



## Pandora's Box: Another New Way to Leak All Your Sensitive Data

Yes, the cloud is still leaking data. This time, we can't blame the SRE team though, everyone has been sharing files publicly, yes, even you probably.



Image Credits: Getty Images

### Introduction

Box is a "cloud based content management platform", primarily used to share files and folders. Much like AWS S3 buckets, these files can be shared to anyone with the link, restricted to those within your company (Box Enterprise), or to specific users.

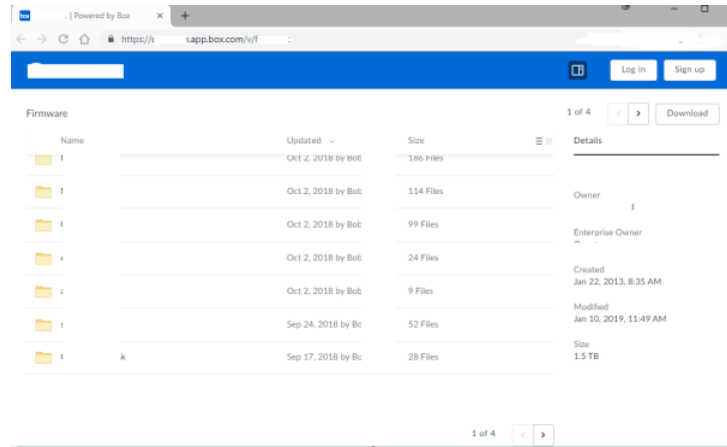
Companies using Box Enterprise get their own sub-domain, and documents saved on Box can be shared to anyone with the unique URL. Users can also name the shared link to whatever they choose. Unfortunately, the sub-domain, URL, and folder names are easily brute-forceable. You can see where this is going.

### What We Found

After identifying thousands of Box customer sub-domains through standard intelligence gathering techniques and using a relatively large wordlist, we discovered hundreds of thousands of documents and terabytes of data exposed across hundreds of customers.

A sampling of data we found:

- Hundreds of Passport Photos
- Social Security and Bank Account Numbers
- High profile technology prototype and design files
- Employees lists
- Financial data, invoices, internal issue trackers
- Customer lists and archives of years of internal meetings
- IT data, VPN configurations, network diagrams



Screenshot displaying 1.5 TB Shared Box Folder.

Initially, we intended to reach out to all the companies affected but we quickly realized that was impossible at this scale. A large percentage of the Box customer accounts we tested had thousands of sensitive documents exposed. We alerted a number of companies that had highly sensitive data exposed, reached out directly to Box, and published this write up.

If your company uses Box, there is a good chance you are leaking sensitive data already and you may want to finish reading this after you disable public file sharing.

### A Feature, Not a Bug

This is not a bug or vulnerability in Box and has been reported on in the past. This was even tweeted out back in June 2017 but didn't seem to get much attention.



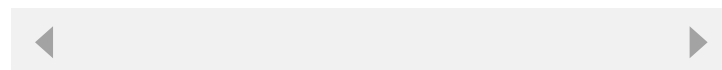
Box was also mentioned in the [news](#) recently for how Google was caching sensitive Box shared document links.

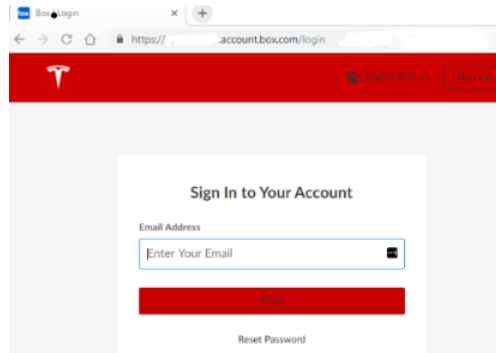
The issue could be compared to AWS S3 buckets publicly hosting any manner of documents. Not all are sensitive, but often times they are. On one hand this issue is worse than the S3 bucket issue because finding a company's Box account is fairly easy, unlike with S3 bucket names which can be long and difficult to guess. On the other hand, employees seem much less likely to store full databases in Box.

### Approach

After accessing some shared files in Box, we noticed the link looked something like this:

`https://<companyname>.app.box.com/v/<file/foldername>`



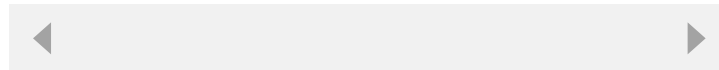


Screenshot of Box Enterprise Sign On page

We began enumerating for sub-domains of other company's Box accounts through standard open source intelligence. These can be easily verified by going to <https://<companyname>.account.box.com>. If the link returns the company's logo, they have a paid account and are probably susceptible.

At that point, we began brute forcing folder and file names which began returning results faster than we could review them.

<https://<companyname>.app.box.com/v/<filename>>



In the first couple days of a running a non-aggressive scan, we had thousands of files and terabytes of data from dozens of companies. A lot of the data was indeed public information or simply marketing material, but a considerable amount was sensitive. As mentioned previously these included passport photos, prototype details with raw CAD files for some very prominent new and coming tech, Social Security Numbers, financial documents, internal IT data including network diagrams and asset information, and innumerable "confidential" slide decks.

## How to Fix Your Box Account

Box specifically calls out the issue of URL guessing and recommends the following changes.

Creating public custom shared links for any content may result in anyone who can guess the URL gaining access to that content. To reduce risk to sensitive content, we recommend that:

Administrators configure Shared Link default access to 'People in your company' to reduce accidental creation of public (open) links by users.

Administrators regularly run a shared link report (as described here) to find and manage public custom shared links.

Users do not create public (open) custom shared links to content that is not intended for public consumption

For more information, see Box's documentation.

<https://community.box.com/t5/Using-Shared-Links/Securing-Shared-Links/ta-p/61843>

## Vendor and Company Response

Fortunately, most companies came back with positive feedback and remediated the issue promptly. We only contacted a small minority of affected companies and vendors with either public responsible disclosure programs or exposed highly sensitive data. Box acknowledged the issue and updated their file sharing guidelines.

## Timeline

September 24th - Reported results to Box

September 28th - Box releases Public Service announcement in regards to report


March 11th - Adversis publishes this article

### **Can this be Bug Bountified?**

Of course! Check out <https://github.com/adversis/PandorasBox>. Pandora's Box will take a list of companies, find the ones that have a valid box account and begin to scan for exposed files and folders.

Please note that you should not do this if you are a Box customer as their terms of service prohibit automated processes to access or use Box.

## **Subscribe to Adversis**

 **Subscribe now**