CSRgroup
computer security consultants

DropSmack: How cloud synchronization services render your corporate firewall worthless

Jake Williams
jwilliams@csr-group.com

CSRgroup
computer security consultants

Feedback Surveys

- Please complete the Speaker Feedback Surveys.
- This will help speakers to improve and for Black Hat to make better decisions regarding content and presenters for future events.

CSRgroup
computer security consultants

Why should you trust me?

- Why should you trust me?
  - More than a decade of work in systems engineering, network defense, malware reverse engineering, penetration testing and forensics
  - Conducing PhD level research in new techniques for botnet detection
  - Two time winner of the DC3 Forensics challenge
  - Developed a course on Cloud Forensics for a client
    - So I've had a LOT of time to research this
  - Blah, blah, blah…
    - Cut the crap, show me the hack!

CSRgroup
computer security consultants

What's this about anyway?

- In case you might be in the wrong room…
  - Security of Cloud Synchronization services (Dropbox)
  - How to use Dropbox to own a protected corporate network while completely bypassing network defenses
  - How to use DropSmack malware to establish C2 and data exfiltration over Dropbox
  - How to stop someone from doing it to you
- Dan Kaminsky is (probably) speaking somewhere else…

Giant Honking Disclaimer

- We pick on Dropbox in this research
  - And our proof of concept implant uses Dropbox
- Dropbox provides a command and control (C2) channel ***by design***
- **Mad props** to Dropbox developers
  - They **set the standard** in client side security among the products we tested
  - Anything we demo with Dropbox can be done **more easily** to most other products
- We are **not** releasing zero-day attacks here
  - The media will spin it that way though…

CSRgroup
computer security consultants

Cloud Synchronization

- Implies more than just online backup
- Files placed in a folder on one participating machine are synchronized to all machines
  - Via the cloud
- Infecting files destined for a backup site would be interesting too
  - We can't get C2 from that
    - But there's nothing like repeat infections from a single attack ☺

History of Insecurity

- Dropbox authentication horribly broken (2011)
  - More on this later
- Dropbox ‘no password day’ (2011)
- Dropbox Mobile file metadata in the clear (2011)

- Why aren’t other products up here?
  - Nobody was looking at the lower tier providers
  - Don’t worry, we are now…
    - Stay tuned for more fun!

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

CSRgroup
computer security consultants

A Little Case Study

- Our client, Massive Dynamic, requests a no holds barred penetration test
  - Act like APT they said
    - No problem, got that covered
  - Long engagement time
  - Completely black box

CSRgroup
computer security consultants

Standard Methods Fail

- Web portals
  - No go
- Outdated patches on public facing services
  - No go
- Social engineering
  - Gets some basic IT info
  - Campaign cut short by astute employees who inform security of the attempted trickery

CSRgroup
computer security consultants

Standard Methods Fail (2)

- Physical security is military grade
  - And guys with big guns scare us…

This guy looks **WAY** too jumpy to try any physical pen testing approaches

His thousand yard stare is a little disconcerting…

CSRgroup
computer security consultants

Standard Methods Fail (3)

- Spam fails too
- We get some quick hits back to our BeEF server
  - Some users are even running slightly older browsers
    - But we never are able to establish any real C2 channel
    - It's like something in the network is cutting out connections to our server
- Continue spamming campaign
  - In case we get lucky
- Time for Plan B

Plan B

- No, not ***THAT*** PlanB!
  - $25 and a college campus vending machine aren't getting us out of ***this*** mess…

CSRgroup
computer security consultants

Social Network Analysis

- We find this guy's personal email address

- He's the CIO
- Facebook tells us he helps organize fundraising for his kid's PTA
  - Nothing like exploiting children to p0wn a target

CSRgroup
computer security consultants

Spam @ Home

- We email him some fundraising information at home and win
  - Own the laptop
- Looking for VPN software on the laptop
  - FAIL!
- Confidential corporate documents on the laptop
  - Check
- WTF? These documents aren't really moving by email or USB drive are they?

