Sleep Country Canada

Forensic Investigation – Daily Status Update

September 15, 2020

Overview

On September 3rd ,2020, Herjavec Group's Incident Response was contacted by Sleep Country Canada's John Baigrie (VP of IT) to assist with a forensic investigation related to an internal employee receiving/sharing of sensitive data. We immediately started working with the Sleep Country Canada team to acquire a forensic image of the user' system "TORLAP398".

The following questions to answer:

- Confirm details of the download.
    - Confirmed, with evidence below.
- Investigate if the file has been opened, altered and / or transmitted.
    - Confirmed, with evidence below.
- Investigate if there is any evidence of "covering up" any of the activity.
    - Confirmed, with evidence below.
- Investigate if there is evidence of other similar incidents.
    - Confirmed, with evidence below.

Herjavec Group Objectives

- Determine if more than the one ZIP archive in question was shared externally.
- Determine if the file was opened, alerted or transmitted to sites not presently known.
- Identify if there is any evidence of the user in question attempting to preform anti-forensics on his system.
- Determine if any other users and/or systems that may have been accessed for data found.

Herjavec Group Support Team

- Nic Stevens - Incident Commander
- Nedra Hamouda – Incident Handler
- Kyle Link - Incident Handler

Activities

The following are the activities are completed:

- Obtained forensic image of “TORLAP398”
- Verified forensic image integrity of “TORLAP398”
- Processed disk image of “TORLAP398” to obtain forensic data for analysis
- Identified file/zip in question found to be shared, in addition to acquiring an original copy off the machine “TORLAP398”
- Identified additional users, accounts, email addresses and any personal webmail accounts along with previously known @sleepcountry.ca accounts
- Continuation of forensics on “TORLAP398”, extracting user registry, deleted files, NTFS artifacts
- Build a timeline of events taken place around time of zip file being shared (May 25th, 2020)
- Provide answers to questions asked by Sleep Country Canada team.

1. **Confirm details of the download**

Contents of 1321719_258736-1_620 Royal Ave - New Westminster BC 10M.zip included:

- 105 excel documents
- 49 PDFs
- 11 PowerPoints
- 402 Text Documents
- 85 Word Documents
- 4 IMG files (Avaya software)

Created: 2020-05-25 13:17:10 UTC

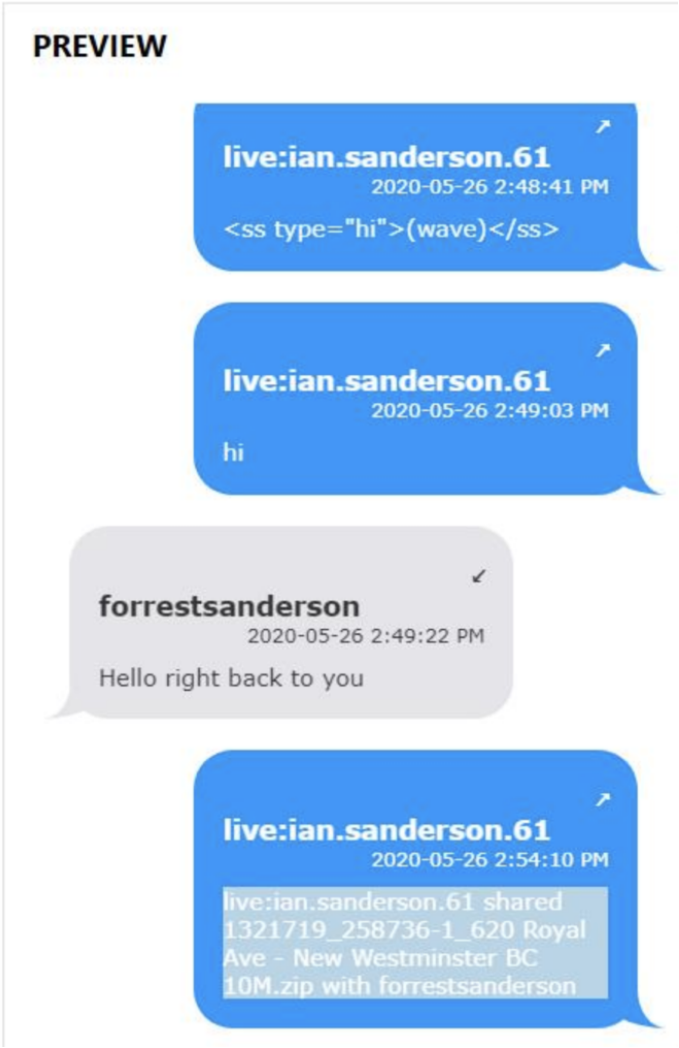
Modified: 2020-05-25 13:24:36 UTC

Accessed: 2020-05-25 13:24:36 UTC

Last Accessed: 2020-05-26 14:49:43 UTC

2. **Investigate if the file has been opened, altered and / or transmitted.**

Yes, file was downloaded and extracted by Ian Sanderson on the host @ TORLAP398. Shared to a Forrest Sanderson via sharefile. In addition, Ian Sanderson (ian.sanderson.61) messaged Forrest Sanderson (forrestsanderson) via Skype chat on 2020-05-26 @ 2:54:10 PM UTC regarding the zip file in question. Appears to have been shared via this Skype chat in addition to the sharefile link @ saasynetworks.sharefile[.]com/d-s96e0a468d9f4f15b



On 2020-05-26 @ 3:30:00 PM EST Ian Sanderson invited Forrest Sanderson "4rest@sympatico.ca" to join him via a Zoom video call. This call was between only Ian Sanderson and Forrest Sanderson.

ARTIFACT INFORMATION

Sender Name	**Ian Sanderson**
Sender Exchange Account	**/o=Sleep Country Canada/ ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/ cn=Recipients/cn=Ian Sandersond12**
Recipients	**Ian Sanderson <Ian.Sanderson@sleepcountry.ca>, 4rest@sympatico.ca**
Subject	**Ian.Sanderson@sleepcountry.ca's Zoom Meeting**
Start Date/Time	**2020-05-26 3:30:00 PM**
End Date/Time	**2020-05-26 8:30:00 PM**

3. **Investigate if there is any evidence of "covering up" any of the activity.**

Evidence of sharefile[.]com URI was deleted from Ian Sanderson's machine, artifact obtained from WebCacheV01.dat was carved (obtained from deleted space) during forensics. Strong indication the user was attempting to cover up the history of his web traffic around the time of the file being shared (May 25th, 2020). It is worth noting that prior to sharefile event there were events relating to logins to a gmail account (obtained from same WebCacheV01.dat carved from deleted).

4. **Investigate if there is evidence of other similar incidents.**

Additional zip archives found relating to Penetration test results, Vulnerability Scan results, Invoices, Scripts, Logs from multiple tools, monthly reports, ACL's for Checkpoint Firewalls, Network Diagrams, User lists. Found no additional signs of similar exfiltration of compressed archives leaving this users computer from the available data given to the Herjavec Group team from Sleep Country Canada.

Next Steps

The following activities are scheduled:

- Call with Sleep Country Canada team to answer any further questions.