Post Exploitation Operations with Cloud Synchronization Services

Jake Williams
jwilliams@csr-group.com
@MalwareJake
Agenda

• The problem (cloud backup/synchronization)
• The solution (DropSmack)
• Next steps
• Insecure Authentication Case Study
• Post Exploitation Activities
• Where to go from here
Chief Scientist at CSRgroup
  – Incident Response/Forensics
  – Penetration Testing
  – Exploit Development
PhD Candidate (Computer Science)
Two time winner of the DC3 Forensics Challenge
SANS Instructor and author – Malware, Cloud Forensics, Offensive Forensics
Disclaimer
(damn lawyers made me do it)

• Our lawyers said to tell you:
  – Dropbox isn’t broken, and neither are their competitors’ products
  – We don’t want you to stop using them
  – You should carefully evaluate your own security posture before cancelling service, changing contracts, etc.
  – DropSmack is NOT malware, it is designed to operate in authorized penetration testing scenarios ONLY
Cloud Synchronization

• Implies more than just online backup
• Files placed in the ‘special folders’ get replicated to all configured machines
  – This may include smartphones
  – Think cross-platform attacks 😊
• Infecting files heading for cloud backup (like Mozy) would be neat too
  – But no command and control (C2)
History of Insecurity

- Dropbox authentication horribly broken
  - More on this later
- Dropbox ‘no password day’
- Dropbox Mobile file metadata in the clear
- Other service providers aren’t getting enough research cycles to make headlines
Foundational Work

• Dark Clouds on the Horizon (2011) detailed the idea of using cloud synchronization software for covert data exfiltration
• Frank McClain and Derek Newton (2011) researched the Dropbox database format and published the details
  – Dropbox promptly changed them
• Ruff and Ledoux (2012) reverse engineered Dropbox software to analyze security
  – Again, Dropbox quickly changed internal details
A Case Study

• A client wants a no-holds barred penetration test, long engagement time, completely black-box

• No out of date patches on publicly facing servers, no poorly coded web portals

• Social engineering fails due to awesomely trained employees
  – Don’t you wish that usually happened?
A Case Study (2)

- Physical security is rock solid
- Guest wireless network is completely segmented from the production network
- Production wireless network is properly secured
Spam – the normal answer

- Spam fails too
- Some users actually hit our server with older browsers but we can never run a payload
- Keep spamming just in case
  - I don’t like dogs anyway 😊

Stop the spam or we'll shoot this dog.
Status

- Social Engineering? Nope
- Spam? Nogo
- Web Apps? Negative
- Vulnerable Network Services? Nein
- Physical Security? HeT
- Wireless? Non
- Overall status???
FAIL

Time for Plan B...
Found the CISO

• We manage to exploit the CISO’s laptop at a local ISSA meeting
  – USB HID attack 😊

• Surprise! Your awesome corporate firewall sucks when your user isn’t behind it

• Now to just pivot into the internal network over the VPN connection...
No VPN? WTF?

- No VPN software on the CISO’s laptop
  - But he had confidential corporate documents
- No evidence of USB drive use
- How is this stuff getting on his machine?
  - You guessed it, Dropbox
  - But could have been ANY cloud synch software
  - The title of the talk might have clued you in 😊
What now?

• It stands to reason that files in the Dropbox folder came through the cloud
  – And that means Dropbox may be installed inside the corporate network
  – And it is allowed out by the firewall!

• We just need C2 over Dropbox
  – We can already deliver files
    • via Dropbox
DropSmack is born

- DropSmack communicates by monitoring the file synch folder for tasking files
- It exfiltrates files using the same mechanism
- Bonus: Many DLP applications see files placed in a Dropbox folder, especially a non-default folder as a **LOCAL FILE COPY**
  - No need for encrypted rar 😊
DropSmack Longevity?

• DropSmack is slow and kludgy
  – I’d prefer not to use it long term
• Now that we have bi-directional C2, we can figure out how to get a more traditional C2 channel past the corporate firewall
  – Being able to observe results from failures always helps
  – Watch legitimate traffic leave the network from the inside
DropSmack Features?

- DropSmack implements the following commands:
  - PUT
  - GET
  - DELETE
  - EXECUTE
  - SLEEP
  - MOVE
- We considered adding more, but this combination gets you everywhere you need to go
  - Everything else is just cake
  - But the cake is a lie!
Deploying DropSmack

• Use a file infector of your choice
  – Office macros are my favorite
  – Get victim to open by employing social engineering (or just wait)

• You must maintain access to the original infection point to task the tool on the other side of the Dropbox service
So what’s new?

