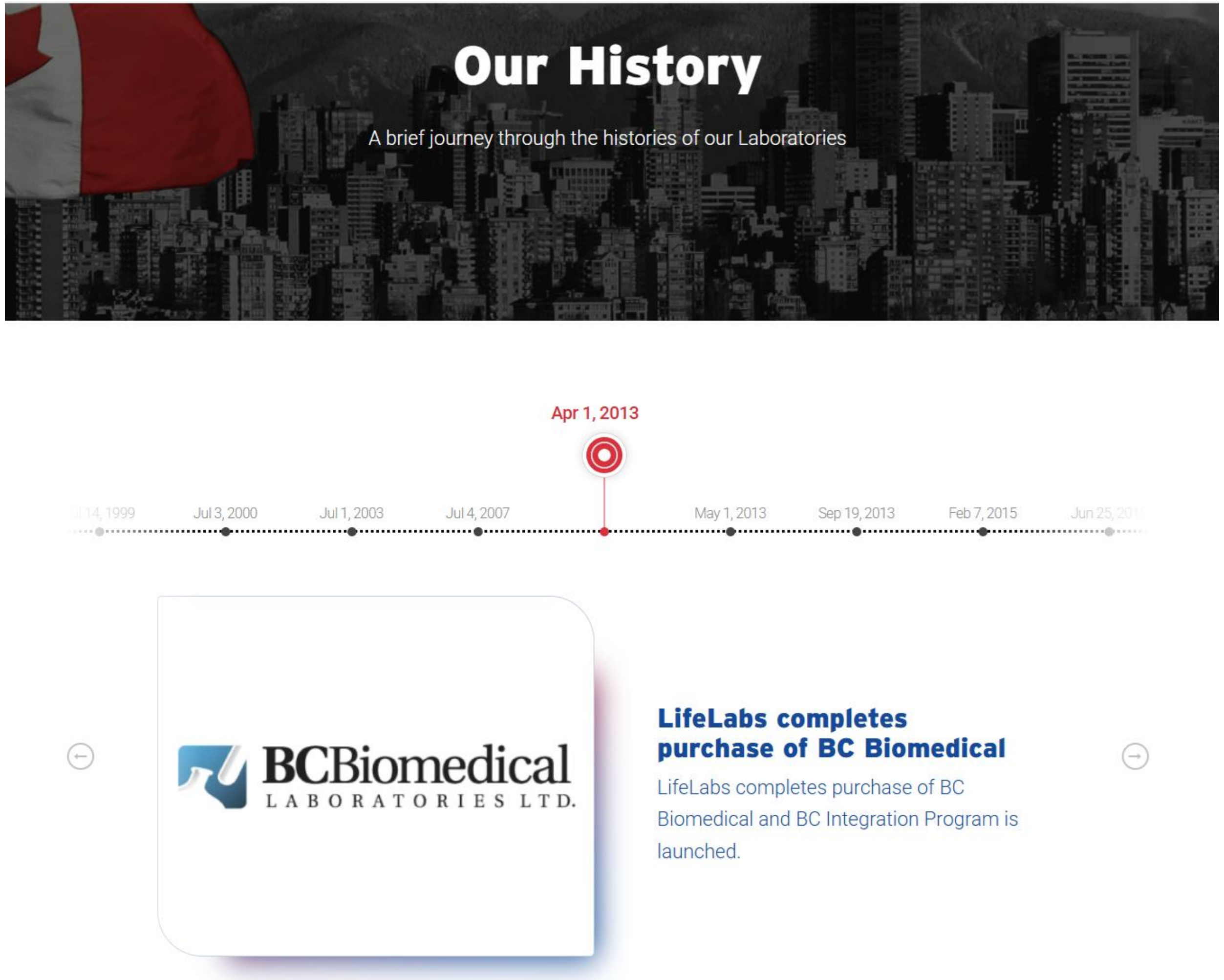
BSIDES VANCOUVER 2025

HACKING LIFELABS

WESLEY WINEBERG

WHO IS LIFELABS?



Our History

A brief journey through the histories of our Laboratories

Apr 1, 2013

LifeLabs completes purchase of BC Biomedical

LifeLabs completes purchase of BC Biomedical and BC Integration Program is launched.

KEY FACTS

LifeLabs is Canada’s largest provider of general health diagnostic and specialty laboratory testing services.

LifeLabs performs over 100 million laboratory tests each year, with 20 million annual patient visits to its locations.

