

NC3

NATIONAL **CYBERCRIME**  
COORDINATION CENTRE

CNC3

CENTRE NATIONAL DE COORDINATION  
CONTRE LA **CYBERCRIMINALITÉ**

# Policing Cybercrime???



# Facing a Highly Motivated, Unscrupulous and Adaptive Human Adversary

**Malware scam circulates after Saskatchewan stabbings**

**Medibank: Hackers release abortion data after stealing Australian medical records**

**Ransomware attack delays patient care at hospitals across the U.S**

**More than half the ransomware attacks in Canada target critical infrastructure**

**N.L. health-care cyberattack is worst in Canadian history, says cybersecurity expert**

(**SECURITY**)

**Cyber-mercenaries for hire represent shifting criminal business model**

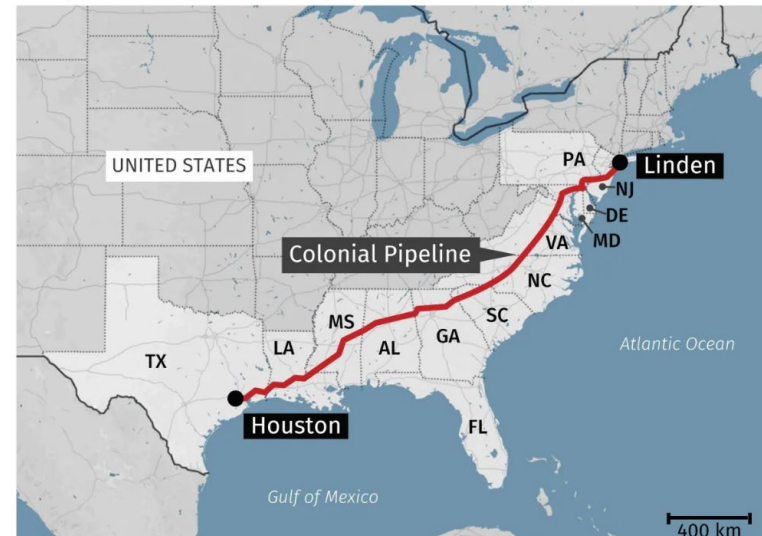
Emerging threat group offers a broad range of attack services

Jeff Burt

Mon 25 Jul 2022 // 17:00 UTC

**B.C. health authority hit with ransomware attack**

**Major U.S. gasoline pipeline hit by cyberattack**





NATIONAL **CYBERCRIME** | CENTRE NATIONAL de coordination  
Coordination Centre | en **CYBERCRIMINALITÉ**







⚠ For immediate assistance - Contact your local police

ⓘ Disclaimer: Please note that this website is for usability research purposes only and should not be considered a production site. The reports generated will not be submitted to the RCMP. By using this website, you acknowledge and accept that this site is for user research to obtain feedback to improve the usability of the application.

## Report Cybercrime and Fraud

Report a scam, fraud or cybercrime online, whether you are the victim or intended target.

Report Online

Update a report

### National Cybercrime and Fraud Reporting System

Reporting a scam or computer crime helps the [Royal Canadian Mounted Police \(RCMP\)](#), the [National Cybercrime Coordination Centre \(NC3\)](#) and the [Canadian Anti-Fraud Centre \(CAFC\)](#) learn more about the nature of these incidents. You can report anonymously if you wish to share helpful information without being identified. We use this information to help protect more people from harm.

### Report by phone

**Toll-free:**  
[1-888-495-8501](tel:1-888-495-8501)

**Hours of service:**  
Monday to Friday 9 am to 4:45 pm (EST) excluding holidays



## Getting started


You may complete this report anonymously and download its copy once submitted.

ⓘ Important! Do not add sensitive information such as your social insurance, bank account or driver's license number when submitting this report.