CSRgroup
computer security consultants

Dropbox…

- We notice that all of the company documents are in the Dropbox folder
  - And Dropbox.exe is in the process list
  - Now we're getting somewhere…
- Pull Dropbox databases to see what we can see
- Databases are encrypted
  - Fail
- Could reverse engineer the Dropbox software to read the databases
  - But…

CSRgroup
computer security consultants

Ain’t nobody got time for that!

CSRgroup
computer security consultants

Where are we?

- What we have so far
  - A way to send files over Dropbox to devices the CIO uses
- What we want
  - A running implant (with command and control) in the corporate network

CSRgroup
computer security consultants

Time to brainstorm

- This will require lots of beer….

CSRgroup
computer security consultants

Time to brainstorm…

- No, I said **LOTS** of beer!

- That's more like it

CSRgroup
computer security consultants

Brainstorming complete

- With a blood alcohol level of .12 and a dose of inspiration, it hits me
- Dropbox can be used to infect the internal network **AND** be our C2 channel
  - If the CIO has Dropbox installed on his corporate machine (behind the firewall)
  - Since we have confidential corporate docs in the Dropbox folder, lets work from that assumption

CSRgroup
computer security consultants

First, we'll need new malware

- We could just deliver a standalone meterpreter
- But nothing else we delivered has been able to call out of the network
- We need malware that can use the Dropbox file synch service instead of traditional network based C2
  - Kind of like a dead drop

