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

$whoami

- Chief Scientist at CSRgroup
  - Incident Response/Forensics
  - Penetration Testing
  - Exploit Development

CSRgroup
computer security
consultants

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- No out of date patches on publicly facing servers, no poorly coded web portals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

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 ☺

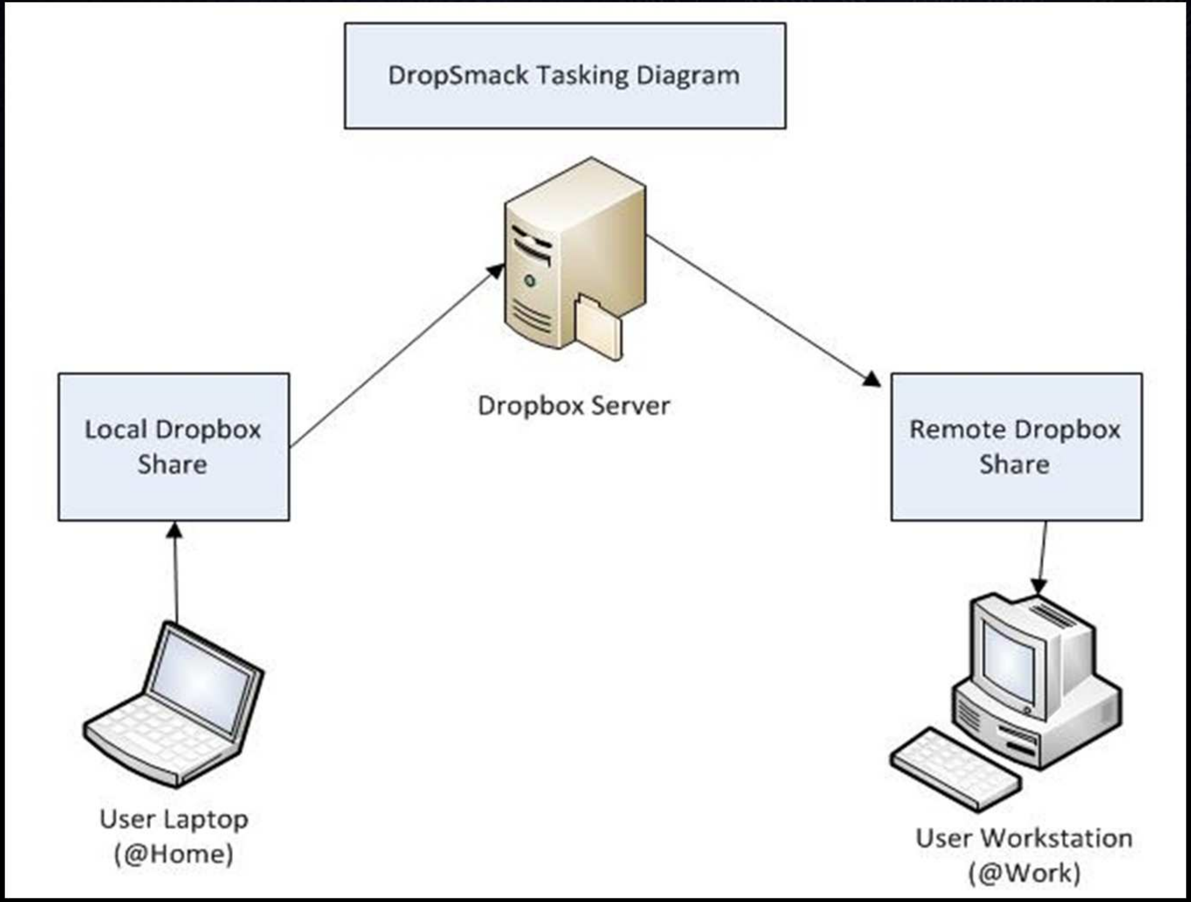
What now?

- 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 Comms



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?

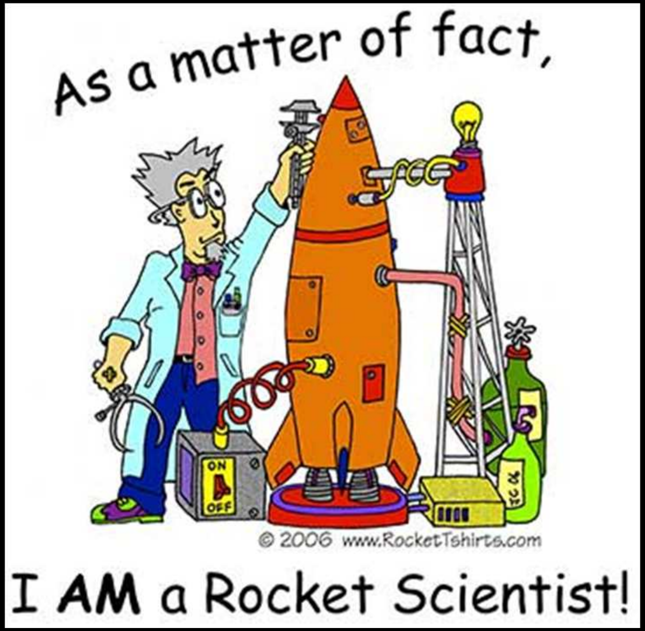
- DropSmack v1 only operated against Dropbox
- But some victims use other synch services
- We need a better mousetrap…

DropSmack v2: a better mousetrap

- DropSmack v2 works against:
  - Dropbox (of course)
  - Box
  - SkyDrive
  - Google Drive
  - Spider Oak
  - SugarSync
  - JustCloud (just because we can)

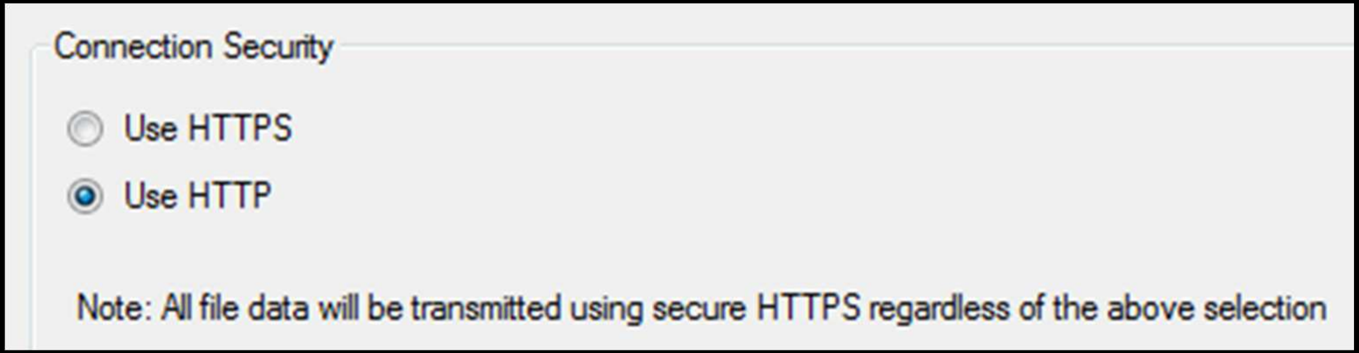
Insecure Auth Case Study

- 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:



