Ransomware: An Interdisciplinary Analysis

M. Robles-Carrillo & P. García-Teodoro
Network Engineering & Security Group (NESG)
Universidad de Granada

I. INTRODUCCIÓN

Home › Cybercrime

Ransomware Attack a Nail in the Coffin as Lincoln College Closes After 157 Years

By Kevin Townsend on May 11, 2022

Share Tweet RSS

Ransomware Attack and Covid-19 Blamed for Closure of Abraham Lincoln's Namesake College After 157 Years

Lincoln College in Illinois, will close its doors on Friday, May 13, 2022. It had survived for 157 years through major world events, depressions and the 1918 flu pandemic – but has finally succumbed to the two great twenty-first century pandemics: Covid-19 and ransomware.

"Lincoln College has survived many difficult and challenging times – the economic crisis of 1887, a major campus fire in 1912, the Spanish flu of 1918, the Great Depression, World War II, the 2008 global financial crisis, and more, but this is different," announced the college at the beginning of this semester. "Lincoln College needs help to survive."

That help has not been forthcoming, and the college has notified the education authorities that it will cease all academic programming at the end of this week.

There is a tragedy here. The college was aware that it needed to improve its new enrollments, and it put measures in place to do so. It experienced record-breaking student enrollment in the Fall of 2019. It seemed the corner had been turned – but within months, the Covid-19 pandemic struck.

Covid had a major negative effect on the college. "The economic burdens initiated by the pandemic required large investments in technology and campus safety measures," says the college. At the same time, enrollments fell again with new students choosing to postpone college.

I. INTRODUCCIÓN

3 minute read · June 4, 2021 1:50 AM GMT+2 · Last Updated a year ago

Exclusive: U.S. to give ransomware hacks similar priority as terrorism

By Christopher Bing

WASHINGTON, June 3 (Reuters) - The U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority as terrorism in the wake of the Colonial Pipeline hack and mounting damage caused by cyber criminals, a senior department official told Reuters.

I. INTRODUCCIÓN

Costa Rica declares national emergency after Conti ransomware attacks

By **Ax Sharma** May 9, 2022 03:53 AM 0

The Costa Rican President Rodrigo Chaves has declared a national emergency following cyber attacks

I. INTRODUCCIÓN

LOHRMANN ON CYBERSECURITY

NATO Adds Cyber Commitments, Potential Ransomware Response

The North Atlantic Treaty Organization (NATO) opened the door for cyber attacks to trigger “Article 5” actions. This is a big deal — here’s why.

June 20, 2021 • Dan Lohrmann

Dan Lohrmann

I. INTRODUCCIÓN

Newsroom Business Employees Job Seekers Students Travelers Visas

U.S. DEPARTMENT of STATE

POLICY ISSUES COUNTRIES & AREAS BUREAUS & OFFICES ABOUT

Home > Office of the Spokesperson > Press Releases > Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice

★ ★ ★

Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice

PRESS STATEMENT

NED PRICE, DEPARTMENT SPOKESPERSON

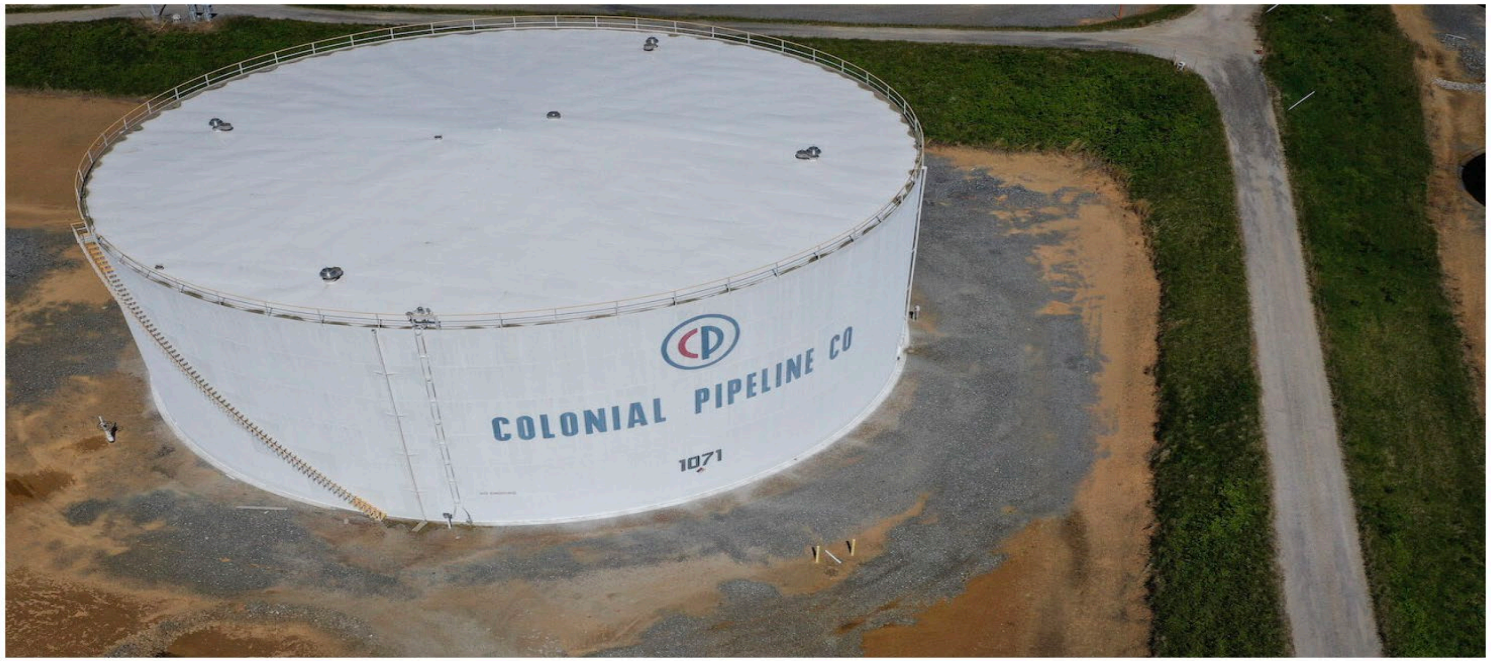
MAY 6, 2022

The Department of State is offering a reward of up to $10,000,000 for information leading to the identification and/or location of any individual(s) who hold a key leadership position in the Conti ransomware variant transnational organized crime group. In addition, the Department is also offering a reward of up to $5,000,000 for information leading to the arrest and/or conviction of any individual in any country conspiring to participate in or attempting to participate in a Conti variant ransomware incident.

I. INTRODUCCIÓN

US proposes $1 million fine for Colonial Pipeline ransomware attack

Derek B. Johnson 9 de mayo de 2022



Fuel holding tanks are seen at Colonial Pipeline's Dorsey Junction Station on May 13, 2021 in Woodbine, Md. A proposed $1 million fine blames Colonial Pipeline executives for failing to correct a number of known safety violations. (Photo by Drew Angerer/Getty Images)

