Malware in the clouds

Building the Undetectable Bot

Who am I?

- Philip Porter
- “nullbnx” – twitter
- nullbnx@bnxnet.com
- Ex-Intel Analyst, Reverse Engineer/Forensic Analyst, studier of advanced threats, Red Teamer, etc. etc.

Two Conflicting Thoughts

- ? 1. What would some really advanced malware C2 look like?
- ? 2. Why can’t I get to Evernote/Dropbox/cloud storage on this network?
- Two separate thoughts that happened at just the right time…

Starting with Malware c2

- Malware C2 has hardly evolved over the previous ~5 years
- Started with a simple web request (for content or direct c2)
  - Recently has moved to more SSL
  - Harder to intercept but just as easy to block
- Hasn’t been any “drastic” evolutions to the hopes of the “blend into the noise” approach

Diving deeper into C2

- Lead to a few new questions…
- Has there been any cases of groundbreaking malware C2?
- If so, what does it look like?

Advanced Malware C2 Examples

- Gmail C2 – cool, but Google is smart
- VPN (PPTP) – hassle, unusual network activity
- Pastebin – cool but not a ton of real feasibility
- VOIP – Defcon talk, cool, but not feasible
- Myspace/Twitter – fun, l33t
- DNS – tricky, but only if you have time
- IPV6 – super hard to detect… unless it's off

Summary of current ADV C2

- Most are complicated
- Some have big problems with being stopped at the service level (accounts disabled, etc)
- Others have problems with complexities (bandwidth??)
- Most have problem of being detected as a network abnormality

There's an easier way!

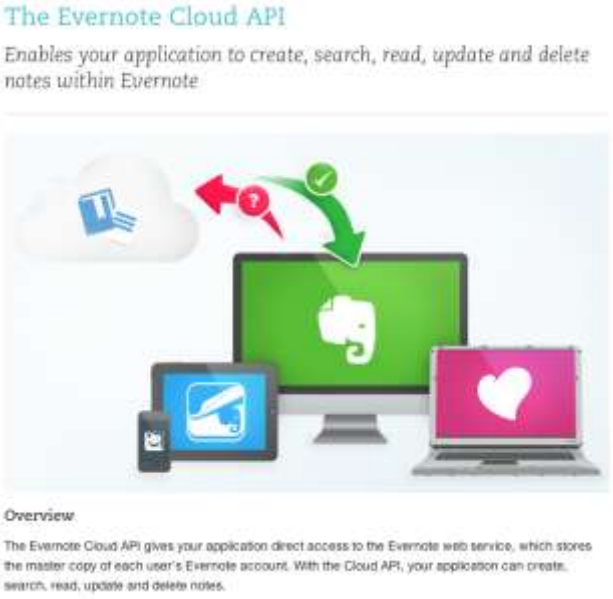
- Remember question 2?
  - "Why can't I get to Evernote/Dropbox/cloud storage on this network?" (real reason was insider threat ☺)
- Find something commonly used on network…
  - Don't want to stand out as an abnormality on the network
- Easy to setup (doesn't require software engineers to build)

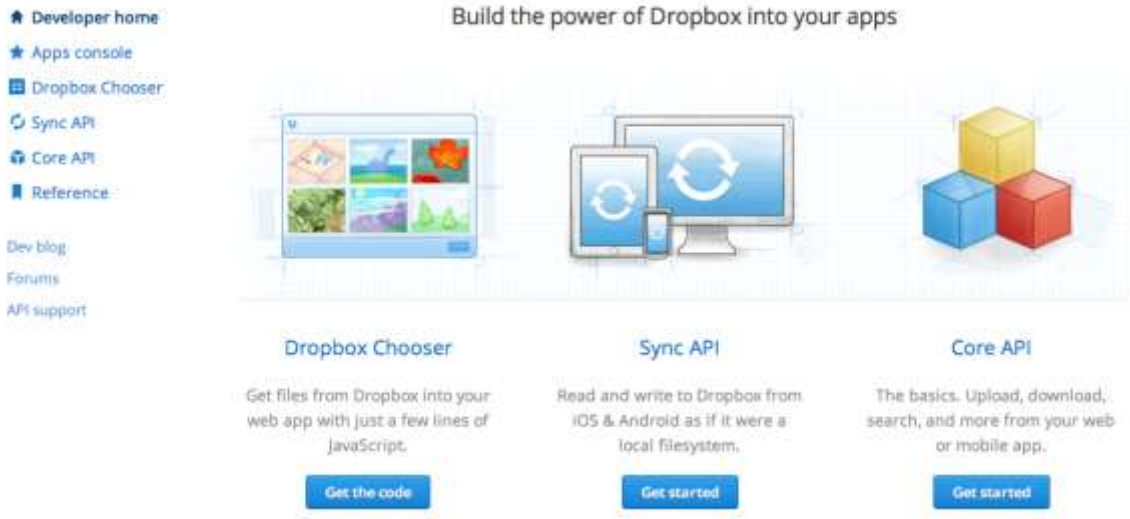
Look to the cloud(s)!

