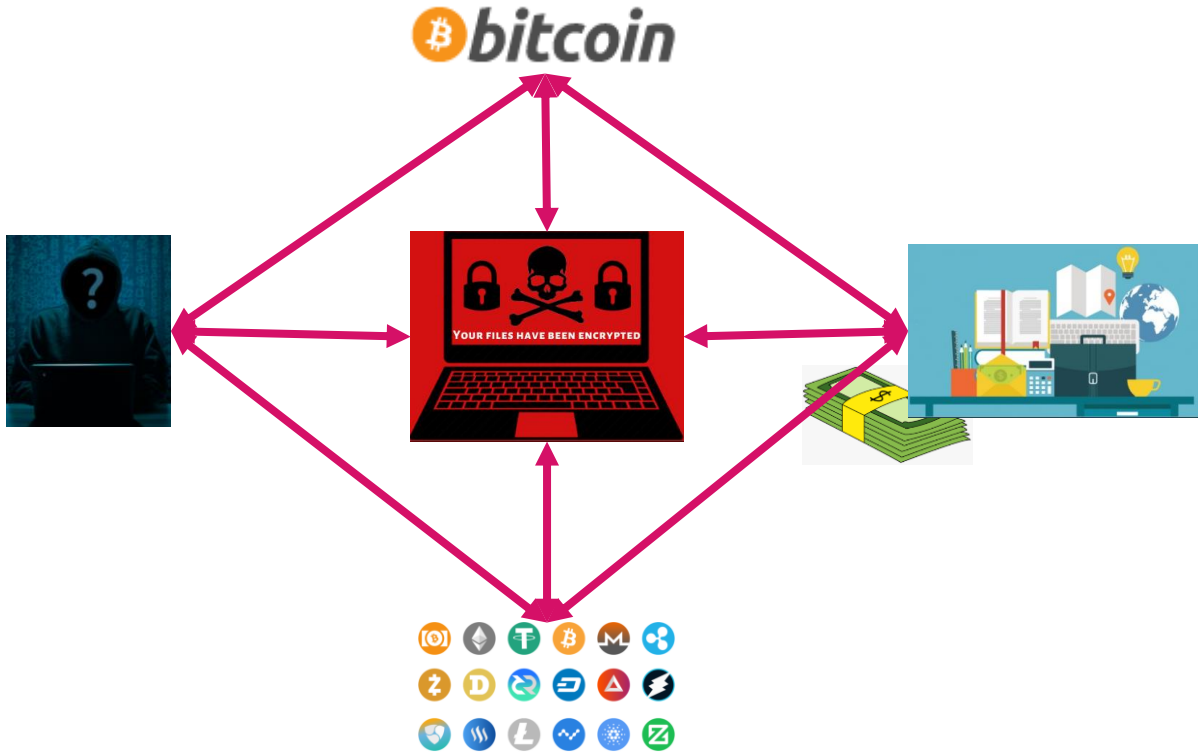
SECTOR SALUD EN PELIGRO: CÓMO PREPARARNOS FRENTE A LA AMENAZA DEL RANSOMWARE

Agenda

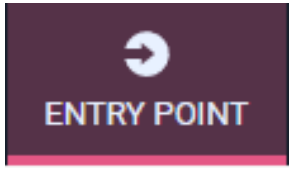
- Ransomware, ¿Qué y Cómo?
- Una alerta de ransomware excepcional
- Algunas prácticas comunes
- Los números
- Top ransomware en América Latina
- El riesgo
- Recomendaciones

Ransomware, ¿Qué y Cómo?

- El ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.



Ransomware, ¿Qué y Cómo?