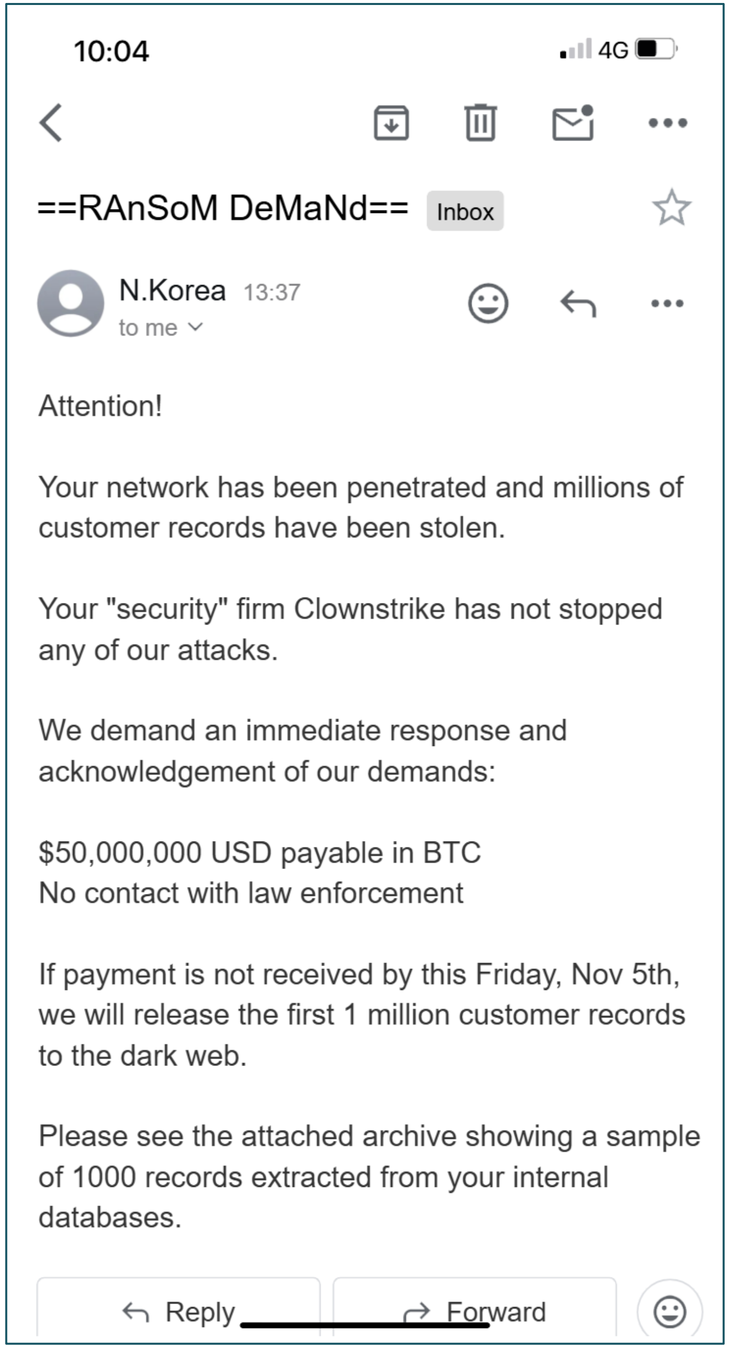
Its website hosts Canada’s largest online patient portal, on which more than 2.5 million individuals access their laboratory results each year.

LET'S GO BACK IN TIME

LET'S GO BACK IN TIME

October 31st, 2019

LET'S GO BACK IN TIME



==RAnSoM DeMaNd==

N.Korea 13:37
to me

Attention!

Your network has been penetrated and millions of customer records have been stolen.

Your "security" firm Clownstrike has not stopped any of our attacks.

We demand an immediate response and acknowledgement of our demands:

$50,000,000 USD payable in BTC
No contact with law enforcement

If payment is not received by this Friday, Nov 5th, we will release the first 1 million customer records to the dark web.

Please see the attached archive showing a sample of 1000 records extracted from your internal databases.

REVISITING THE PAST

2018

Hackers Compromise Lifelabs Servers

2019

Lifelabs Publicly Announces the Data Breach

2024

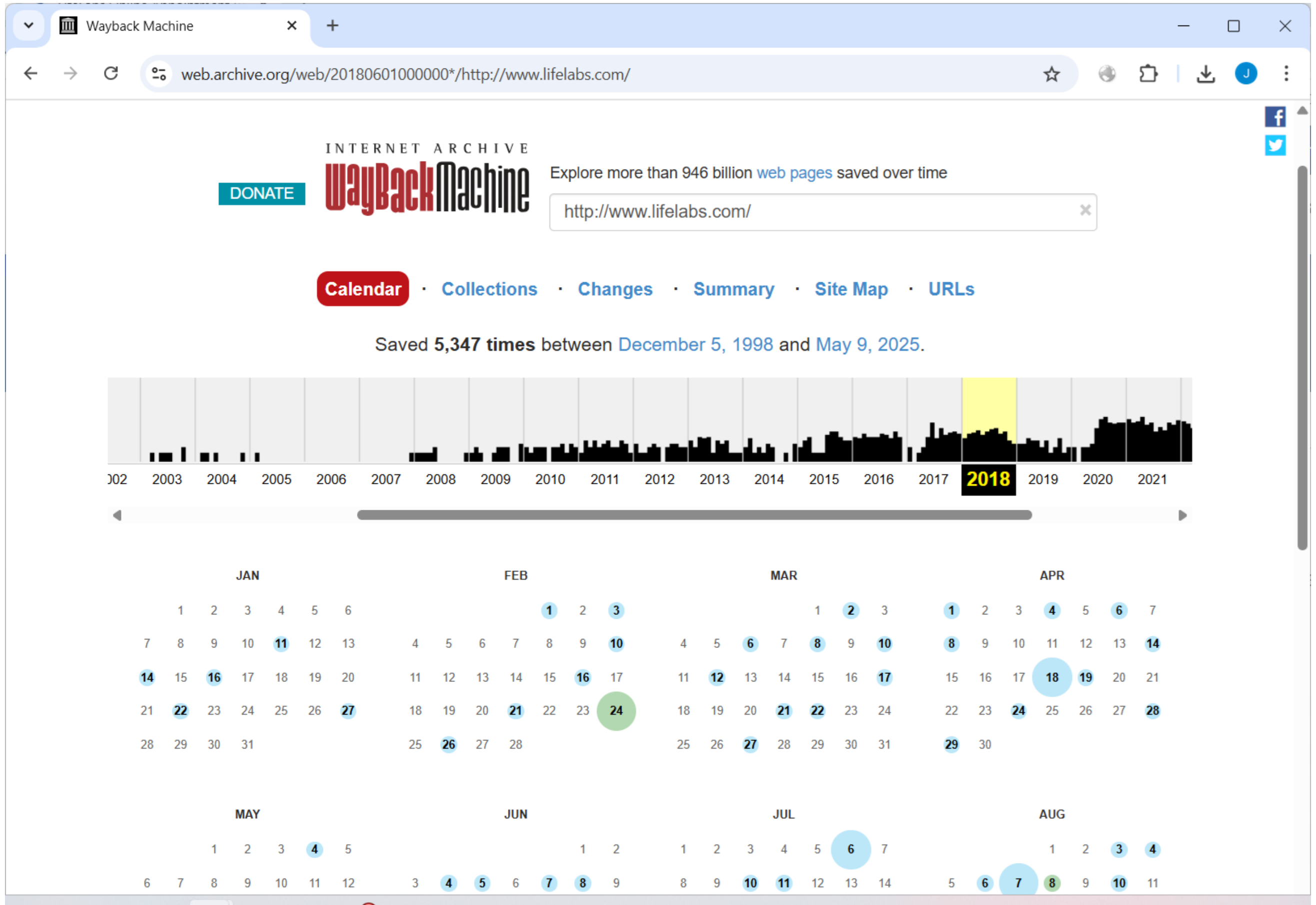
Ontario and BC Privacy Commissioners Win Case To Release Lifelabs Report

