DRIDEX, LOCKY AND CRIMINAL TRANSITIONING

someBrit@SANSDFIRsummit ~$ whoami

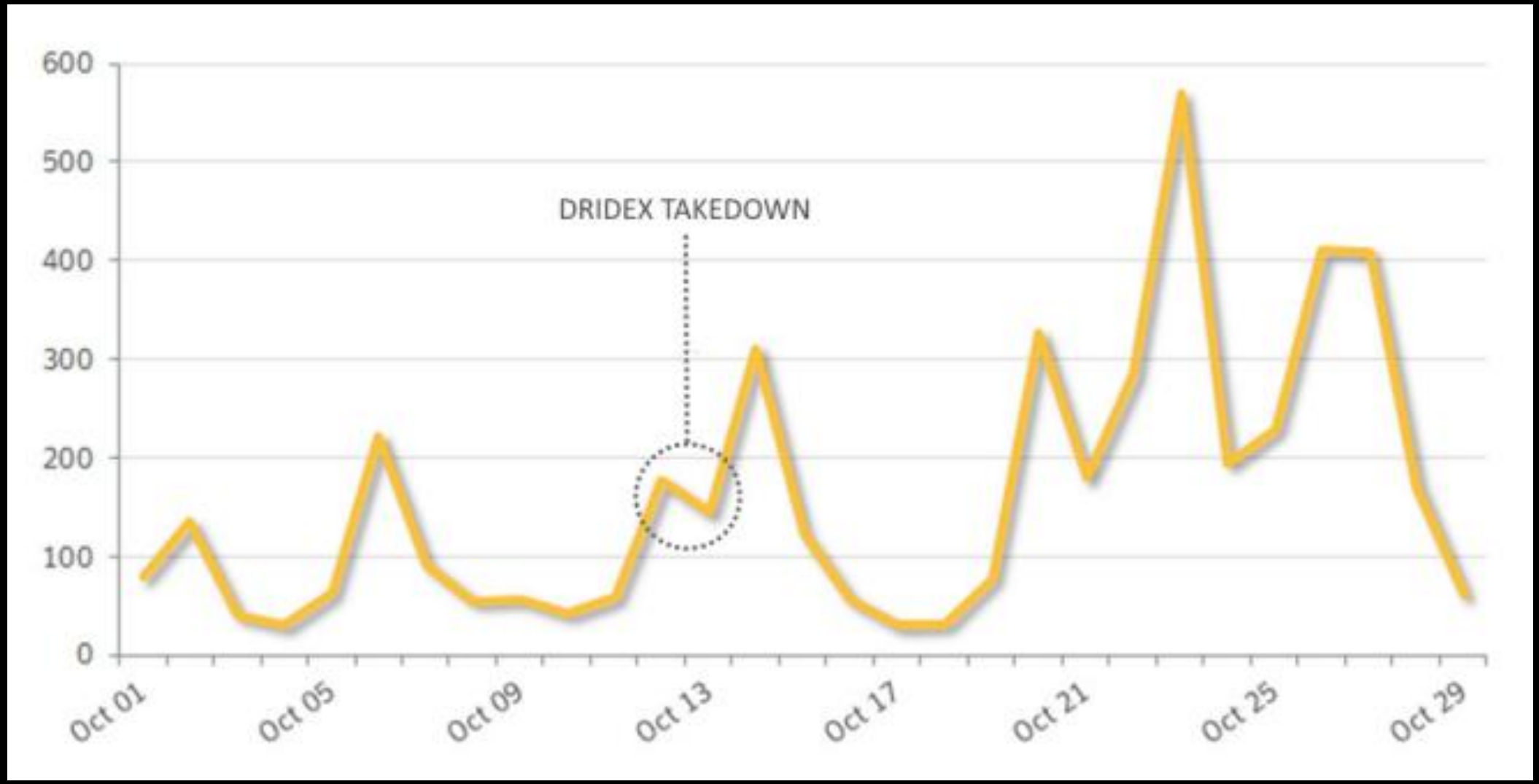
- Twitter > @sudosev
- Security Operations Analyst Intern
- Amateur malware hunter & analyst
- Forever a blue teamer!
- Sometimes I try to red team things.
- Student
  - Computer & Network Security @ Staffordshire University, UK.
- I play video games
  - Mostly Steam games
    - To collect Malware that is randomly sent to me in poor phishing attempts
      - Knife.jpg.exe hmm.