- Adjuntos por email
- Navegación web
- Link en email
- Descargado por otro malware
- Propagación por red

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Logon 1 event	Command-Line Interface 4 events	Registry Run Keys / Startup Folder 1 event	Process Injection 22 events	Modify Registry 683 events		Browser Bookmark Discovery 10 events		Data from Local System 1929 events	Commonly Used Port 13 events		Data Encrypted for Impact 35 events
Valid Accounts 1 event	Execution through API 663 events	Valid Accounts 1 event	Valid Accounts 1 event	Process Injection 22 events				Data from Network Shared Drive 1 event			Inhibit System Recovery 2 events
	Scripting 4 events			Scripting 4 events				Man in the Browser 6 events			Process Termination 44 events
	Unsigned Process 2 events			Valid Accounts 1 event							Service Stop 368 events
	User Execution 1 event										

Ransomware, ¿Qué y Cómo?

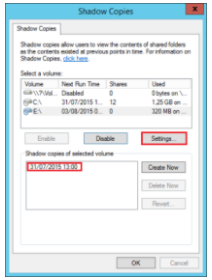
ACTIVITY

Ejecución de archivos

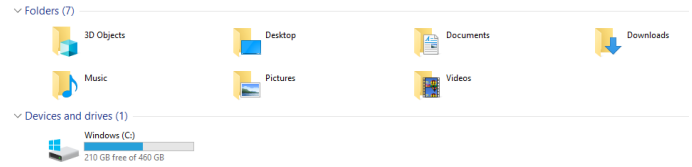
Shellcode

Nuevos procesos

Comunicaciones (updates, descarga de llaves, C&C)



Shadow copy



Escaneo de directorios

Cifrado

Instrucciones de pago

Descarga de nuevos módulos

Una alerta de ransomware excepcional

JOINT CYBERSECURITY ADVISORY

Ransomware Activity Targeting the Healthcare and Public Health Sector

AA20-302A

October 28, 2020

Updated October 29, 2020

- Conti
- TrickBot
- BazarLoader
- Ryuk

Alert (AA20-302A)

Ransomware Activity Targeting the Healthcare and Public Health Sector

Original release date: October 28, 2020 | Last revised: November 02, 2020

Print | Tweet | Send | Share

Summary

This advisory was updated to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection.

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). This advisory describes the tactics, techniques, and procedures (TTPs) used by cybercriminals against targets in the Healthcare and Public Health (HPH) Sector to infect systems with ransomware, notably Ryuk and Conti, for financial gain.

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 7 framework. See the ATT&CK for Enterprise version 7 for all referenced threat actor tactics and techniques.

CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

Click here for a PDF version of this report.

Key Findings

- CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services.
- These issues will be particularly challenging for organizations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.

Technical Details

Threat Details

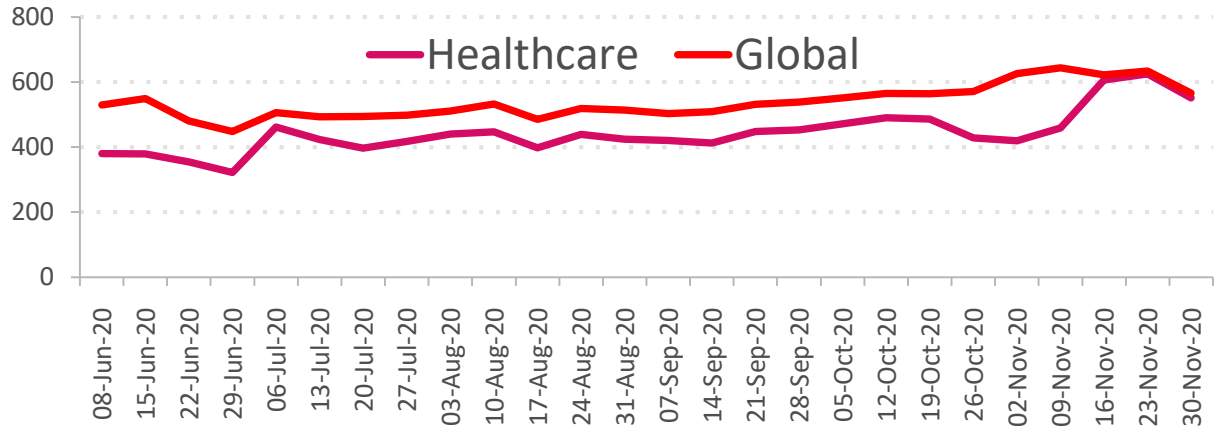
The cybercriminal enterprise behind TrickBot, which is likely also the creator of BazarLoader malware, has continued to develop new functionality and tools, increasing the ease, speed, and profitability of victimization. These threat actors increasingly use loaders—like TrickBot and BazarLoader (or BazarBackdoor)—as part of their malicious cyber campaigns. Cybercriminals disseminate TrickBot and BazarLoader via phishing campaigns that contain either links to malicious websites that host the malware or attachments with the malware. Loaders start the infection chain by distributing the payload; they deploy and execute the backdoor from the command and control (C2) server and install it on the victim's machine.

- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Bureau of Investigation (FBI)
- Department of Health and Human Services (HHS).

Algunas prácticas comunes

- SO operativos Windows XP, Windows 7 aún en uso
- RDP habilitado
- Uso de navegador IE (muy vulnerable)
- Navegación web restringida por URL
- Área de TI no es 24x7
- Sin restricciones a dispositivos USB externos
- Protección básica en los equipos de cómputo
- No hay planes de respuesta a incidentes cibernéticos
- Proceso de respaldo de la información incompleto o con fallas

Los números



774 Ataques promedio por empresa/semana

VS

537 Ataques promedio por empresa/semana a nivel mundial

60%

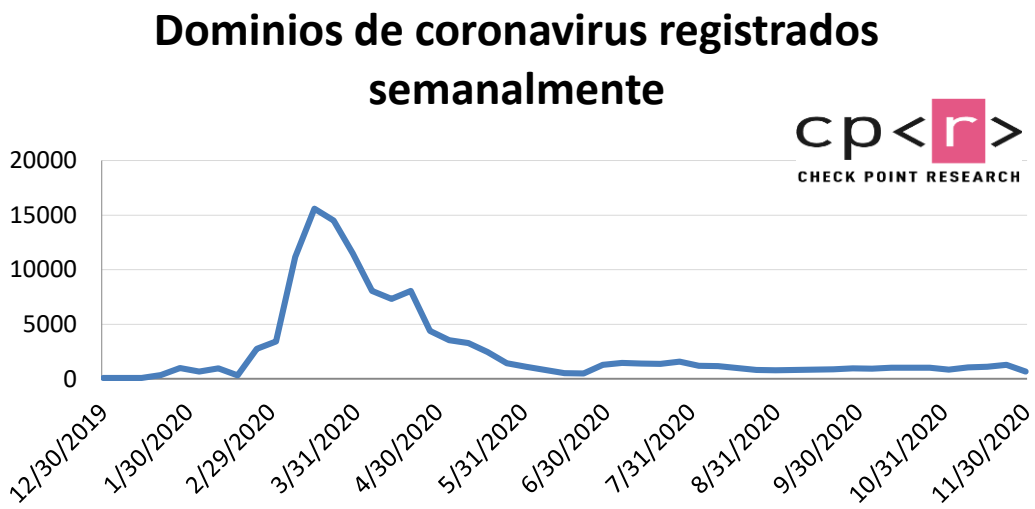
De los archivos maliciosos se entregaron por correo electrónico