Connection Security

○ Use HTTPS

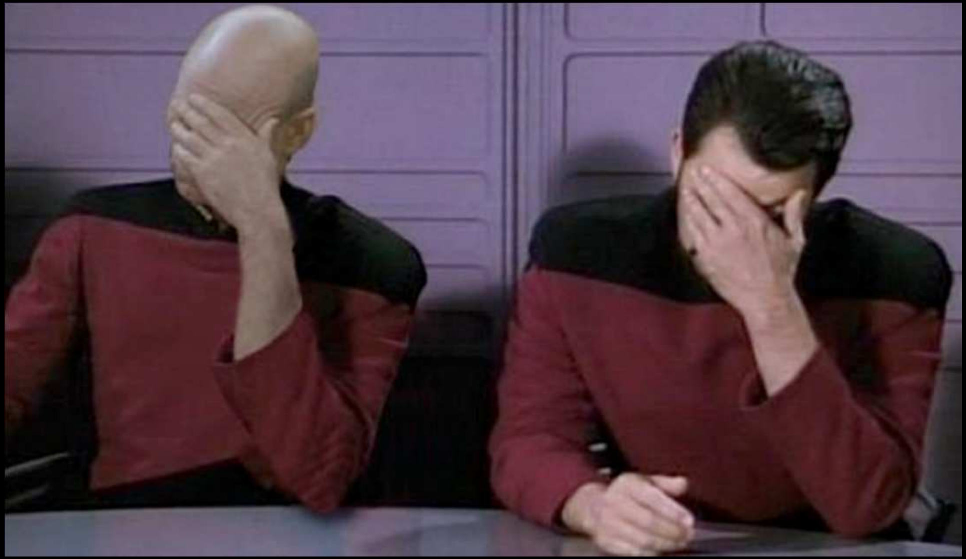
● Use HTTP

Note: All file data will be transmitted using secure HTTPS regardless of the above selection

- Which, by the way, is the default

FAIL, tons of FAIL

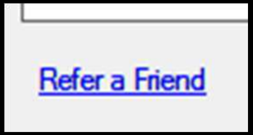
- Who the f%^$ cares how your files are transmitted if you auth using HTTP????



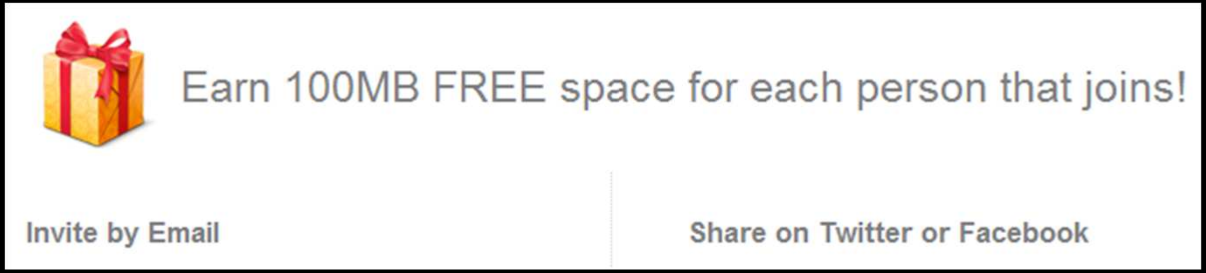
- One facepalm isn't enough to do this justice

Refer a friend!

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



Refer a Friend



Earn 100MB FREE space for each person that joins!

Invite by Email

Share on Twitter or Facebook

So who is this?

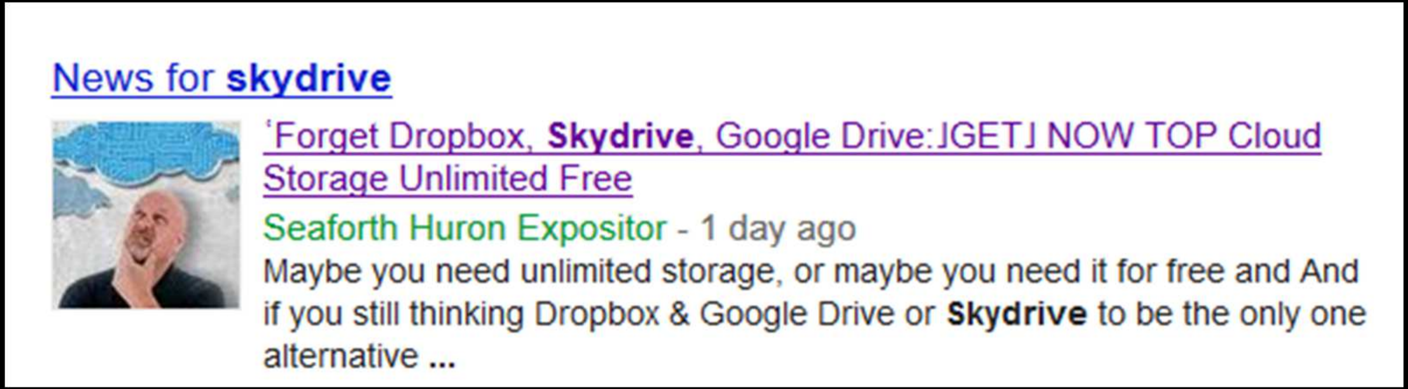
- Who produced this Big Bag of Fail™ (BBoF)?
- This one is branded as JustCloud, a company you’ve probably never heard of