ATTACKER FIRST STEPS

- Choose your own adventure:
- Mass scan and look for any finds
- Enumerate and target a specific company / system
- Unclear the approach used here
- Ransomware is almost *always* coordinated through multiple crime groups

VISIT THE ARCHIVES

- Archive.org is valuable to attack, defense, and more!
- The 2018 (prelogin) version of the Lifelabs site can be viewed



Wayback Machine
web.archive.org/web/20180601000000*/http://www.lifelabs.com/
INTERNET ARCHIVE
WaybackMachine
DONATE

Explore more than 946 billion web pages saved over time

http://www.lifelabs.com/

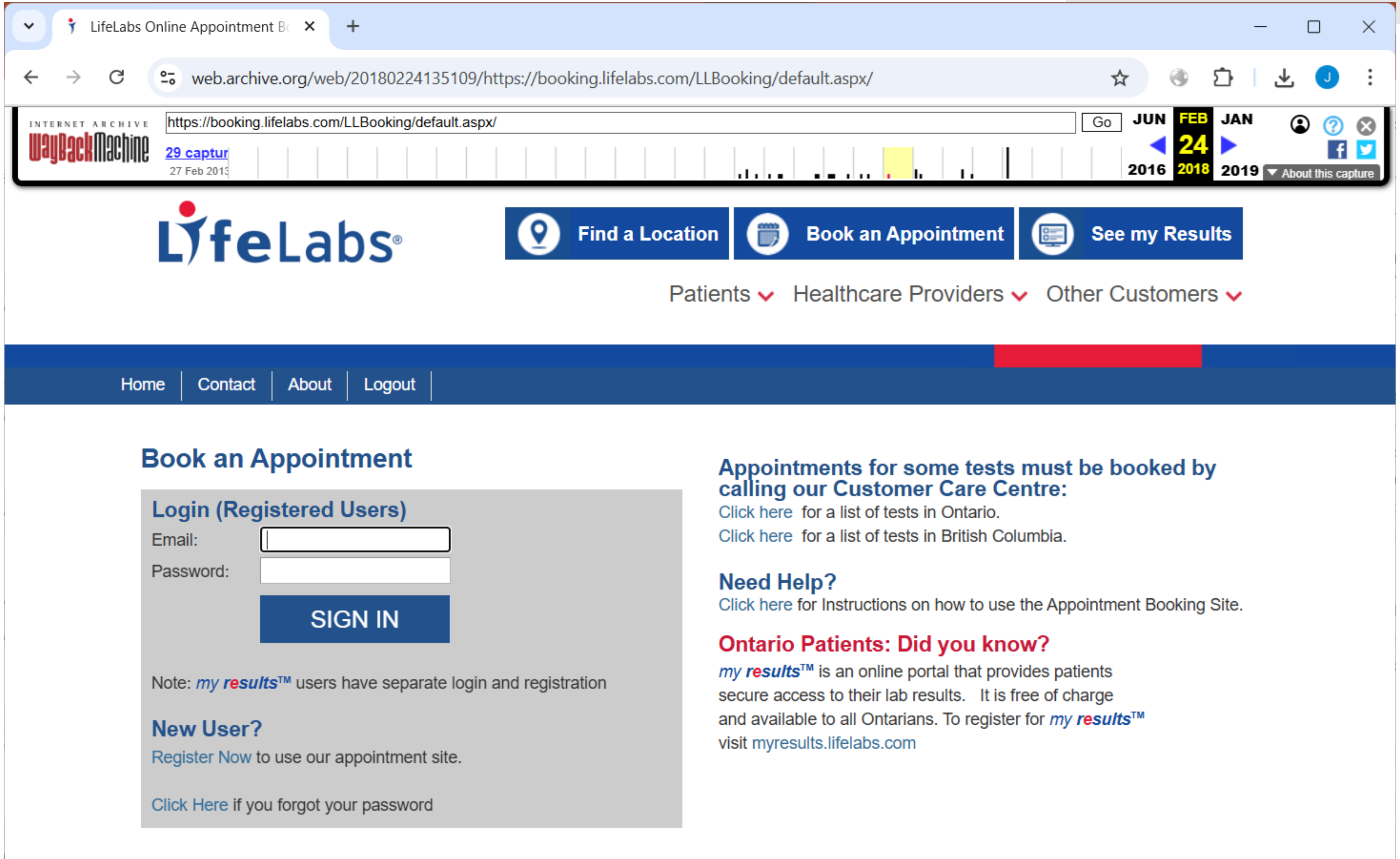
Calendar · Collections · Changes · Summary · Site Map · URLs