Gather all the information you can about the incident, such as:


- Details about what happened and how you were affected
- Documents, messages, transaction receipts and/or emails ⓘ
- Details that could reveal suspect identity (e.g. contact information, IP address, username/email)

### \* I'm reporting for:




**Myself**

I was the target of a scam or cybercrime



**Someone I know**

Someone I know was the target of a scam or cybercrime



**A business or organization**

My business or organization, or the business or organization I work for, was the target of a scam or cybercrime

# NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE







# THIS WEBSITE HAS BEEN SEIZED

## OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

To determine if you have been victimized, visit: [haveibeenpwned.com](https://haveibeenpwned.com)

Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we're interested: [FBIMW-Genesis@fbi.gov](mailto:FBIMW-Genesis@fbi.gov)

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
225	+150	+1461	+5826	466106
Grouped by				
ES	+29	+166	+720	36791
PL	+12	+171	+638	32192
TR	+13	+107	+488	25787
RO	+6	+126	+443	33218
US	+11	+95	+378	6604
IT	+1	+78	+359	57651
CL	+22	+87	+343	9544

# THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,  
as part of a coordinated law enforcement action taken against Hive Ransomware.

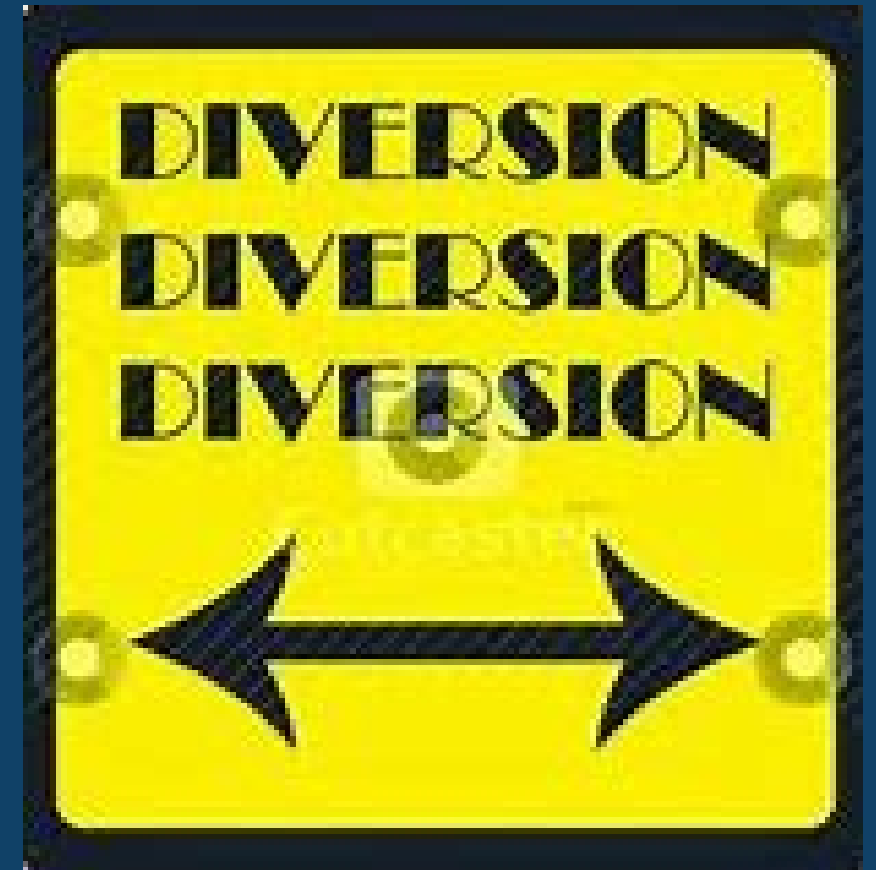
NC3 | NATIONAL CYBERCRIME  
COORDINATION CENTRE



The action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice, with substantial assistance from Europol and Reutlingen Police Headquarters - CID Esslingen.

**RCMP** @rcmpgrcpolice · Jan 26  
Replying to @rcmpgrcpolice @Europol and 2 others  
Working with partners, the NC3 notified a number of HIVE victims in Canada and, where feasible, helped facilitate access to decryption keys so that the impacts of the group's ransomware attacks were reduced or negated.

# Law Enforcement Activities – A Balance...







# Help for Victims

NC3

NATIONAL **CYBERCRIME**  
COORDINATION CENTRE

CNC3

CENTRE NATIONAL DE COORDINATION  
CONTRE LA **CYBERCRIMINALITÉ**