justcloud.com

- 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



News for **skydrive**

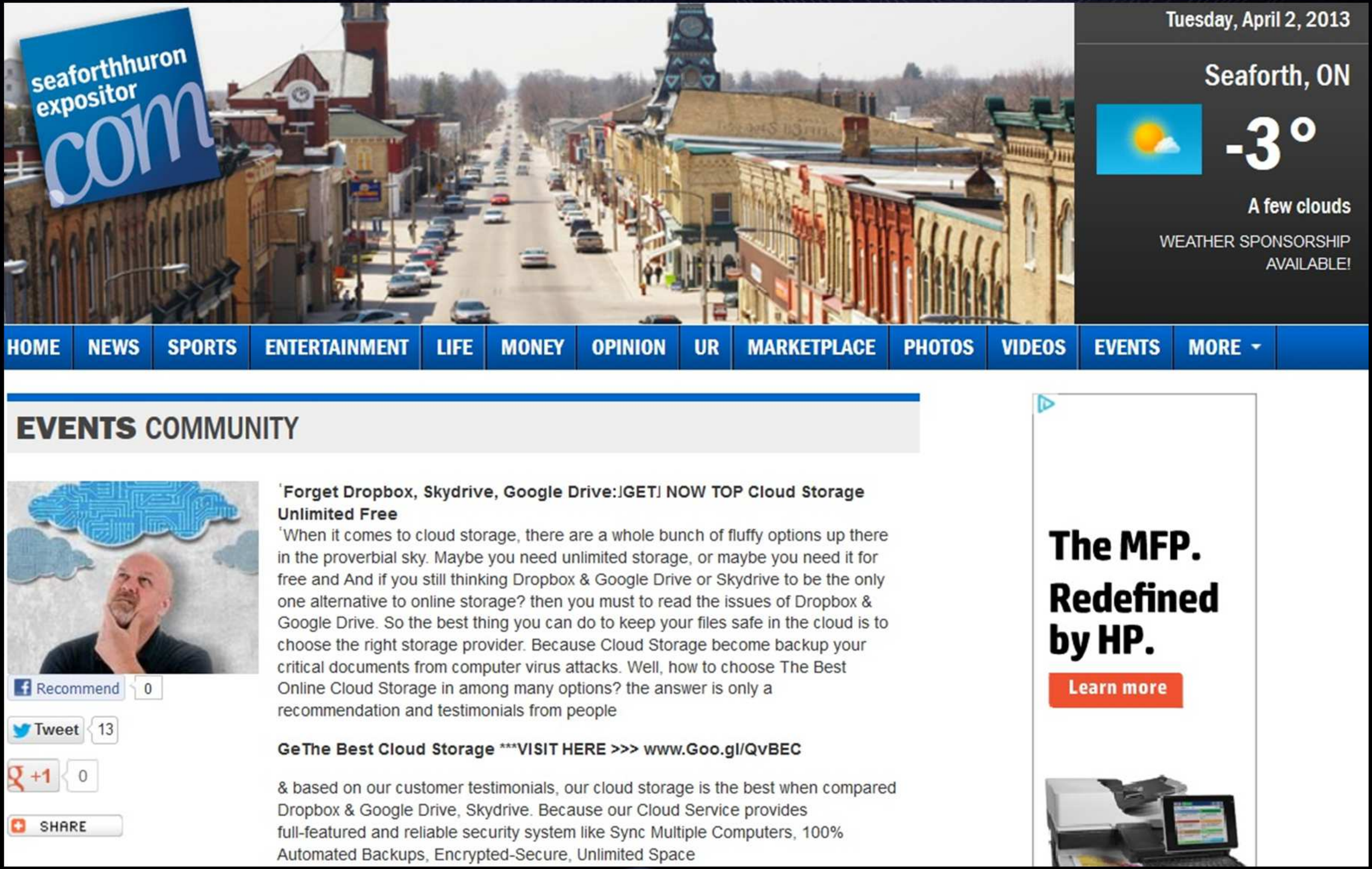
'Forget Dropbox, **Skydrive**, Google Drive:JGETJ NOW TOP Cloud Storage Unlimited Free

Seaforth Huron Expositor - 1 day ago

Maybe you need unlimited storage, or maybe you need it for free and And if you still thinking Dropbox & Google Drive or **Skydrive** to be the only one alternative **...**

- I thought “what the hell, I’ve got nothing better to do…”

Is this really news?



seaforthhuron expositor .com

Tuesday, April 2, 2013

Seaforth, ON

-3°

A few clouds

WEATHER SPONSORSHIP AVAILABLE!

HOME | NEWS | SPORTS | ENTERTAINMENT | LIFE | MONEY | OPINION | UR | MARKETPLACE | PHOTOS | VIDEOS | EVENTS | MORE

EVENTS COMMUNITY

'Forget Dropbox, Skydrive, Google Drive:」GET」 NOW TOP Cloud Storage Unlimited Free

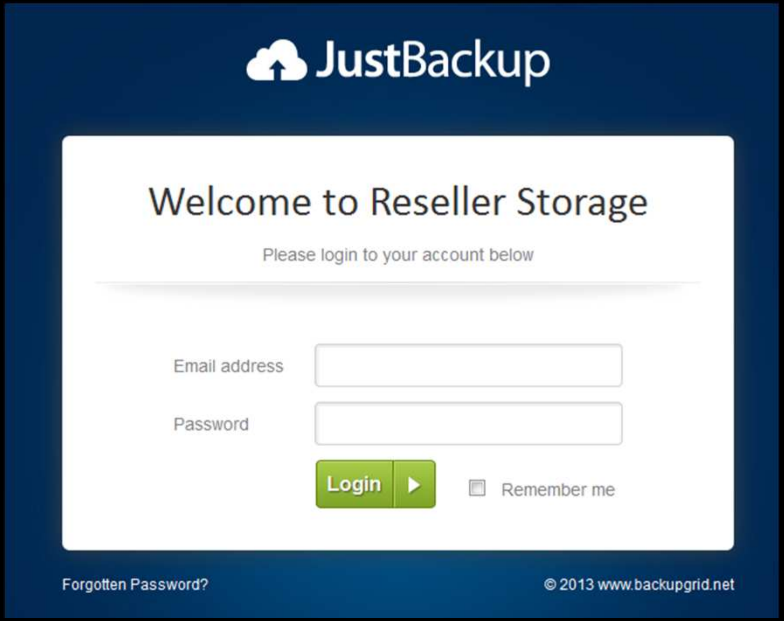
'When it comes to cloud storage, there are a whole bunch of fluffy options up there in the proverbial sky. Maybe you need unlimited storage, or maybe you need it for free and And if you still thinking Dropbox & Google Drive or Skydrive to be the only one alternative to online storage? then you must to 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