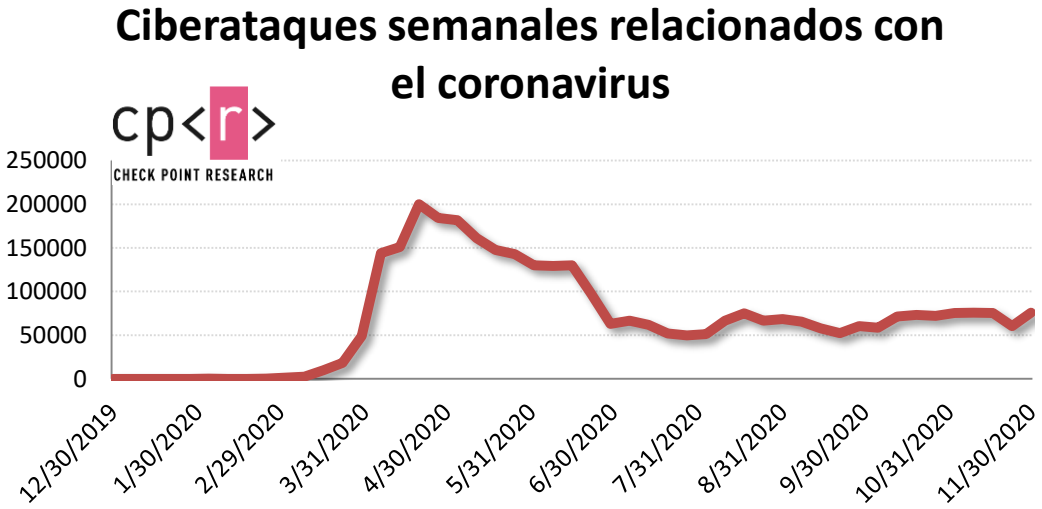
90 Días

1/35

En los últimos 90 días, 1 de cada 35 organizaciones de atención médica se vio afectada un ataque de ransomware.

Los números





Los ataques se están produciendo en muchas plataformas e incluyen:

- Aplicaciones maliciosas relacionadas con coronavirus
- Sitios web relacionados con coronavirus
- Correos electrónicos dirigidos que utilizan la pandemia de coronavirus en sus nombres de archivo / asunto de correo electrónico