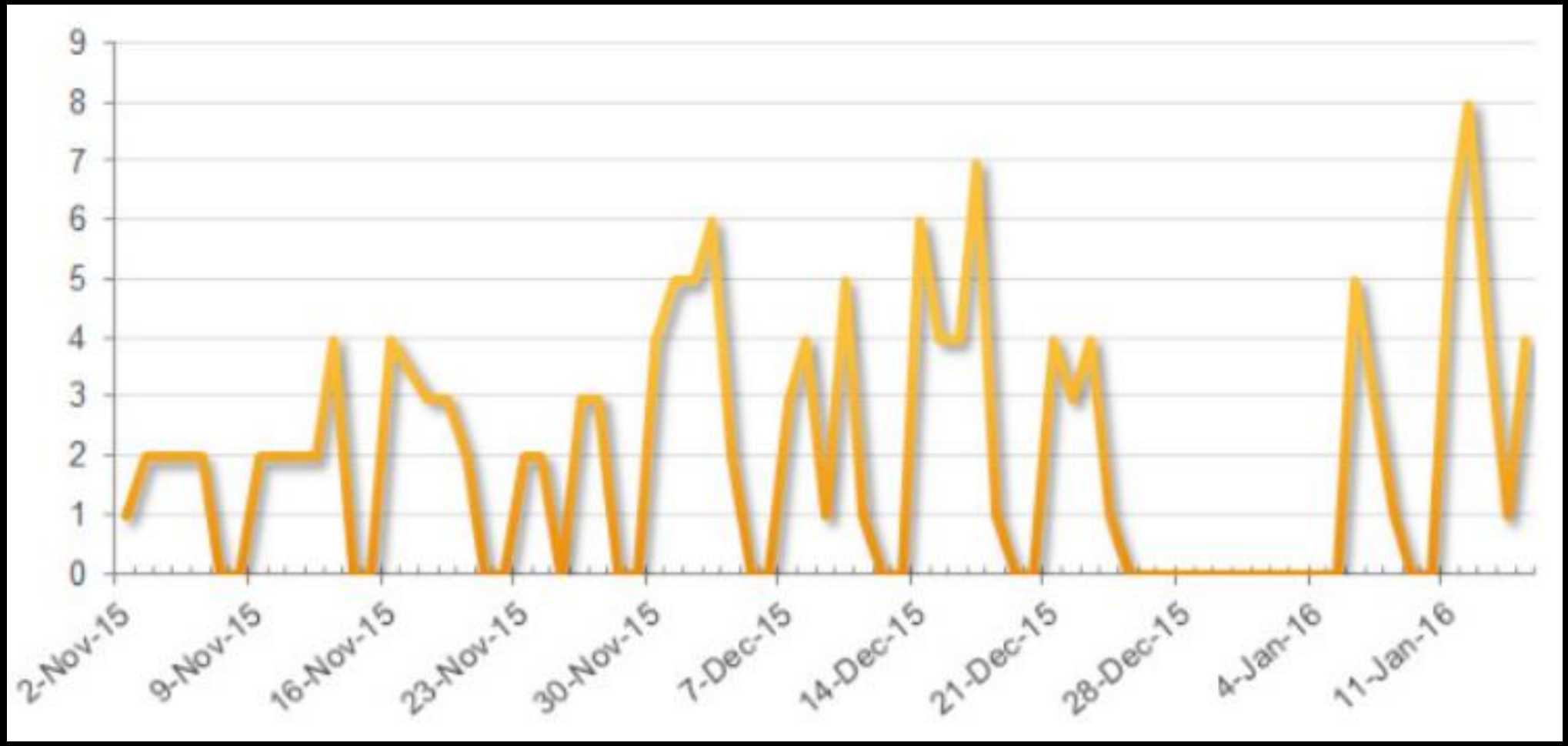
Why are we here again?