- DropSmack v1 only operated against Dropbox
- But some victims use other synch services
- We need a better mousetrap...
DropSmack v2: a better mousetrap

• DropSmack v2 works against:
  – Dropbox (of course)
  – Box
  – SkyDrive
  – Google Drive
  – Spider Oak
  – SugarSync
  – JustCloud (just because we can)
Insecure Auth Case Study

• When I started looking at synch applications, everything I saw was HTTPS
• So I thought “Cool. These guys aren’t total idiots”
• But I kept looking anyway…
WTF??? Is it 1999?

• And then I found this:

• Which, by the way, is the default
FAIL, tons of FAIL

• Who the f%^$ cares how your files are transmitted if you auth using HTTP????

• One facepalm isn’t enough to do this justice
Refer a friend!

- Do you hate your coworkers? Your ex? Refer them to the service and get free storage!

Earn 100MB FREE space for each person that joins!

Invite by Email

Share on Twitter or Facebook
So who is this?

- Who produced this Big Bag of Fail™ (BBoF)?
- This one is branded as JustCloud, a company you’ve probably never heard of

![justcloud.com](justcloud.com)

- But they have several different brandings that are part of BackupGrid
- The ones I looked at use the same AWESOME, secure software
How did I find JustCloud?

• I searched Google for ‘skydrive’ looking for some pictures for another presentation

• I thought “what the hell, I’ve got nothing better to do...”
Is this really news?

Forget Dropbox, Skydrive, Google Drive: NOW TOP Cloud Storage Unlimited Free
When it comes to cloud storage, there are a whole bunch of fluffy options up there in the proverbial sky. Maybe you need unlimited storage, or maybe you need it for free, and if you still thinking Dropbox & Google Drive or Skydrive to be the only one alternative to online storage? then you must to read the issues of Dropbox & Google Drive. So the best thing you can do to keep your files safe in the cloud is to choose the right storage provider. Because Cloud Storage become backup your critical documents from computer virus attacks. Well, how to choose The Best Online Cloud Storage in among many options? the answer is only a recommendation and testimonials from people

Get The Best Cloud Storage >>> Visit Here >>> www.Goo.gl/QvBEC

Based on our customer testimonials, our cloud storage is the best when compared Dropbox & Google Drive, Skydrive. Because our Cloud Service provides full-featured and reliable security system like Sync Multiple Computers, 100% Automated Backups, Encrypted-Secure, Unlimited Space
Responsible Disclosure Fail

• This was great! No contact info. At all...

• But the login form is, you guessed it, HTTP
• Wait... I can log in with my JustCloud account?
• Ok, maybe I’ll contact support about these issues

[Image: Account Support]

• Oops, they forgot the link to actually submit a support request...
  – Are they clowning me???
This isn’t only JustCloud

• Another service called ‘ZipCloud’ uses exactly the same software (and storage backend)
• www.thetop10bestonlinebackup.com (my ‘go to’ source for advice on all things cloud) rates JustCloud as the #1 backup service!
More clowns please!

<table>
<thead>
<tr>
<th>Trend</th>
<th>Company</th>
<th>Price</th>
<th>Storage</th>
<th>Score</th>
<th>Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>↑</td>
<td>justcloud.com</td>
<td>Free (Limited Time)</td>
<td>Unlimited</td>
<td>98% Rate</td>
<td>Read Review</td>
</tr>
<tr>
<td>↓</td>
<td>zip cloud</td>
<td>$4.95</td>
<td>250GB</td>
<td>97% Rate</td>
<td>Read Review</td>
</tr>
<tr>
<td>↑</td>
<td>myPCBackup.com</td>
<td>$2.95</td>
<td>Unlimited</td>
<td>96% Rate</td>
<td>Read Review</td>
</tr>
<tr>
<td>↓</td>
<td>SGS</td>
<td>$6.66</td>
<td>50GB</td>
<td>93% Rate</td>
<td>Read Review</td>
</tr>
<tr>
<td>↓</td>
<td>SugarSync</td>
<td>$9.99</td>
<td>60GB</td>
<td>92% Rate</td>
<td>Read Review</td>
</tr>
<tr>
<td>↓</td>
<td>mozy</td>
<td>$7.99</td>
<td>125GB</td>
<td>91% Rate</td>
<td>Read Review</td>
</tr>
<tr>
<td>↑</td>
<td>BackupGenie</td>
<td>$4.95</td>
<td>250GB</td>
<td>91% Rate</td>
<td>Read Review</td>
</tr>
<tr>
<td>↓</td>
<td>Dropbox</td>
<td>$9.99</td>
<td>50GB</td>
<td>91% Rate</td>
<td>Read Review</td>
</tr>
<tr>
<td>↓</td>
<td>box</td>
<td>$9.99</td>
<td>25GB</td>
<td>90% Rate</td>
<td>Read Review</td>
</tr>
</tbody>
</table>
Are we done with JustCloud?