Saved **5,347 times** between December 5, 1998 and May 9, 2025.

```
JAN                    FEB                    MAR                    APR
    1  2  3  4  5  6               1  2  3               1  2  3   1  2  3  4  5  6  7
 7  8  9 10 11 12 13    4  5  6  7  8  9 10    4  5  6  7  8  9 10   8  9 10 11 12 13 14
14 15 16 17 18 19 20   11 12 13 14 15 16 17   11 12 13 14 15 16 17  15 16 17 18 19 20 21
21 22 23 24 25 26 27   18 19 20 21 22 23 24   18 19 20 21 22 23 24  22 23 24 25 26 27 28
28 29 30 31            25 26 27 28            25 26 27 28 29 30 31  29 30

MAY                    JUN                    JUL                    AUG
       1  2  3  4  5                  1  2    1  2  3  4  5  6  7            1  2  3  4
 6  7  8  9 10 11 12    3  4  5  6  7  8  9    8  9 10 11 12 13 14   5  6  7  8  9 10 11
```

VISIT THE ARCHIVES



LifeLabs Online Appointment B
web.archive.org/web/20180224135109/https://booking.lifelabs.com/LLBooking/default.aspx/
INTERNET ARCHIVE WaybackMachine
https://booking.lifelabs.com/LLBooking/default.aspx/
Go
29 captur
27 Feb 2013
JUN FEB JAN
24
2016 2018 2019
About this capture
LifeLabs
Find a Location
Book an Appointment
See my Results
Patients
Healthcare Providers
Other Customers
Home
Contact
About
Logout

Book an Appointment

Login (Registered Users)

Email:

Password:

SIGN IN

Note: *my results*™ users have separate login and registration

New User?

Register Now to use our appointment site.

Click Here if you forgot your password

Appointments for some tests must be booked by calling our Customer Care Centre:

Click here for a list of tests in Ontario.

Click here for a list of tests in British Columbia.

Need Help?

Click here for Instructions on how to use the Appointment Booking Site.

Ontario Patients: Did you know?

my results™ is an online portal that provides patients secure access to their lab results. It is free of charge and available to all Ontarians. To register for *my results*™ visit myresults.lifelabs.com

FINGERPRINTING

- Archive.org shows booking.lifelabs.com versions over time:
- Using Telerik 2015.2.729.45 in Feb 2018, Jan 2019 and March 2019
- (Attack discovered Oct 2019)
- Updated to 2020.2.512.45 by Aug 12th, 2020

TELERIK VULNERABILITIES

CVE-2017-9248

- Telerik.Web.UI.DialogHandler.aspx
- Encryption vulnerability
- Base64 decoding “oracle”
- Allows for file access including uploads
- Upload a webshell = RCE

CVE-2017-11317

- Telerik.Web.UI.WebResource.axd
- Hardcoded Encryption Key
- Allows for uploading files
- Upload a webshell = RCE

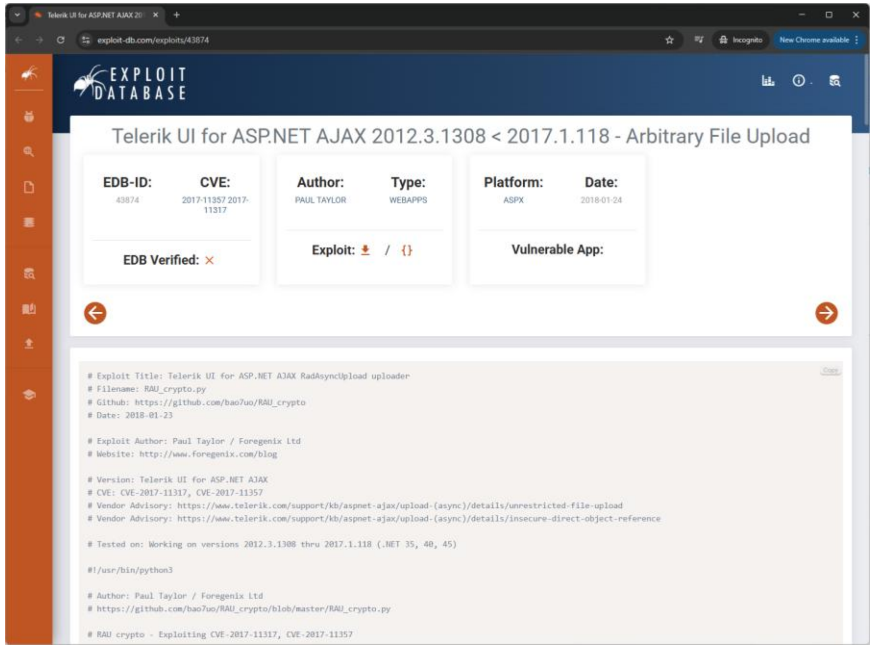
Telerik UI for ASP.NET AJAX

CVE-2017-11317

- Public PoC Since January 2018
- RAU_crypto.py
- Run with:

```
python RAU_crypto.py -P "c:\inetpub\wwwroot" 2014.1.403.35
webshell.aspx "http://4.4.4.4/path"
```