Los números

Países más atacados en la región

#1 Ecuador

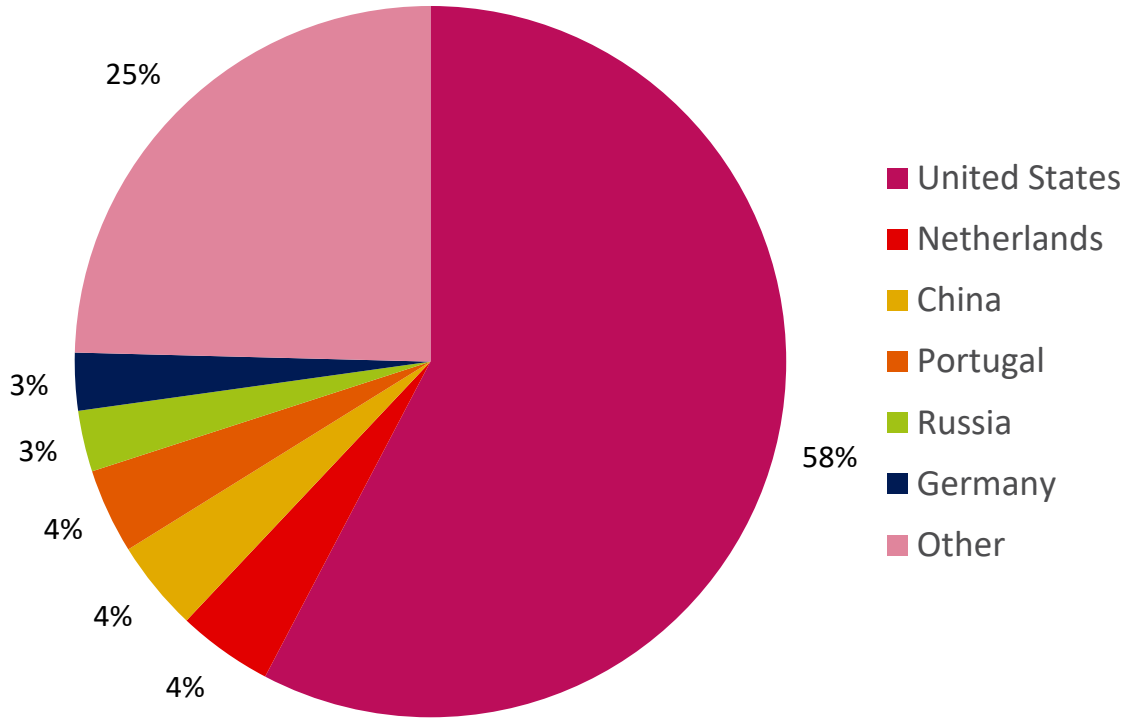
#2 Colombia

#3 Jamaica

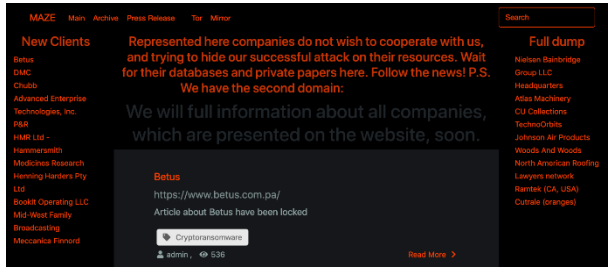
#4 México

#5 Bolivia

Principales países de origen de amenazas



Top ransomware en América Latina

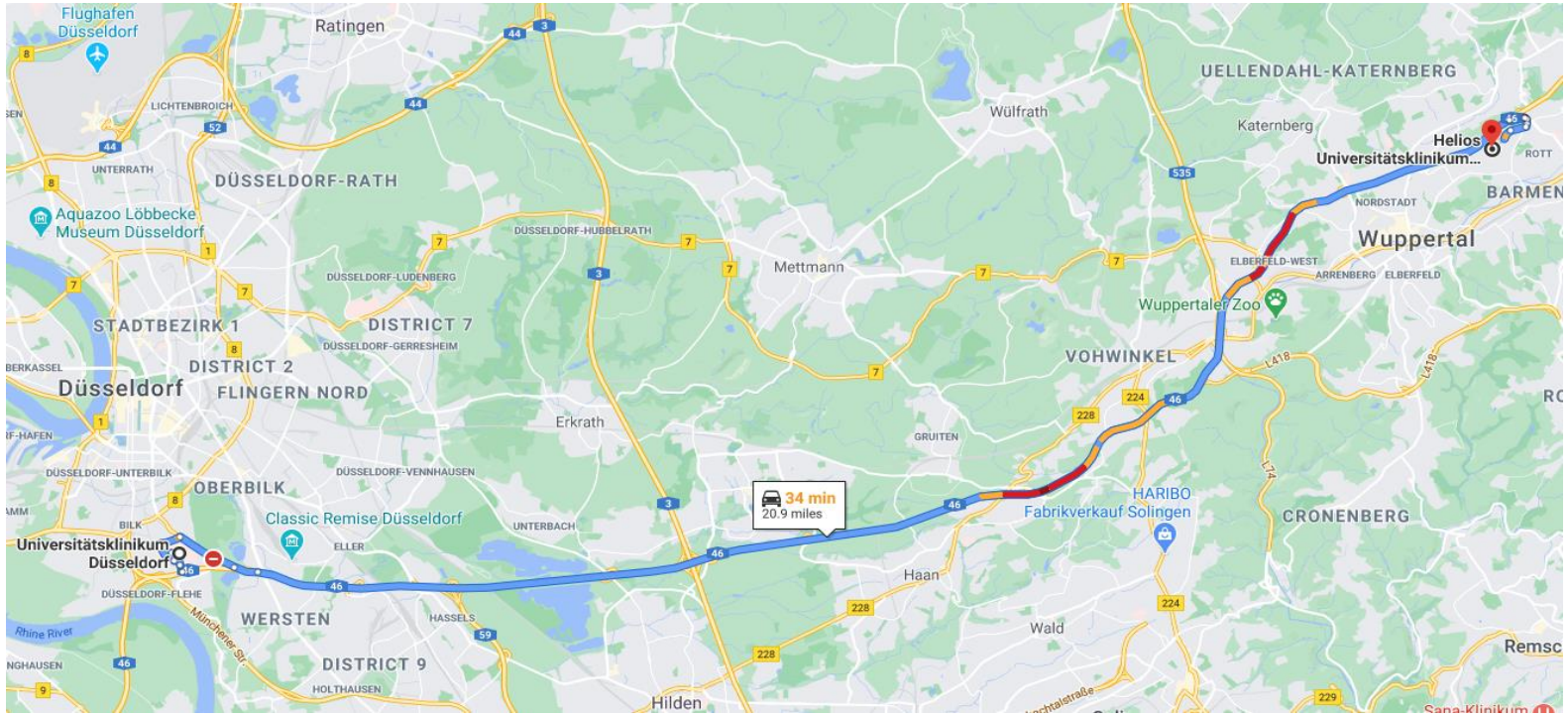


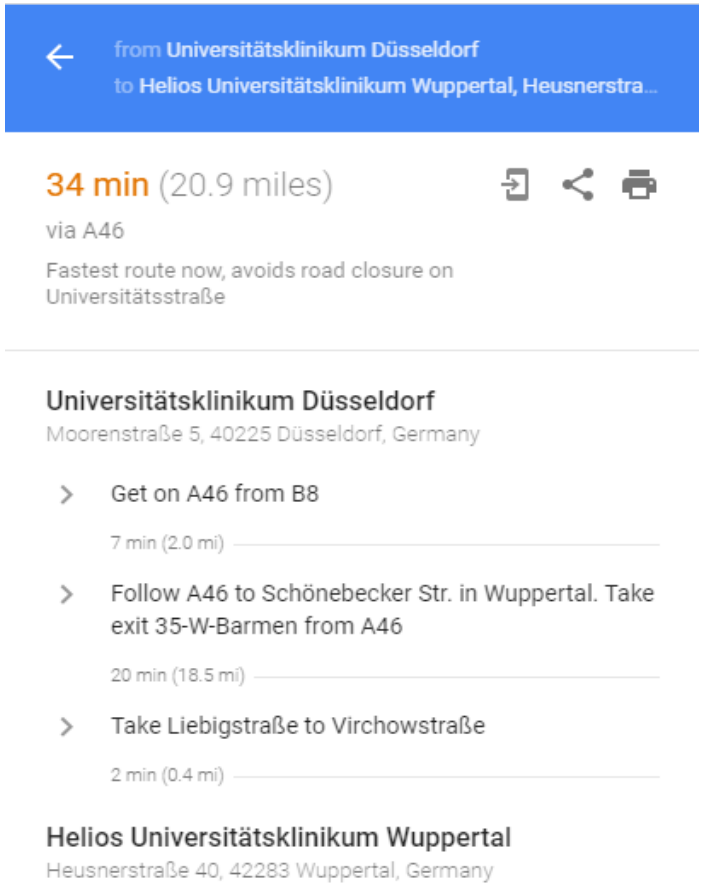
Maze

Ryuk

Sodinokibi

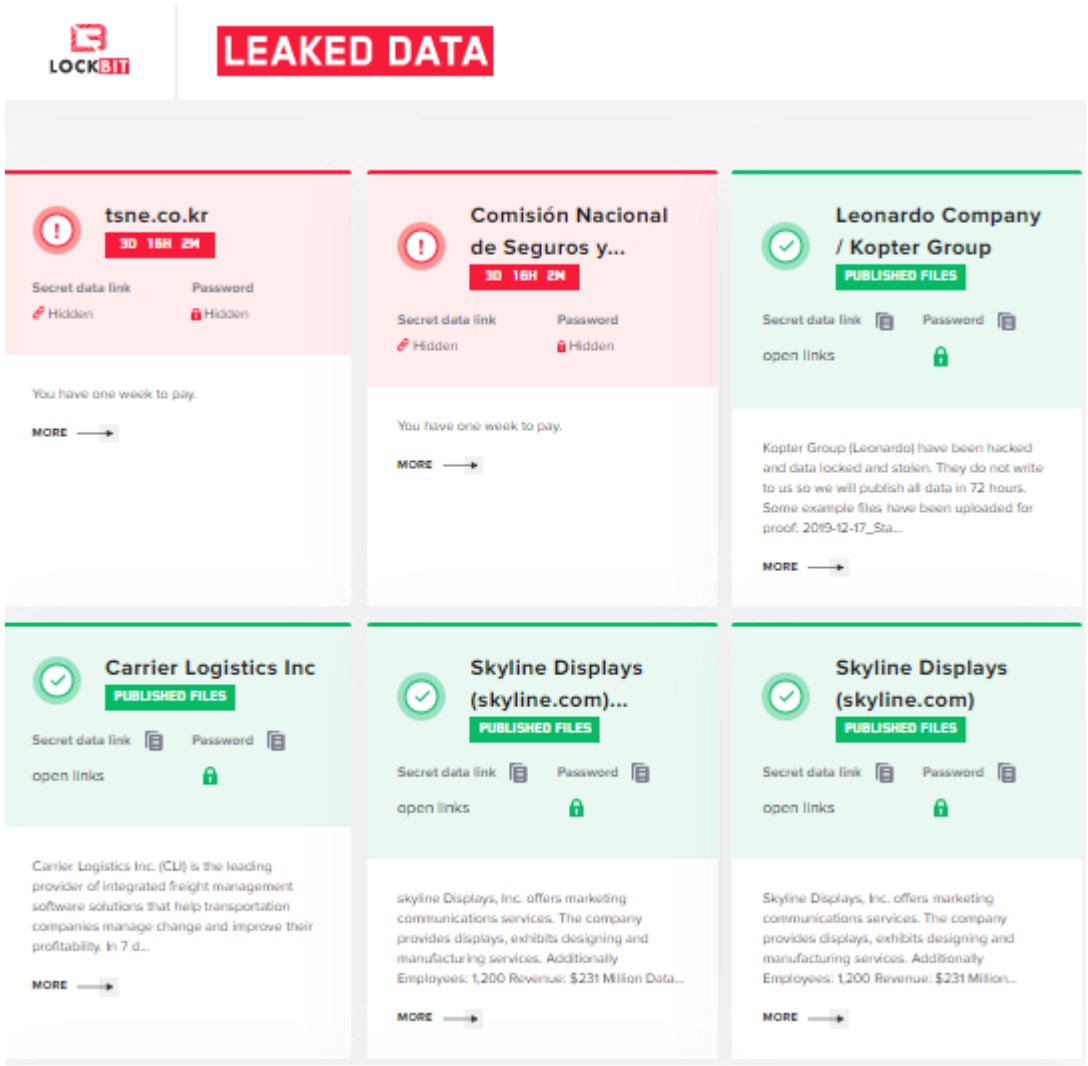
El riesgo





Muere una mujer durante un ataque de 'ransomware'
a un hospital de Dusseldorf (Alemania)

El riesgo



Recomendaciones

- Únase e interactúe con organizaciones de ciberseguridad.
- Es fundamental mantener copias de seguridad de datos cifradas, fuera de línea y probadas periódicamente.
- Cree, mantenga y ponga en práctica un plan básico de respuesta a incidentes.
- Desarrollar un plan de gestión de riesgos que mapee los servicios de salud críticos y la atención a los sistemas de información necesarios, identifique y mapee los vectores de infección.
- Realizar el correspondiente proceso de “Hardening” a los dispositivos:
  - https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
  - https://www.cisecurity.org/cis-benchmarks/
  - https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

THANK YOU