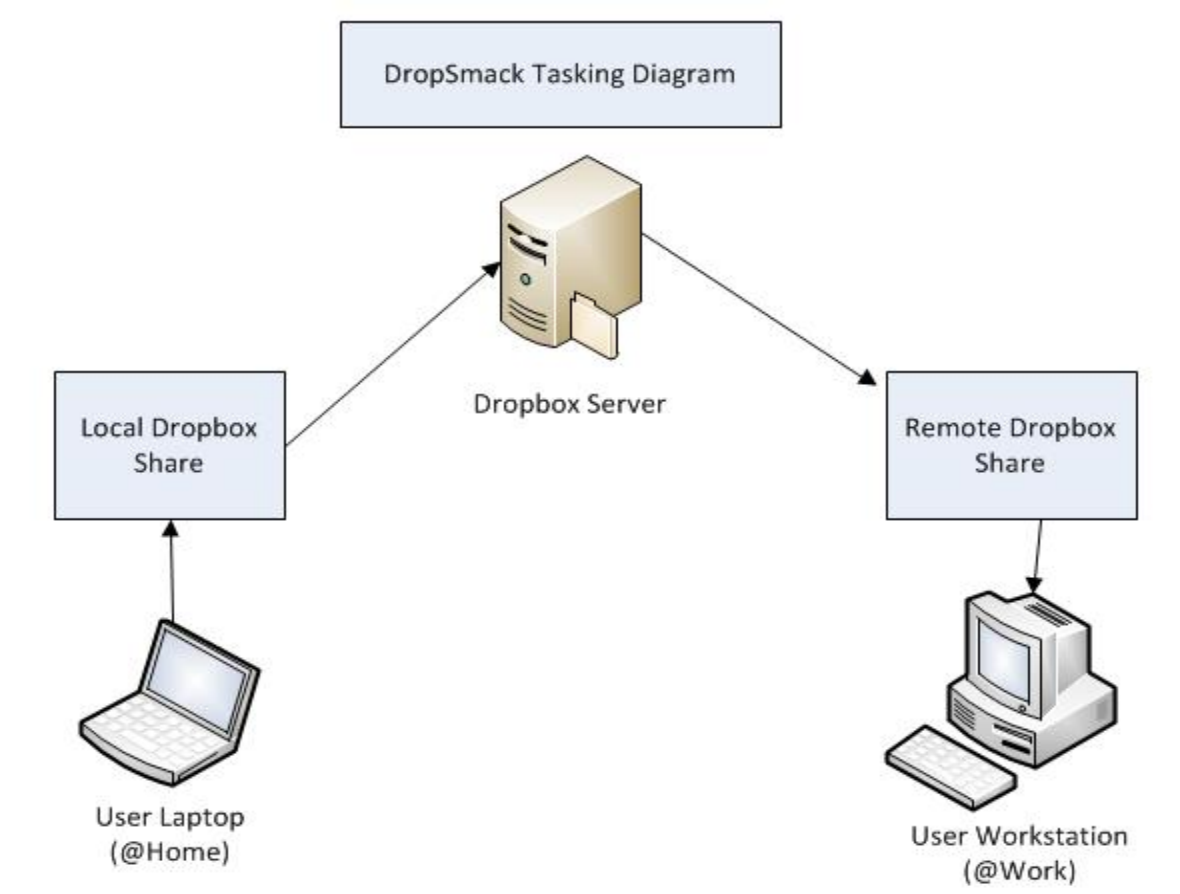
    *Pun **definitely** intended

DropSmack FTW

- So DropSmack was born
- DropSmack is new proof of concept malware designed to use files synchronized by Dropbox for C2
  - Guess what? This isn't fast
- Data exfiltration and command output are also sent via Dropbox synchronization
  - Not surprisingly exfil isn't fast either
    - Thanks to a recent Dropbox change, it's a lot faster
    - Thanks Dropbox development team!

DropSmack Comms

- For the benefit of those that prefer a picture…



CSRgroup
computer security consultants

DropSmack for long term use?

- 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 gravy
    - Yummm, gravy…

CSRgroup
computer security consultants

Deploying DropSmack

- We can't do everything for you
- General steps (suggested):
  - Embed DropSmack in a file the victim has already sync'd
  - Add some macro goodness
  - Load file back to the machine you can access
  - File automatically synchronizes
- Now all you have to do is wait for the victim to open the file on the internal network
  - But…

CSRgroup
computer security consultants

Ain’t nobody got time for that!

CSRgroup
computer security consultants

Social Engineering (redux)

- Social engineering is much more likely to be successful when you have lots of background information
- Remember:
  1. You know the file contents
  2. The victim thinks **they** created the file
- It doesn't get much easier than that…
  - If you *can't* convince the subject to open the file, get out of the business!

CSRgroup
computer security consultants

DropSmack Demo

- Play video here….

CSRgroup
computer security consultants

Detecting this Tom Foolery

- IDS
  - Worthless
- Firewall
  - Mostly worthless*
- Antivirus
  - Do I really need to say it?
- DLP Software
  - Worthless too
    - But for a whole lot more than just this…
- Whitelisting Software
  - Won't let the new application (DropSmack) execute

CSRgroup
computer security consultants

Next Generation Firewalls (NGFW)

- I can hear the CISO now:
  - "Certainly the shiny new next generation firewall will save us from this horror"
    - Sort of.
- In a 2012, more than 75% of respondents using NGFWs said that their workloads increased due to the installation of the firewall
  - This sounds like IDS in the 90's
- Still a black and white decision on whether to allow Dropbox
  - Can't surgically filter content with an NGFW

Do you allow synch software?

- All of the detection methods we'll cover focus on finding ***illicit*** synchronization software installations
- Remember, this channel exists ***by design***
- If you allow the software, you are implicitly allowing the covert channel with it

Detection strategies that mostly suck

- Dropbox uses LanSync
  - TCP and UDP port 17500
- Look for DNS requests to servers related to synchronization services
  - Let me know how this works
- Block access to Amazon S3 (Dropbox back-end)
  - This isn't really feasible, breaks other stuff
- Scan user profile directories for illicit synchronization software installations
  - Remember, these programs install into user profiles so no UAC

CSRgroup
computer security consultants

Better detection strategies?