- https://github.com/bao7uo/RAU_crypto



Telerik UI for ASP.NET AJAX 2012.3.1308 < 2017.1.118 - Arbitrary File Upload

EDB-ID: 43874

CVE: 2017-11357 2017-11317

Author: PAUL TAYLOR

Type: WEBAPPS

Platform: ASPX

Date: 2018-01-24

EDB Verified: ✗

Exploit: ⬇ / {}

Vulnerable App:

```
# Exploit Title: Telerik UI for ASP.NET AJAX RadAsyncUpload uploader
# Filename: RAU_crypto.py
# Github: https://github.com/bao7uo/RAU_crypto
# Date: 2018-01-23

# Exploit Author: Paul Taylor / Foregenix Ltd
# Website: http://www.foregenix.com/blog

# Version: Telerik UI for ASP.NET AJAX
# CVE: CVE-2017-11317, CVE-2017-11357
# Vendor Advisory: https://www.telerik.com/support/kb/aspnet-ajax/upload-(async)/details/unrestricted-file-upload
# Vendor Advisory: https://www.telerik.com/support/kb/aspnet-ajax/upload-(async)/details/insecure-direct-object-reference

# Tested on: Working on versions 2012.3.1308 thru 2017.1.118 (.NET 35, 40, 45)

#!/usr/bin/python3

# Author: Paul Taylor / Foregenix Ltd
# https://github.com/bao7uo/RAU_crypto/blob/master/RAU_crypto.py

# RAU_crypto - Exploiting CVE-2017-11317, CVE-2017-11357
```

CVE-2017-11317 - FINGERPRINTING

- Telerik.Web.UI.WebResource.axd?type=rau
- IIS web applications typically have a path associated:
  - `/Telerik.Web.UI.WebResource.axd?type=rau` - If it’s the root path
  - `/appname/Telerik.Web.UI.WebResource.axd?type=rau` - If it’s not
- Version Number Needed:

'2007.1423', '2007.1521', '2007.1626', '2007.2918', '2007.21010', '2007.21107', '2007.31218', '2007.31314', '2007.31425',
'2008.1415', '2008.1515', '2008.1619', '2008.2723', '2008.2826’, '2008.21001', '2008.31105', '2008.31125', '2008.31314',
'2009.1311', '2009.1402', '2009.1527', '2009.2701', '2009.2826', '2009.31103', '2009.31208', '2009.31314',
'2010.1309', '2010.1415', '2010.1519', '2010.2713', '2010.2826',
'2010.2929', '2010.31109', '2010.31215', '2010.31317’, '2011.1315', '2011.1413', '2011.1519', '2011.2712', '2011.2915’,
'2011.31115', '2011.3.1305’, '2012.1.215', '2012.1.411', '2012.2.607', '2012.2.724', '2012.2.912',
'2012.3.1016', '2012.3.1205', '2012.3.1308’, '2013.1.220', '2013.1.403', '2013.1.417', '2013.2.611', '2013.2.717',
'2013.3.1015', '2013.3.1114', '2013.3.1324’, '2014.1.225', '2014.1.403', '2014.2.618', '2014.2.724', '2014.3.1024',
'2015.1.204', '2015.1.225', '2015.1.401', '2015.2.604', '2015.2.623’, '2015.2.729', '2015.2.826', '2015.3.930', '2015.3.1111',
'2016.1.113', '2016.1.225', '2016.2.504', '2016.2.607', '2016.3.914’, '2016.3.1018', '2016.3.1027',
'2017.1.118', '2017.1.228', '2017.2.503', '2017.2.621', '2017.2.711','2017.3.913'

https://web.archive.org/web/20190103014005/https://booking.lifelabs.com/LLBooking/default.aspx/

Live Hacking Time

FOLLOW ALONG!