- Most use SSL / Oauth
- Almost all are based on storage of information (in some regards) – good for C2
- Almost every network allows access to them! (mine didn't for insider threat, NOT malware threat) – better for C2
- Can't easily filter good from bad!! – best for C2

Deeper look at the cloud(s)

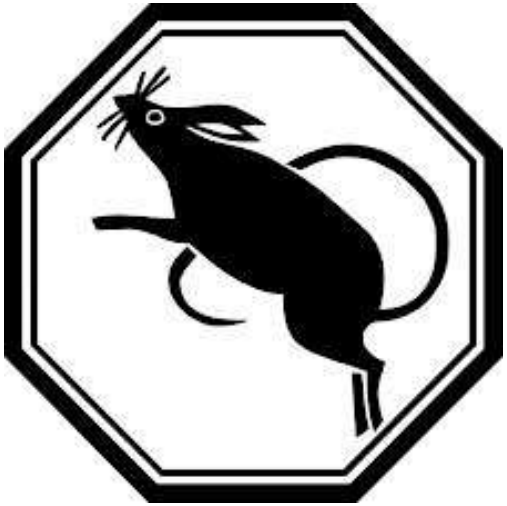
- Cloud based APIs are easy (and powerful) to setup :)
- Most use SSL / Oauth
- Examples : Dropbox, Evernote





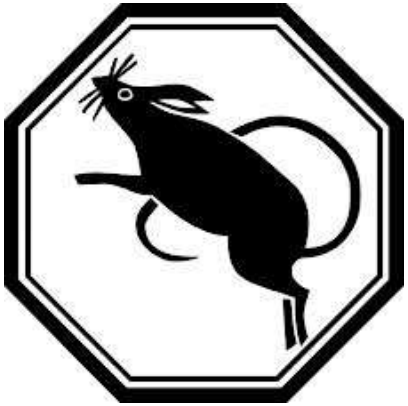
Straight from the cloud… EverRAT

- Let's call this a remote admin tool (for legal reasons of course)
- Maybe citrix can find a use? :)
- Nice iPhone/Android controlled RAT!



It’s not about EverRAT… There’s more to be had!

- Really this talk isn’t about EverRat
  - I put work into the RAT but there could be much more
- It’s really a talk to make you aware and maybe…
  - MSF with Dropbox/Evernote/cloud C2? ☺
  - Shellcode with Dropbox/Evernote/cloud?



Lets take a look

- **Demo time!**
- Multiple hosts call back…
- Easy to manage interface.. oh yeah, it's the evernote client! :)
- Mange from iphone/android… ;)

Can we be stopped?

- Traffic doesn't look any different then normal evernote (as long as we don't create a crazy callback times)
- No crazy domains
- Still need host level evasion like anything else
- Good part about python :)
- Also works on any OS, just need to be mindful of sending out global commands
- Needs some things to make it more stealthy then just an executable
- Saw the talk by X online after writing this in Python, C# wouldn't be a bad idea

Security issues with allowing Dropbox installations on client PC's in our organisation

7

2

Does anyone know if there is any good reasons not to allow Dropbox installations on our client PC's? All the PC's have antivirus installed and running. I know it is an additional attack vector to spreading files, but the kind of risk I am specific worried about is automatic spreading due to synchronization of files.

