

# The Duties Beyond Assisting the Public: Darknet Threats Against Canadian Health & Support Organizations

---

[ke-la.com/duties-beyond-assisting-the-public/](https://ke-la.com/duties-beyond-assisting-the-public/)

May 10, 2020



As if a global pandemic crisis isn't enough, organizations focused on the health and support of citizens have been forced to combat not only a widespread virus (and the public needs that come with it), but also threats coming at them from the underground world. As the pandemic continues to affect all types of both private- and government-affiliated organizations worldwide, KELA's Cyber Intelligence Center took a look into various assets pertaining to Canadian health and support organizations to assess how their attack surfaces may be affected. This blog post will highlight just a couple of darknet findings that our team has detected, which exemplify how threat actors are targeting these types of organizations in Canada.

## Exploring New Victims

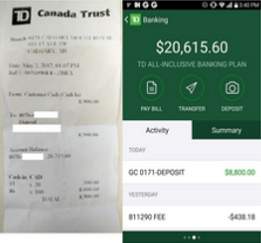
---

As COVID-19-related scams continue to rise, actors behind cheque fraud have now expanded their portfolio, targeting a new group of victims — Canadian relief programs. Take the Canadian Emergency Response Benefit (CERB) for example. Our analysts at KELA

discovered various offerings for cheques claimed to resemble those of CERB, inviting fraudsters to profit by receiving potential funding. It works very simply. Threat actors make these cheques ready to use by offering buyers either scans or prints of lookalike government cheques, which they then can deposit into their “drop” accounts, preferably via mobile deposit.

Here’s a peak into some of the CERB offerings that were available last week on a credible and well-known Canadian-focused underground market:

**{{NEW}}★★★★★ MOBILE CHEQUE DEPOSIT DIRECTLY INTO BANK ACCOUNT ★★★★★**



Sold by: [REDACTED]

Trust rating: Medium

Feedback score: 100

Contact [REDACTED]

View [REDACTED] profile

Buy now

500 CAD

356 USD

You are protected by **ESCROW**

Product DescriptionRefund PolicySeller's Feedback

**★★★★★ BEST CHEQUES IN THE GAME ★★★★★**

**\$\$\$ LOADING ALL BANK ACCOUNTS WITH DEPOSITS \$\$\$**

- > I CAN LOAD (ANY) BANK ACCOUNTS WITH ANY AMOUNT YOU REQUEST
- > CANADIAN CERB GOVERNMENT CHEQUES ALSO AVAILABLE
- > ALL CHEQUES ARE 100% VALID AND GUARANTEED TO CLEAR
- > NUMBERS ON CHEQUE ARE ALL REAL AND WILL 100% CLEAR SENDERS ACCOUNT
- > YOU KEEP ALL PROFIT ( I do not ask for a 50/50 or 60/40 split ).

PLEASE HAVE BANKING INFO READY FOR DEPOSITS

[NEW] CERB CHEQUE SCANS TO TOP YOUR DROPS !

[NEW] CERB CHEQUE SCANS TO TOP YOUR DROPS !



2020

Sold by: [REDACTED]


Trust rating: High


Feedback score:98

Contact [REDACTED]

View [REDACTED] profile

Buy now

75 CAD 

53 USD 

You are protected by ESCROW 

Product Description

Refund Policy

Seller's Feedback

YOU WILL HAVE TO PROVIDE ME:

-NAME OF THE DROP

I WILL PROVIDE YOU:

-SCAN OF THE FRONT CHEQUE

-SCAN OF THE BACK CHEQUE

INSTRUCTIONS TO DEPOSIT:

-PRINT THE CHEQUE WITH ANY PRINTER (WITH COLORS)

-CUT THE CHEQUE, THE SIZE IS ALREADY GOOD

-DEPOSIT THE CHEQUE THROUGH YOUR MOBILE BANKING APP

THE CHEQUES ARE A1 !