GeThe 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…



Welcome to Reseller Storage

Please login to your account below

Email address

Password

□ Remember me

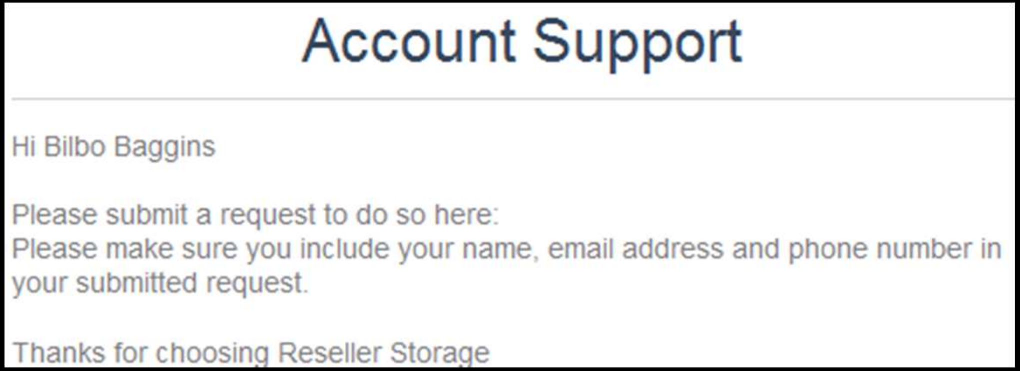
Forgotten Password?

© 2013 www.backupgrid.net

- But the login form is, you guessed it, HTTP

Cool, it let me log in

- Wait… I can log in with my JustCloud account?
- Ok, maybe I'll contact support about these issues



Account Support

Hi Bilbo Baggins

Please submit a request to do so here:
Please make sure you include your name, email address and phone number in your submitted request.

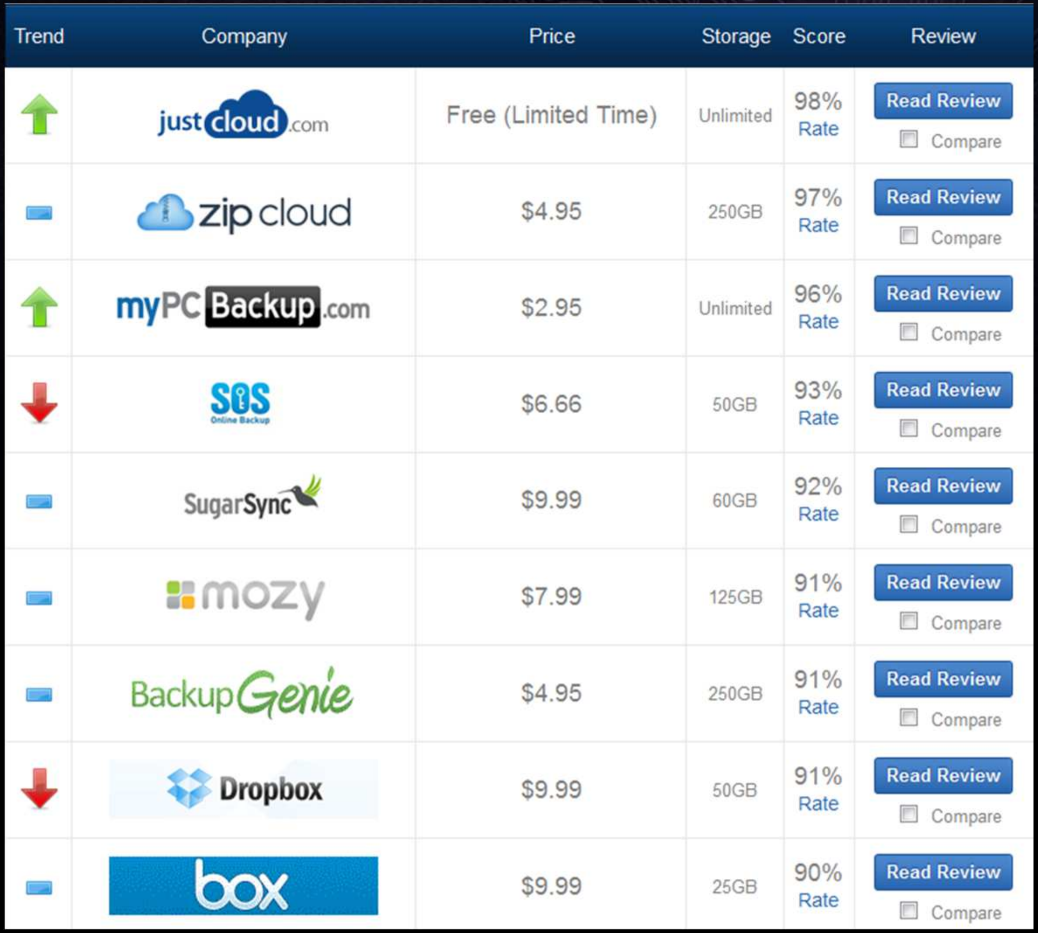
Thanks for choosing Reseller Storage

- 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!