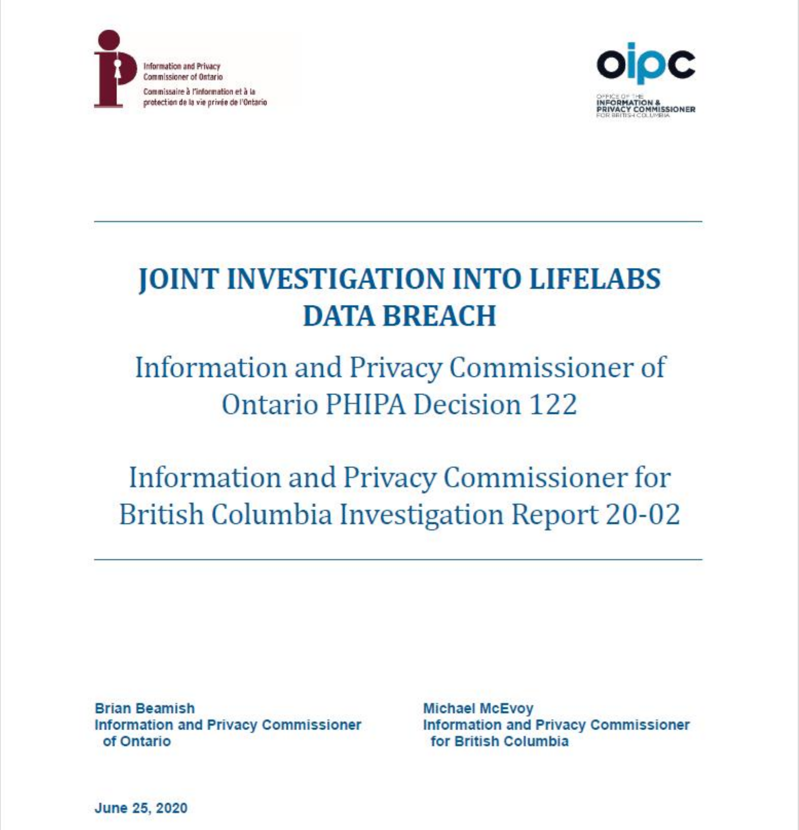
DEFENDER VIEWPOINT

WHAT DID LIFELABS SEE?

(Not much)

PUBLIC REPORTS

- BC & Ontario Combined Privacy Commissioner Report
  - Only 36 pages, you should read it!
- Alberta, Saskatchewan, etc have released their own reports / info



Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

oipc
OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

JOINT INVESTIGATION INTO LIFELABS DATA BREACH

Information and Privacy Commissioner of Ontario PHIPA Decision 122

Information and Privacy Commissioner for British Columbia Investigation Report 20-02

Brian Beamish
Information and Privacy Commissioner
of Ontario

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

June 25, 2020

BANGERS

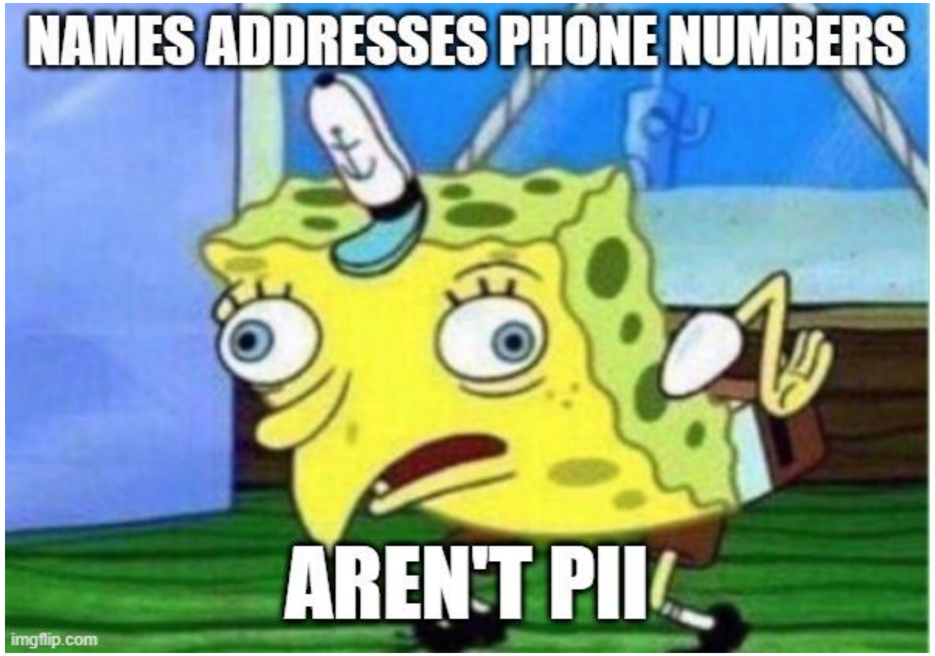
“The attackers claimed to have had the ability to move progressively (or “laterally” as it is known in information security parlance) through LifeLabs’ network with a domain administrator token. However, LifeLabs’ investigation was unable to verify actual lateral movement due to a lack of evidence and available forensic information.”

BANGERS

"Thus, the only real evidence limiting the scope of information compromised in the breach to the four datasets returned by the attackers is the attackers' own claim to that effect, a claim made while negotiating a ransom settlement with their victim."

