Policing Cybercrime???
Facing a Highly Motivated, Unscrupulous and Adaptive Human Adversary

Malware scam circulates after Saskatchewan stabbings

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

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

Cyber-mercenaries for hire represent shifting criminal business model

Emerging threat group offers a broad range of attack services

B.C. health authority hit with ransomware attack

Medibank: Hackers release abortion data after stealing Australian medical records

More than half the ransomware attacks in Canada target critical infrastructure

Major U.S. gasoline pipeline hit by cyberattack
NATIONAL CYBERCRIME Coordination Centre | CENTRE NATIONAL de coordination en CYBERCRIMINALITÉ
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

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
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

Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we’re interested: FBIMW-Genesis@fbi.gov
THIS HIDDEN SITE HAS BEEN SEIZED

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

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 @rcmpgrc policing Jan 26
Replying to @rcmpgrc policing @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...
LEFT OF

BOOM

Cyber crime