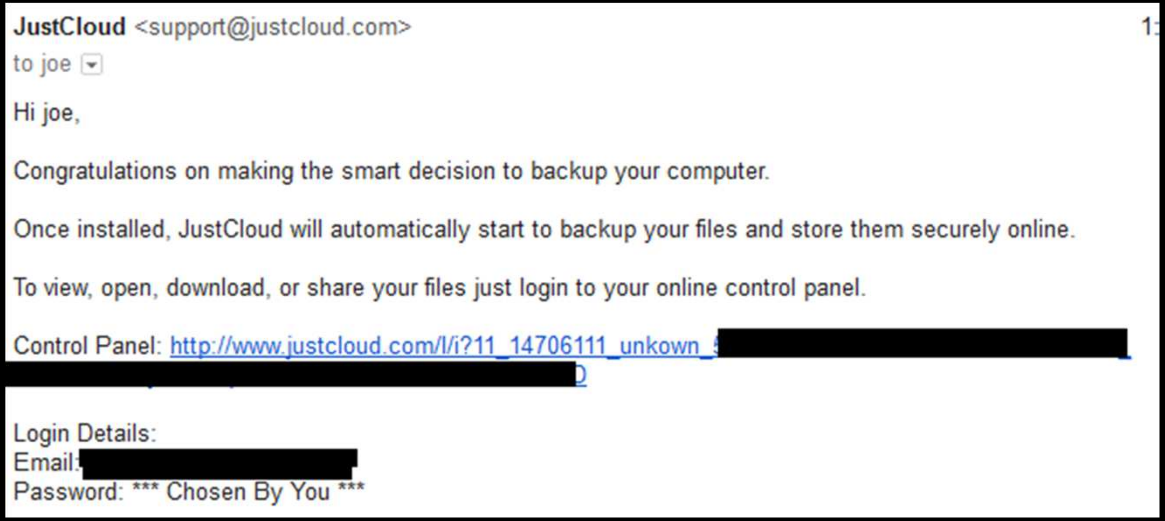
Trend	Company	Price	Storage	Score	Review
↑	justcloud.com	Free (Limited Time)	Unlimited	98% Rate	Read Review □ Compare
▬	zipcloud	$4.95	250GB	97% Rate	Read Review □ Compare
↑	myPCBackup.com	$2.95	Unlimited	96% Rate	Read Review □ Compare
↓	SOS Online Backup	$6.66	50GB	93% Rate	Read Review □ Compare
▬	SugarSync	$9.99	60GB	92% Rate	Read Review □ Compare
▬	mozy	$7.99	125GB	91% Rate	Read Review □ Compare
▬	BackupGenie	$4.95	250GB	91% Rate	Read Review □ Compare
↓	Dropbox	$9.99	50GB	91% Rate	Read Review □ Compare
▬	box	$9.99	25GB	90% Rate	Read Review □ Compare

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…



JustCloud <support@justcloud.com> 1:

to joe

Hi joe,

Congratulations on making the smart decision to backup your computer.

Once installed, JustCloud will automatically start to backup your files and store them securely online.

To view, open, download, or share your files just login to your online control panel.

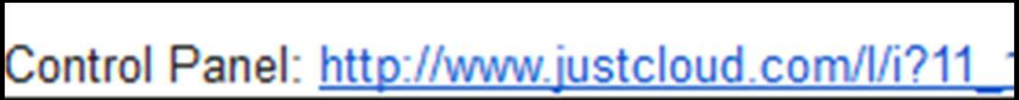
Control Panel: http://www.justcloud.com/l/i?11_14706111_unkown_[redacted]

Login Details:
Email:[redacted]
Password: *** Chosen By You ***

- Anything else stand out?

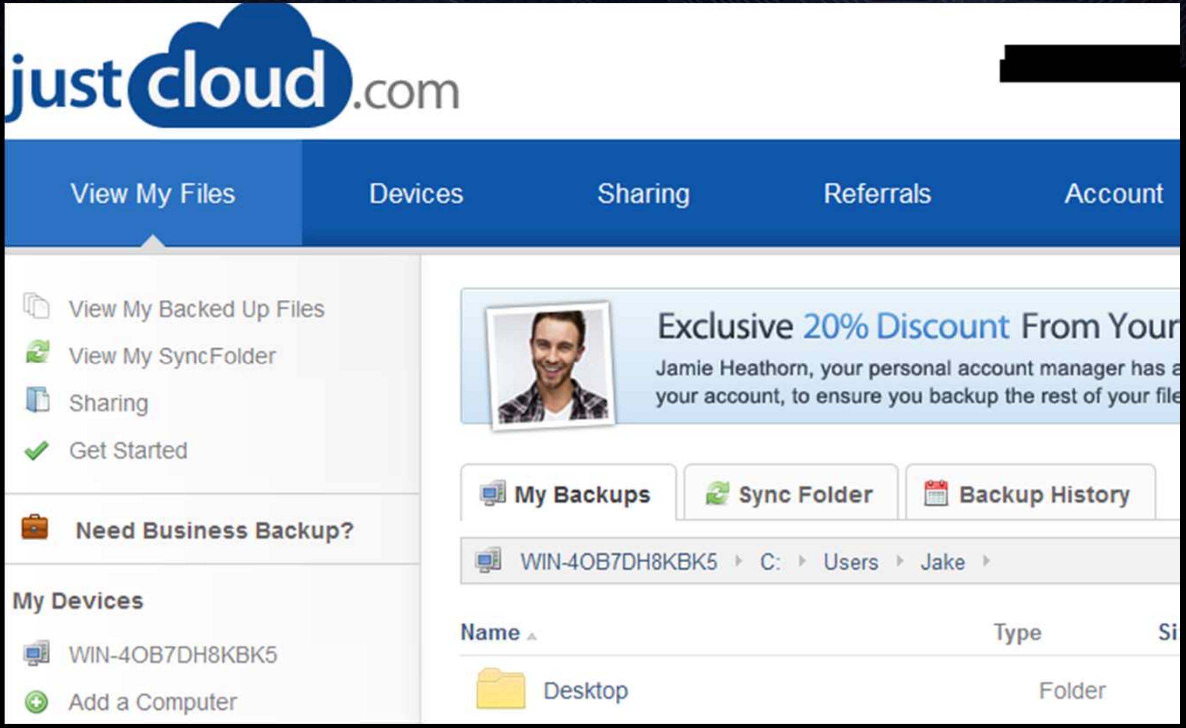
HTTP Again???

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



Control Panel: http://www.justcloud.com/l/i?11_

Free Beer!



justcloud.com [redacted]

Exclusive 20% Discount From Your

Jamie Heathorn, your personal account manager has a

your account, to ensure you backup the rest of your file

Name	Type	Si
Desktop	Folder	

- It actually logs you in!
  - Login link **never** expires, multiple use auth token

Wow. I’m speechless…

Anyone else?