• Nope.
• If you are sitting on the mail server and see email from JustCloud, it might just be your lucky day!
Email Links

- Ok, good. They didn’t send the password in plaintext. That’s a step in the right direction...

- Anything else stand out?
HTTP Again???

- HTTP again? Really?
- At least that link is only used to verify the email address I registered with.
  - Phew, we’re safe!

• It actually logs you in!
  – Login link **never** expires, multiple use auth token
Wow. I’m speechless...

QUADRUPLE FACEPALM

I had to grow extra arms to show you how much you failed.
Anyone else?

- We’re continuing to look at other applications and possible exploitation avenues they might provide
- Nobody else we’ve seen was close to this bad
General Post Exploitation

• The obvious:
  – Pilfer files directly from the cloud
  – Upload infected files to the cloud

• The interesting:
  – Find other connected devices

• The Evil:
  – Cancel the account, deleting stored files from the cloud!
General Post Exploitation (2)

- Log files stored on the client often show information about files previously sent to the cloud (files may no longer exist locally)
  - Ex. SkyDrive device log
General Post Exploitation (3)

- Databases stored on the client often show valuable information about files previously sent to the cloud
  - Ex. JustCloud mpcb_file_cache.db

```
<table>
<thead>
<tr>
<th>path</th>
<th>fileName</th>
<th>hash</th>
<th>size</th>
</tr>
</thead>
<tbody>
<tr>
<td>{syncfolder}</td>
<td>{syncfolder}</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>{syncfolder}\</td>
<td>JustCloud Quick Start Guide.pdf</td>
<td>9e92b30d89e47418651552e040561176</td>
<td>991271</td>
</tr>
<tr>
<td>{source:11210377}\</td>
<td>C:</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>{source:11210377}\</td>
<td>Users</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>{source:11210377}\</td>
<td>Jake</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>{source:11210377}\</td>
<td>Desktop</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>{source:11210377}\</td>
<td>desktop.ini</td>
<td>9e36cc3537ee9ee1e3b1f0a4e761045b</td>
<td>282</td>
</tr>
<tr>
<td>{source:11210377}\</td>
<td>regshot.exe</td>
<td>a9a8fbcace9c4999a77d53e0fa085</td>
<td>73728</td>
</tr>
</tbody>
</table>
```
Post Exploitation (JustCloud)

• Users may be enticed to enter phone numbers for free add-on storage
  – Phone numbers useful to social engineering or...
Post Exploitation (JustCloud)

- Web Interface allows file upload
  - With automatic synch back to clients
- With the email link, you can move malware to the endpoint client
  - I’m thinking DropSmack!
Post Exploitation (Dropbox)

• An RSS interface for their Dropbox account?
  – Cyber stalk your victims!

• RSS Feed Example – at least you have to auth to get the file...

![RSS Feed Example](image)
Post Exploitation (SpiderOak)

• SpiderOak is sort of special because they don’t store anything unencrypted
• Everything is encrypted client side
  – Like BoxCryptor
• Prevents upload/download of files from web interface
• But SpiderOak allows local network backup
  – With saved creds
Post Exploitation (SpiderOak)

• I was totally going to RE getting stored creds from SpiderOak’s config
• Stored creds allow you to pivot to other network locations 😊
• But then I noticed that FTP is allowed!
  – Start FTP server
  – Change config
  – Put files in sync folder
  – Capture creds
  – Profit!
Post Exploitation (SpiderOak)

- What the f%$ are “Remote Diagnostics??”
- That sounds like trouble to me....
- Ran out of time to look at this, but betting it’s another BBoF™
Prevention

• For the love of security, start whitelisting
  – Not a silver bullet, but makes my job much harder
• Use services like SpiderOak that don’t store files unencrypted in the cloud
• BoxCryptor is another option
  – Bonus: you can keep using the same service
  – Note: BoxCryptor doesn’t help if you unwittingly encrypt and decrypt tasking files/exfil
Detection

• Look for tasking files on the end hosts
• Employ an NGFW and watch for sensitive data leaving the network
  – This presumes some exfil to detect
• Watch your process lists
  – This shouldn’t be news
• For the love of security, start whitelisting
  – Not a silver bullet, but makes my job much harder
Future Work

• DropSmack can get better
  – Up next: re-implement as a shell extension

• Bridging multiple synchronization services is a pain
  – Different DropSmack installations tend to get confused if they are looking for files with the same tasking names
  – Unique identifiers would help resolve this
Future Work (2)

• The client side popup problem still needs to be addressed
  – Most services create popups when new files are delivered

• Overall we need a better mechanism for hiding the tasking files
  – Exfil less of an issue
Moar Demos

- Time permitting of course

I demand

MOAR!!!!1!
Thank You!

Please complete your speaker feedback surveys

@MalwareJake
jwilliams@csr-group.com