ALL THE SCANS ARE 2,000\$, THE CLEARING RATE IS 100% NOW

TOP YOUR DROP YOURSELF WITH NO MIDDLEMAN !

CERB/PCU GOVERNMENT CHEQUE (2K\$)



Sold by: [REDACTED]


Trust rating: High


Feedback score:97


Contact [REDACTED]

View [REDACTED] profile

Buy now

60 CAD 

43 USD 

You are protected by ESCROW 

Product Description

Refund Policy

Seller's Feedback

Thanks to the government here's a new cheque once more. Load your drops away. Clients that cashed out 10K this week alone using this. Only buy if you know how to use. You get front and back edit cheque number and drop using mobile deposit or print if you got what you need to do so. Good quality scan.

## Exploring New Markets

Familiar and “everyday” threats are targeting very sensitive organizations during this crisis, but there are some rather “new” threat types booming as well. In addition to the botnet markets, hacking forums, instant messaging platforms, and other underground sites that KELA automatically monitors, KELA’s technologies now gather intelligence from automated shops that sell access to compromised servers.

We dived into a market of this type and detected webshell access to a subdomain of the one of the largest hospitals in Toronto (among other health-related organizations) for sale. The fortunate threat actor that purchases this can instantly be granted access to remotely control the hospital’s server at any time, which in turn enables them to perform a variety of different actions depending on the breached server purchased. To state an example, let’s take something very common that’s been hitting many headlines recently – ransomware attacks. Being granted access to controlling one’s servers from a distance can, among other things, lead to a ransomware attack, therefore placing organizations in a high-risk situation amid all other COVID-19 issues they are faced with. Organizations – especially those related to the healthcare sector – cannot afford even the smallest potential cyber attack as they deal with larger, more critical issues.

The screenshot displays a web interface for managing web shell access. At the top, a red header bar contains the text "ca - Web Shell Access". Below this, the interface is divided into several sections:

- HOST INFORMATION:** A table listing details for the host:

Hostname	[Redacted]
Website Title	Pregnancy & Infant Loss [Redacted]
Technology	PHP
CMS	Wordpress
- COMPROMISE DETAILS - SHELL #89178:** A table listing details for the specific shell:

Access Type	Web Shell Access
File Permissions	Full file editing permissions
- COMPROMISE METADATA:** A table listing metadata for the shell:

Seller	[Redacted]
Price	300
Tool	N/A

**Web Shell Access**

**HOST INFORMATION**

- Hostname: [REDACTED]
- Website Title: Home
- Technology: PHP
- CMS: Wordpress

**COMPROMISE DETAILS · SHELL #145255**

- Access Type:** Web Shell Access
- File Permissions:** Full file editing permissions, Edit server root directory, Server index file can't be edited
- Database Permissions:** Size of SQL user table: 3.1k
- Server Information:** Operating system: [REDACTED], Website PHP version: 7.2.25

**COMPROMISE METADATA**

- Seller:** [REDACTED]
- Price:** 84.15
- First checked:** Apr 30th, 2020
- Tool:** [REDACTED]

These are two examples of webshell access for sale pertaining to two different health-related organizations in Canada. These listings were posted in a remote access marketplace. KELA's DARKBEAST indexes data from this market, among others, and allows users to search through them in real-time.

## What Can We Do?

Let's state the truth: threat actors – for the most part – aren't on pause with much of the rest of the world. So, the real question asked is *How can security practitioners develop some level of protection as COVID-19 continues?* The key here is for organizations to establish and maintain resiliency – in our case, with targeted threat intelligence monitoring. These professionals should be investing all efforts in monitoring their sensitive assets as seen by the underground community, in an aim of deterring potential cyberattacks against them. With proactive monitoring, organizations related to the health and support of citizens can focus their efforts on dealing with citizen-focused issues during these unprecedented times.

Interested in learning more about how you can receive real-time targeted intelligence straight from KELA's data lake? [Contact us](#) today to learn more.