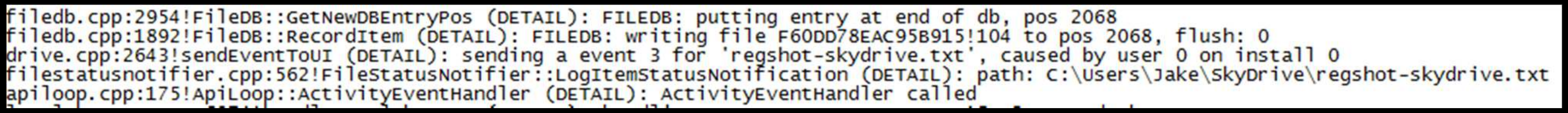
- We’re continuing to look at other applications and possible exploitation avenues they might provide
- Nobody else we’ve seen was close to this bad

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)

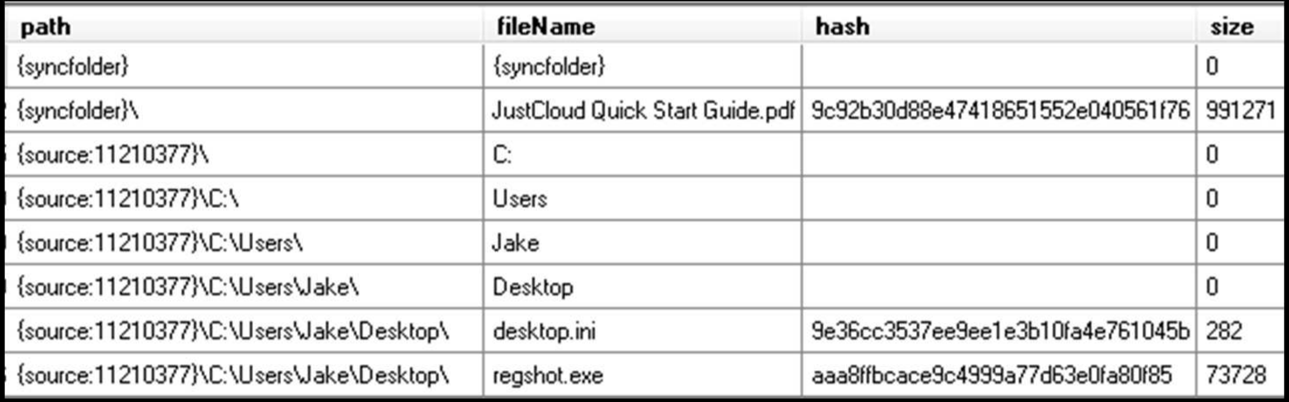
- Log files stored on the client often show information about files previously sent to the cloud (files may no longer exist locally)
  - Ex. SkyDrive device log



```
filedb.cpp:2954!FileDB::GetNewDBEntryPos (DETAIL): FILEDB: putting entry at end of db, pos 2068
filedb.cpp:1892!FileDB::RecordItem (DETAIL): FILEDB: writing file F60DD78EAC95B915!104 to pos 2068, flush: 0
drive.cpp:2643!sendEventToUI (DETAIL): sending a event 3 for 'regshot-skydrive.txt', caused by user 0 on install 0
filestatusnotifier.cpp:562!FileStatusNotifier::LogItemStatusNotification (DETAIL): path: C:\Users\Jake\SkyDrive\regshot-skydrive.txt
apiloop.cpp:175!ApiLoop::ActivityEventHandler (DETAIL): ActivityEventHandler called
```

General Post Exploitation (3)

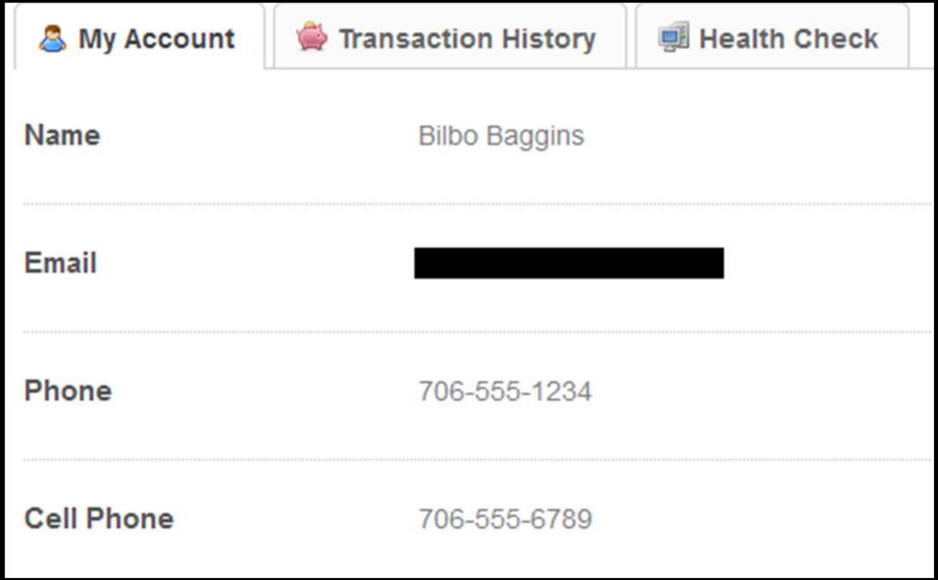
- Databases stored on the client often show valuable information about files previously sent to the cloud
  - Ex. JustCloud mpcb_file_cache.db



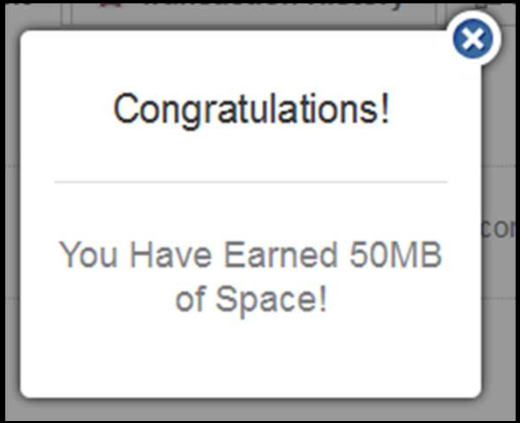
path	fileName	hash	size
{syncfolder}	{syncfolder}		0
{syncfolder}\	JustCloud Quick Start Guide.pdf	9c92b30d88e47418651552e040561f76	991271
{source:11210377}\	C:		0
{source:11210377}\C:\	Users		0
{source:11210377}\C:\Users\	Jake		0
{source:11210377}\C:\Users\Jake\	Desktop		0
{source:11210377}\C:\Users\Jake\Desktop\	desktop.ini	9e36cc3537ee9ee1e3b10fa4e761045b	282
{source:11210377}\C:\Users\Jake\Desktop\	regshot.exe	aaa8ffbcace9c4999a77d63e0fa80f85	73728

Post Exploitation (JustCloud)

- Users may be enticed to enter phone numbers for free add-on storage
  - – Phone numbers useful to social engineering or…