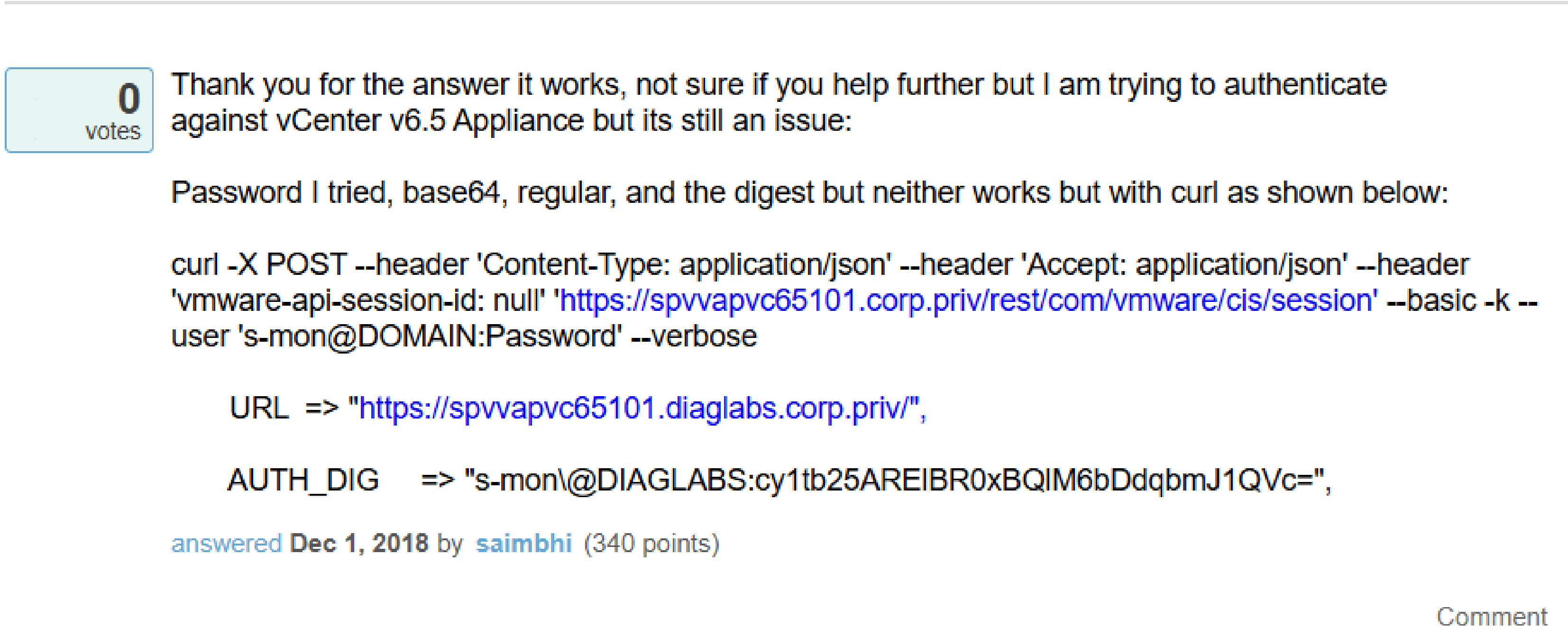
BANGERS

“We disagree with LifeLabs’ assessment and find their approach to be very cavalier regarding the privacy of their clients’ health information. For example, we completely reject the idea that health card numbers are not sensitive”



WHAT WOULD WE FIND IN 2025?

- Unfortunately we can't "really" test too much without permission...
- OSINT shows a lot! Plus a find from 2018:



0 votes

Thank you for the answer it works, not sure if you help further but I am trying to authenticate against vCenter v6.5 Appliance but its still an issue:

Password I tried, base64, regular, and the digest but neither works but with curl as shown below:

```
curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' --header
'vmware-api-session-id: null' 'https://spvvapvc65101.corp.priv/rest/com/vmware/cis/session' --basic -k --
user 's-mon@DOMAIN:Password' --verbose

    URL  => "https://spvvapvc65101.diaglabs.corp.priv/",

    AUTH_DIG     => "s-mon\@DIAGLABS:cy1tb25AREIBR0xBQIM6bDdqbmJ1QVc=",
```

answered **Dec 1, 2018** by **saimbhi** (340 points)

HOW TO DO IR WRONG

DON'T DO THESE THINGS!

- Wipe the infected PC's
- Restart systems (both reboots or "recovering too early")
- Announce a breach before investigating
- Trust insurance, law enforcement, legal counsel to handle *everything*
- Move slowly
- Have no logs

DO THIS INSTEAD:

- Engage an experienced DFIR firm
- Negotiate even if you will not pay
- Get experienced legal advice
- Take care of your mental health

WHY DO WE ALLOW PAYMENTS TO CRIMINALS?

- If Canada banned (made illegal) ransom payments, would breaches increase?
- If Canada regulated Bitcoin the same as real currency, what would be the downsides to the country and the taxpayers?
- How many times has the government of BC or Canada paid a ransom? Why should private corps (or local municipalities) be different?

THOUGHT LEADERSHIP

CARROT OR STICK?