I. INTRODUCCIÓN

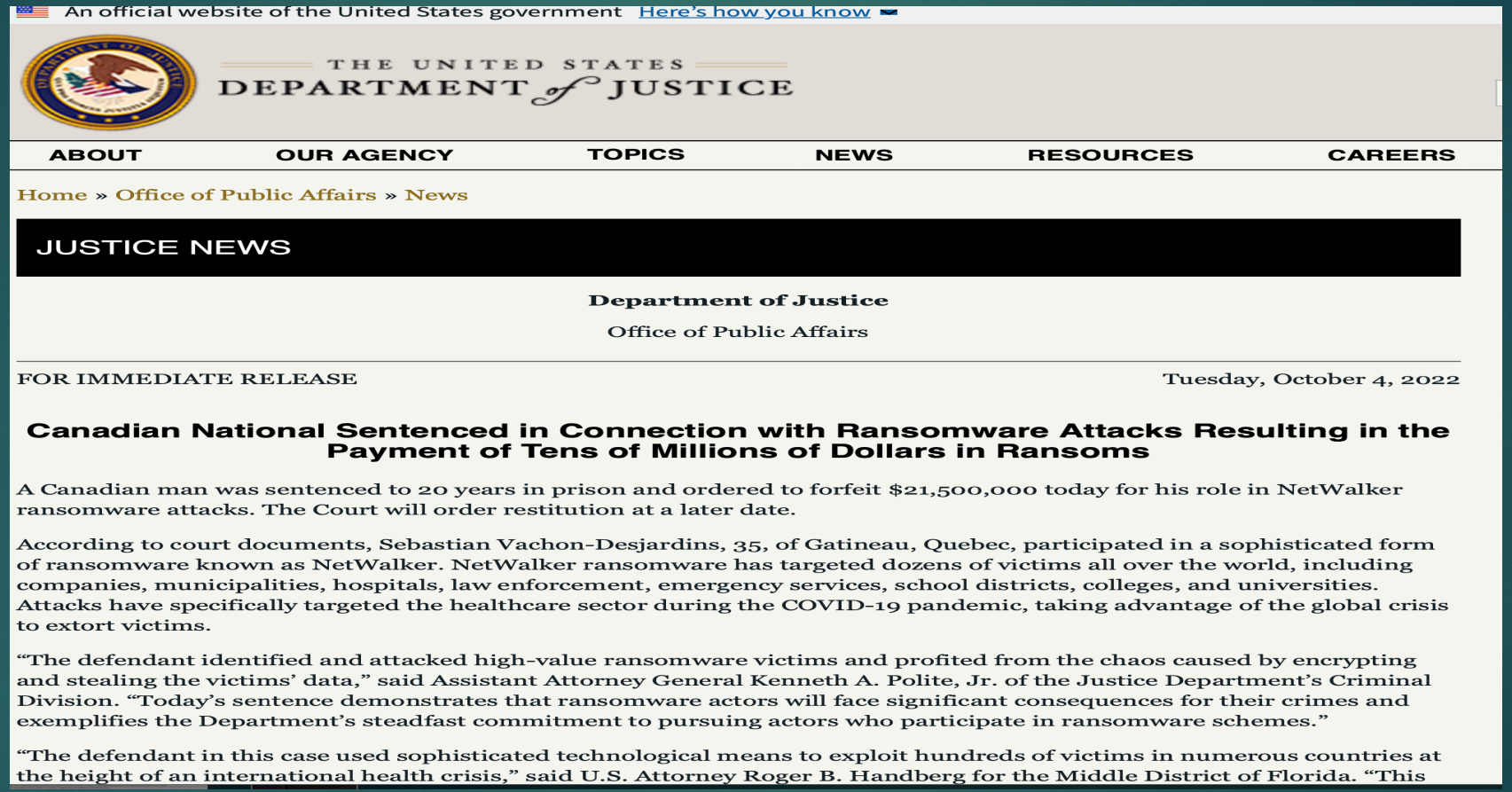
AXA n'indemnisera plus les ransomwares

En France, AXA risque de perdre son statut de meilleur assureur dans le domaine des cyberattaques en 2021. Une annonce qui survient à un moment où le nombre de ransomwares n'a jamais été aussi élevé.

Par Valentin Cimino - @ciminix
Publié le 12 mai 2021 à 07h49

Comme les hackers sont capables de cibler leur victime en fonction de leur couverture assurantielle, AXA préfère mettre fin à l'indemnisation des rançonlogiciels. Image : Shutterstock

I. INTRODUCCIÓN



An official website of the United States government Here's how you know

THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT | OUR AGENCY | TOPICS | NEWS | RESOURCES | CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Tuesday, October 4, 2022

Canadian National Sentenced in Connection with Ransomware Attacks Resulting in the Payment of Tens of Millions of Dollars in Ransoms

A Canadian man was sentenced to 20 years in prison and ordered to forfeit $21,500,000 today for his role in NetWalker ransomware attacks. The Court will order restitution at a later date.

According to court documents, Sebastian Vachon-Desjardins, 35, of Gatineau, Quebec, participated in a sophisticated form of ransomware known as NetWalker. NetWalker ransomware has targeted dozens of victims all over the world, including companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities. Attacks have specifically targeted the healthcare sector during the COVID-19 pandemic, taking advantage of the global crisis to extort victims.

"The defendant identified and attacked high-value ransomware victims and profited from the chaos caused by encrypting and stealing the victims' data," said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department's Criminal Division. "Today's sentence demonstrates that ransomware actors will face significant consequences for their crimes and exemplifies the Department's steadfast commitment to pursuing actors who participate in ransomware schemes."

"The defendant in this case used sophisticated technological means to exploit hundreds of victims in numerous countries at the height of an international health crisis," said U.S. Attorney Roger B. Handberg for the Middle District of Florida. "This

I. INTRODUCCIÓN

Ciberataque de ransomware afecta a hospitales y ambulatorios de Cataluña

viernes, 7 de octubre de 2022 | Publicado por el-brujo

El Consorci Sanitari Integral (CSI) ha sufrido **un ataque informático de ransomware (por segunda vez en dos años)** que afecta a todos sus centros asistenciales en Barcelona y el Baix Llobregat. La **actividad sanitaria y la atención de pacientes se mantienen en lo que no requiere servicios informáticos**, con las consultas prácticamente solo para urgencias, pues los sanitarios **no tienen acceso a la información de los pacientes ni a trámites a través de los ordenadores. El grupo de ransomware responsable es RansomExx.**

Consorci Sanitari Integral

- El CSI es una entidad pública que presta sus servicios en el ámbito de Barcelona, l'Hospitalet y el Baix Llobregat.
- El ciberataque afecta desde esta madrugada al funcionamiento de los hospitales, CAP y el resto de centros que pertenecen al Consorci Sanitari Integral.
- El impacto económico de este tipo de cibercrimen es superior al del narcotráfico

Según confirmó el conseller de Salut, Josep Maria Argimon, el ataque sería "grave", se trata de un ataque "ransomware" -- un secuestro de información por el que se pide un rescate económico-- y afecta al funcionamiento de la red de asistencia de varios hospitales y otros centros sanitarios catalanes, sobre todo de la Región Metropolitana Sur.