Name	Bilbo Baggins
Email	[redacted]
Phone	706-555-1234
Cell Phone	706-555-6789

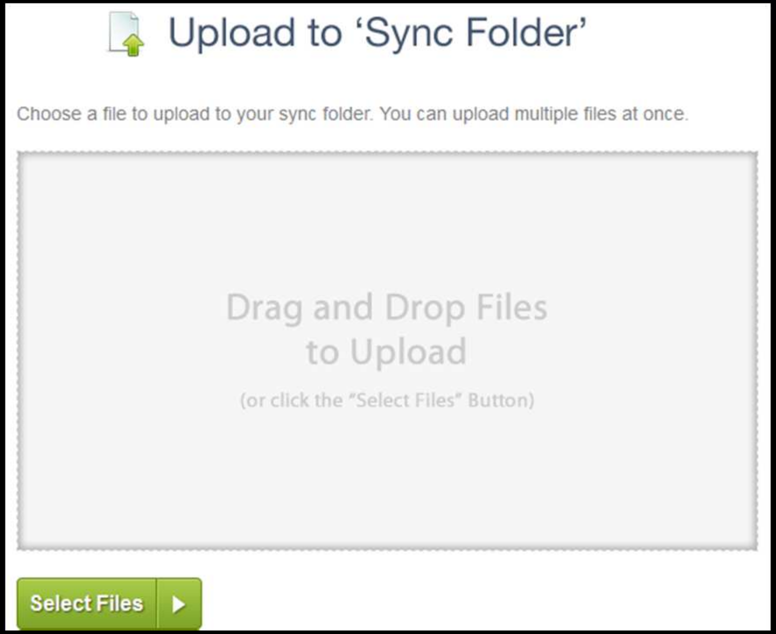


Congratulations!

You Have Earned 50MB of Space!

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!

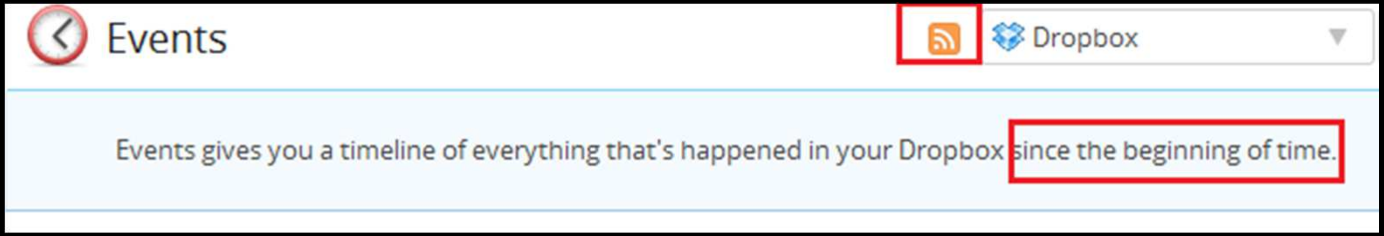


Upload to ‘Sync Folder’

Choose a file to upload to your sync folder. You can upload multiple files at once.

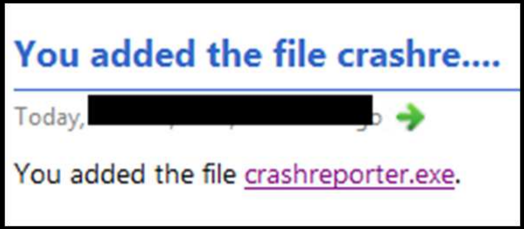
Post Exploitation (Dropbox)

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



Events gives you a timeline of everything that's happened in your Dropbox since the beginning of time.

- RSS Feed Example – at least you have to auth to get the file…



You added the file crashre....

Today, [redacted]

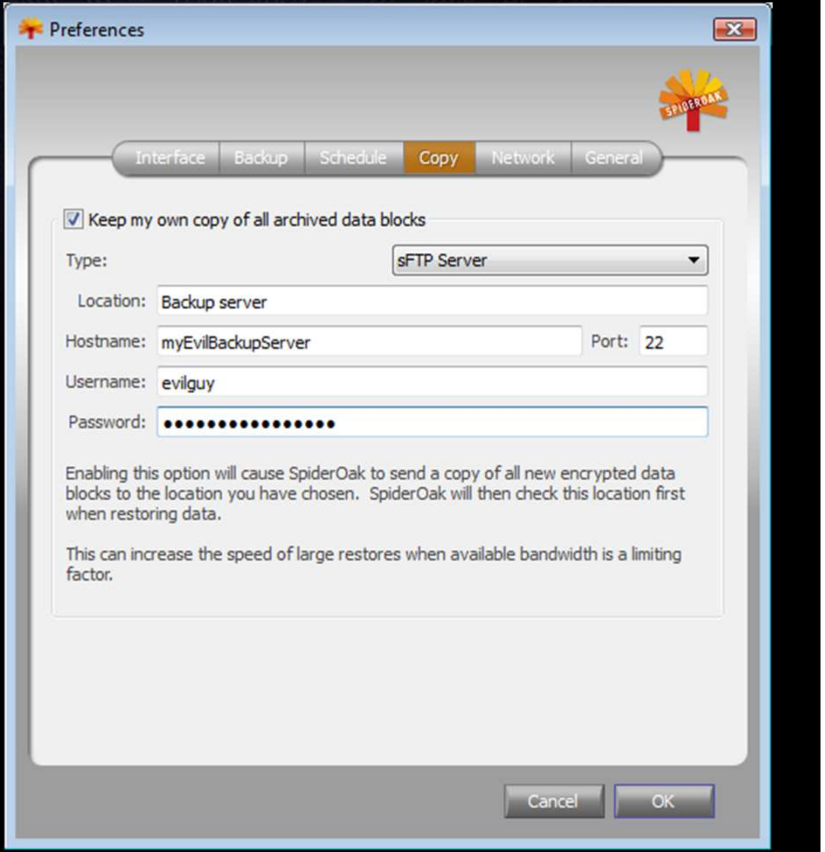
You added the file crashreporter.exe.