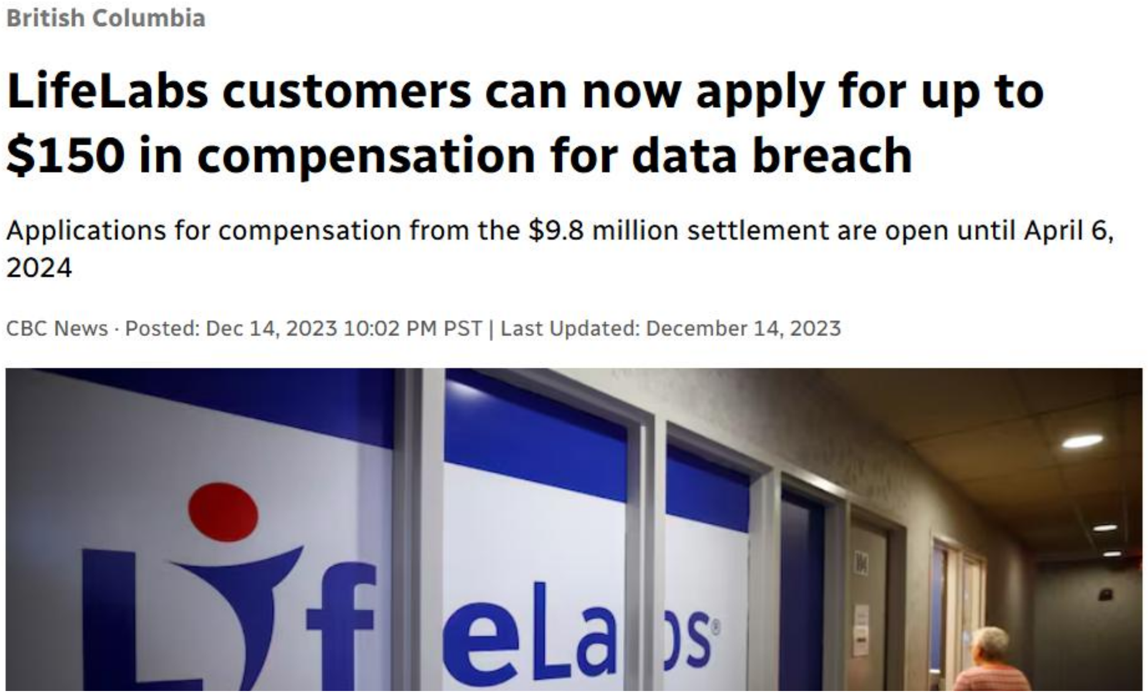
What costs more in the long run?

Hiring and staffing a security team?
Paying a PR firm?

Punishable by fine means legal for a price
Until we meet again

THOUGHT LEADERSHIP

WHAT IS PRIVACY WORTH IN CANADA?

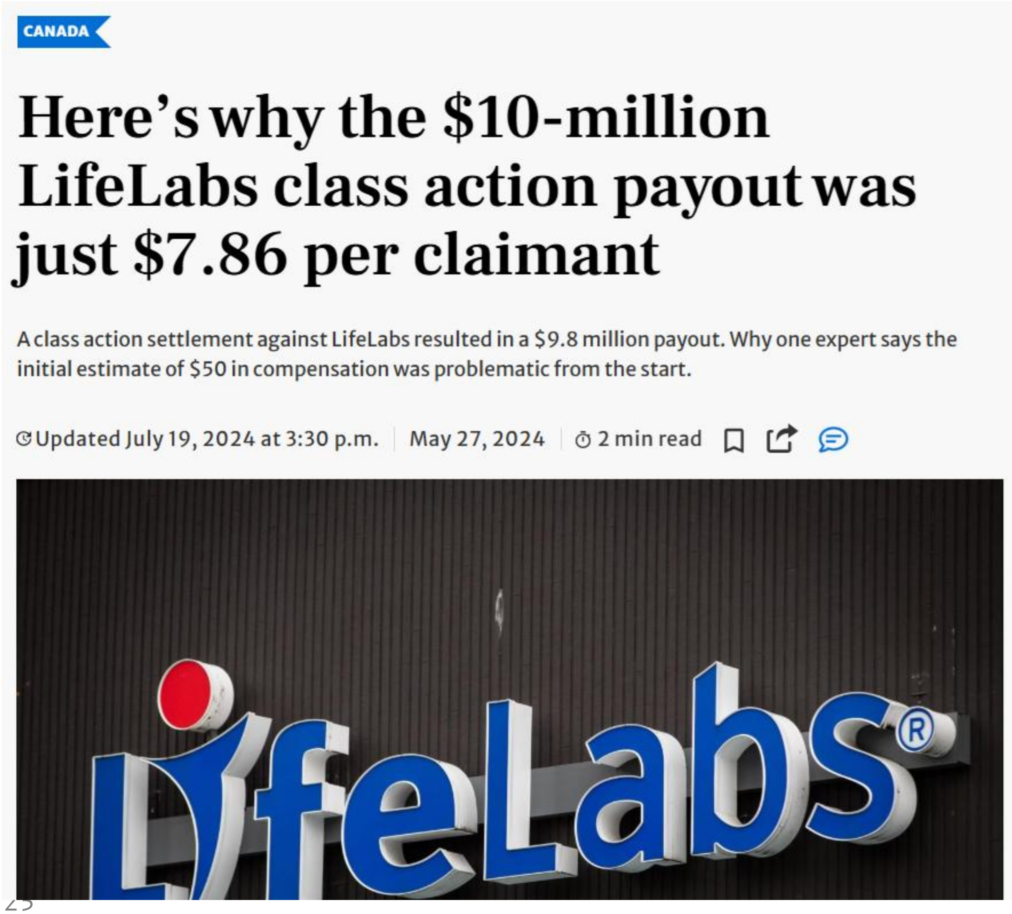


British Columbia

LifeLabs customers can now apply for up to $150 in compensation for data breach

Applications for compensation from the $9.8 million settlement are open until April 6, 2024

CBC News · Posted: Dec 14, 2023 10:02 PM PST | Last Updated: December 14, 2023



CANADA

Here’s why the $10-million LifeLabs class action payout was just $7.86 per claimant

A class action settlement against LifeLabs resulted in a $9.8 million payout. Why one expert says the initial estimate of $50 in compensation was problematic from the start.

Updated July 19, 2024 at 3:30 p.m. | May 27, 2024 | 2 min read

Real Life Rocket Surgeons

THANKS!

WESLEY@EXFILTRATED.COM