- In short, no
- Again, you take the vulnerability with the convenience

- Time to talk to management and find out what the policy on these services really should be

CSRgroup
computer security consultants

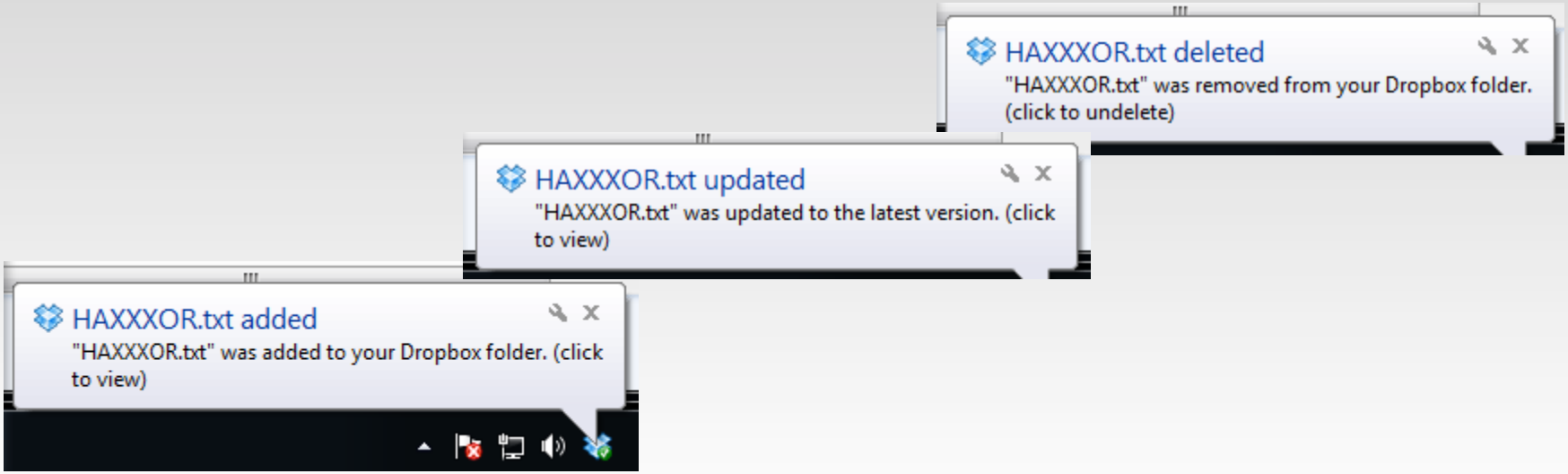
Future work

- Need to be able to read and extract information from Dropbox configs
  - Those damn encrypted databases again…
- DropSmack currently assumes a default synchronization folder location
  - Changing the default breaks this version of DropSmack

CSRgroup
computer security consultants

Future work (2)

- Dropbox issues popup notifications when new files are added, deleted, or changed remotely
  - Users probably appreciate this
  - I don't
- Need to adopt strategies to get rid of these popups since we create a lot of them



Future work (3)

- Build proof of concept malware that uses other synchronization services
  - Dropbox users shouldn't have all the pain
- Most other services we've looked at don't use encrypted databases
  - Takes away all the challenges we have with Dropbox
- Note to vendors: **Encrypt your databases**
  - It makes my job much harder

CSRgroup
computer security consultants

Future work (4)

- Extract login information for web front ends from client side databases
  - This would allow us to take the laptop out of the loop after the initial compromise
  - Or entirely if we got credentials some other way
- This is an active research area for us

CSRgroup
computer security consultants

Conclusion

- DropSmack isn't rocket science
  - Almost anyone could have written it
  - If you are a pen tester who finds this useful, glad I could be of help
- The real point is to demonstrate the vulnerability that file synchronization applications represent
  - If you are comfortable with the vulnerability, fine
  - This started out as a project to help our clients make an informed decision about risk

CSRgroup
computer security consultants

Feedback Surveys

- Please complete the Speaker Feedback Surveys.
- This will help speakers to improve and for Black Hat to make better decisions regarding content and presenters for future events.

Questions?

Thanks for your time and attention

I'm happy to answer any questions you may have

Jake Williams
jwilliams@csr-group.com