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 ☺



☑ Keep my own copy of all archived data blocks

Type: sFTP Server

Location: Backup server

Hostname: myEvilBackupServer Port: 22

Username: evilguy

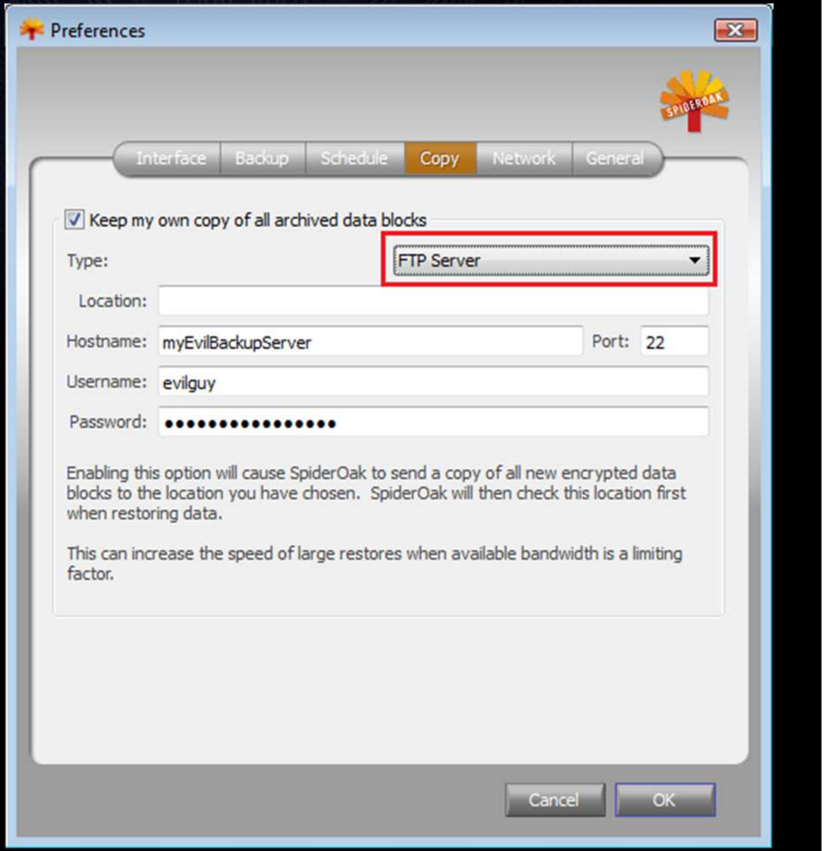
Password: ●●●●●●●●●●●●●●●●●

Enabling this option will cause SpiderOak to send a copy of all new encrypted data blocks to the location you have chosen. SpiderOak will then check this location first when restoring data.

This can increase the speed of large restores when available bandwidth is a limiting factor.

Post Exploitation (SpiderOak)

- But then I noticed that FTP is allowed!
  - Start FTP server
  - Change config
  - Put files in sync folder
  - Capture creds
  - Profit!



☑ Keep my own copy of all archived data blocks

Type: FTP Server

Location:

Hostname: myEvilBackupServer Port: 22

Username: evilguy

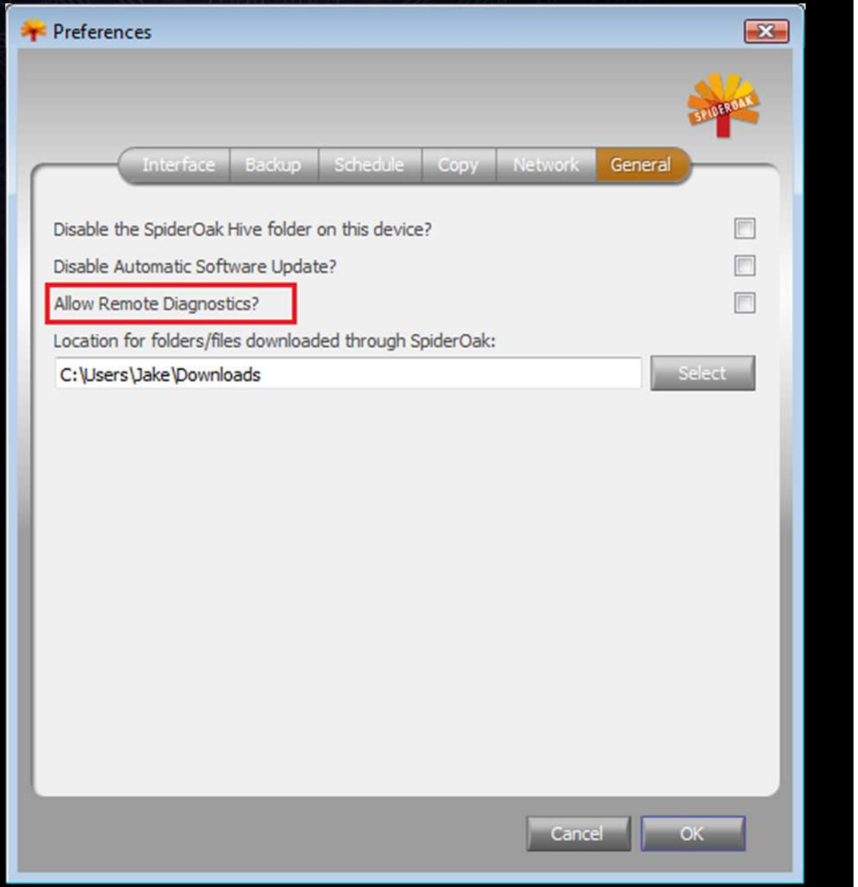
Password: ●●●●●●●●●●●●●●●●

Enabling this option will cause SpiderOak to send a copy of all new encrypted data blocks to the location you have chosen. SpiderOak will then check this location first when restoring data.

This can increase the speed of large restores when available bandwidth is a limiting factor.

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™



Disable the SpiderOak Hive folder on this device? □

Disable Automatic Software Update? □

Allow Remote Diagnostics? □

Location for folders/files downloaded through SpiderOak:

C:\Users\Jake\Downloads

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

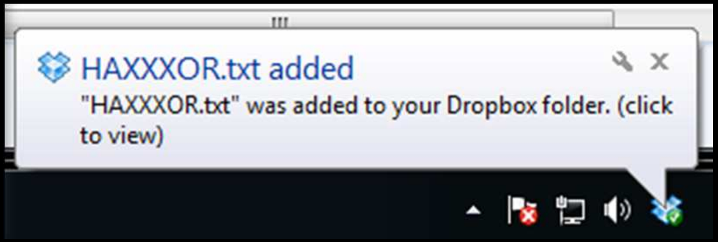
- Look for tasking files on the end hosts
- Employ an NGFW and watch for sensitive data leaving the network
  - This presumes some exfil to detect
- Watch your process lists
  - This shouldn't be news
- For the love of security, start whitelisting
  - Not a silver bullet, but makes my job much harder

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



HAXXXOR.txt added

"HAXXXOR.txt" was added to your Dropbox folder. (click to view)

Moar Demos

- Time permitting of course

Thank You!

Please complete your speaker feedback surveys

@MalwareJake
jwilliams@csr-group.com