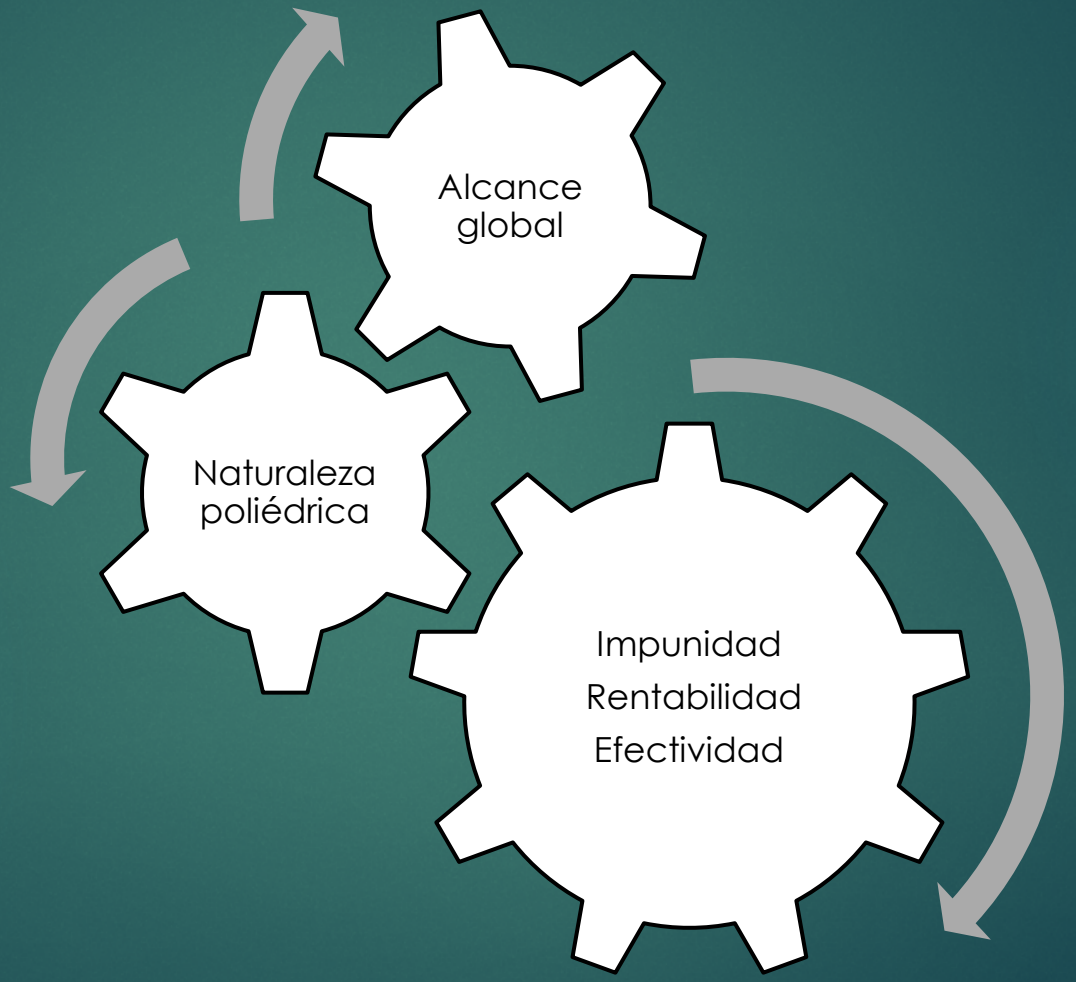
AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

I. INTRODUCCIÓN

La banda Ransomexx reivindica el ciberataque contra hospitales catalanes y filtra datos de pacientes

La organización criminal difunde un paquete de 54 gigas entre los cuales se hallan informes médicos y documentación personal

II. EL PROBLEMA DEL RANSOMWARE



III. EL DILEMA DEL RANSOMWARE

- El estado del arte
- El problema jurídico
- Carencias y disfunciones
- Aspectos técnicos y jurídicos
- Metodología interdisciplinar

IV. DIRECTRICES DE RESPUESTA

IV. CONCLUSIONES

- Problema global, de naturaleza poliédrica y cuestión de seguridad
- Efectividad + Impunidad
- Respuesta interdisciplinar:
  - Tipificación como delito autónomo por su naturaleza técnica
  - Penalización de la incitación, la complicidad y la tentativa
  - Prohibición del seguro y del pago del ransomware
  - Aumento y fortalecimiento de la cooperación internacional