Can potential virus on the dropbox spread easier once the file is in the cloud as it potentially could be synchronized to our client, and then automatically spread? Is there any security mechanisms to prevent this kind of spreading?

I am not taking into consideration that files may be infected when the user opens them. These kinds of risks are already considered in all the other applications that allow file sharing (email, USB dongles and so on).

The kind of risk I am specific worried about is automatic spreading due to synchronization of files.

malware known-vulnerabilities virus

share improve this question

edited Aug 14 '11 at 19:36

AviD ♦
17.9k 3 44 101

asked Aug 12 '11 at 12:15

Chris Andrè Dale
8,750 5 21 55

As long dropbox isn't hacked it can be categorized as safe(kinda). But as soon that happens and you have dropbox installed on your computer its a trojan. Whats the first thing firewall asks when drop box is installed? Drop box on your pc is an actual trojan, just waiting for someone to exploit it. – user10956 Jun 29 '12 at 15:53

@Filter, I disagree with labeling dropbox a trojan. Any application with the ability to send/receive data and save data to your computer would be a trojan by that def. Yes, if an attacker got on to dropbox's servers they could and insert malware/viruses onto your computers (though until you manually chose to execute those files or open in an application with vulnerabilities to those files you wouldn't be at any risk). But you shouldn't store executables on dropbox. Using dropbox with say plaintext files (or simple encrypted) files and opening in simple editors presents minimal risk. – dr jimbob Jun 29 '12 at 21:11

Welcome!

This is a collaboratively edited question and answer site for **IT security professionals**. It's 100% free, no registration required.

Got a question about the site itself? meta is the place to talk about things like what questions are appropriate, what tags we should use, etc.

about » faq » meta »

tagged

malware × 214

virus × 132

known-vulnerabilities × 121

asked **1 year ago**
viewed **5685 times**
active **8 months ago**

Community Bulletin

meta which site to locate career question

meta How/Do you reference your work here on LinkedIn?

Tags: business, cloud, Evernote
Topic: Security

Answer this Question

Share this question Login or register to post answers Permalink

Know someone who knows the answer? Send this question to a friend!

Answers 2 total

Filter by:

jimlynch 35 weeks ago

I'd suggest allowing it, but with defined rules as to its use. You should specify which types of data related to your business that it should not be used for, and you should let users know that if they violate your clearly spelled out policies then you may remove access to the application at any time. Vote Up (7)

Share this answer | Permalink

kreiley 35 weeks ago

We allow Evernote, but not Dropbox. I'm not sure how that is a coherent security regime, but there you go. Basically, so many of us use Evernote as a productivity tool that while we accept that there is some risk of proprietary information being compromised, but find the level acceptable. Let's face it, most people aren't using Evernote to save the quarterly report that they are working on, they use it to remind themselves to talk to Bob (or whoever) about the quarterly report at 9:30 the next morning. If I worked at a hospital or the White House or something, I might feel differently, but the world of injection molded plastics just isn't as sensitive. It is just glamourous. Vote Up (8)

Share this answer | Permalink

Answer this Question

How close to perfection?

- These services can deactivate you if they were looking for something like this
- Can still migrate to another account
- Not super tiny (python, not c)
- Didn't design it for a nation state to use on a large scale, just to illustrate the point and give pentesters something else to use

Where to go from here?

- Well you can take this as far as you want
- It's smart to use this as a primary C2 (never exposes your other callbacks)
- Use this to bring other tools, or have them staged
- And then this happened….
  - thanks trend micro & china :/

The future

- As a mostly defense community we need to start watching for this
- If the network is whitelisted with dropbox or evernote or...
- There has been talks that the adversary is already using Dropbox
- Wasn't able to find a good write up/sample
- Things could get much harder from here…
- Cost vs Benefit

Wrap up

- Check out bnxnet.com for more info
  - I'll have my blog posting online right after the talk
- The code isn't the best, feel free to take it further! :)