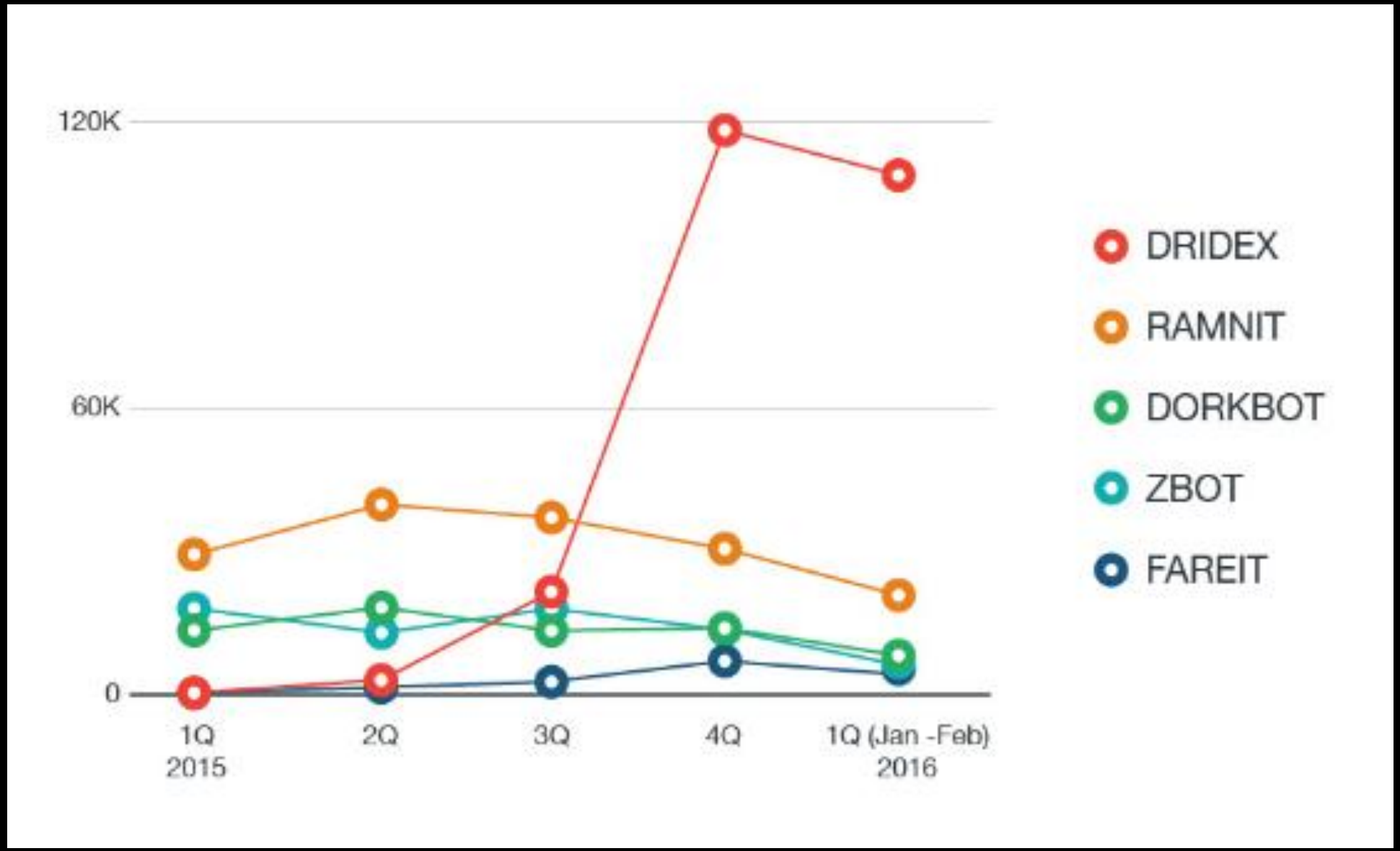
- What is Dridex?
- How does it operate?
- What about their distribution infrastructure?
- What's a Locky?
- How scary is the future, Sev?
- To look at kittens.

Dridex

- Around since November 2014
- Evolution of malware families such as Bugat, Geodo, Feodo, Cridex
- Complex network infrastructure
- Somebody put effort into the development of Dridex
- Target: Everybody
- Over $50m stolen from the UK alone in under a year
- Over $100m globally


600
500
400
300
200
100
0
DRIDEX TAKEDOWN
Oct 01
Oct 05
Oct 09
Oct 13
Oct 17
Oct 21
Oct 25
Oct 29


9
8
7
6
5
4
3
2
1
0
2-Nov-15
9-Nov-15
16-Nov-15
23-Nov-15
30-Nov-15
7-Dec-15
14-Dec-15
21-Dec-15
28-Dec-15
4-Jan-16
11-Jan-16


120K
60K
0
1Q
2015
2Q
3Q
4Q
1Q (Jan -Feb)
2016
DRIDEX
RAMNIT
DORKBOT
ZBOT
FAREIT

Dridex 1 – Sev 0

Dridex BOT @DridexBOT · 10 Dec 2015
@sudosev Hi man, i like you ;-)
1 3

Dridex BOT @DridexBOT · 10 Dec 2015
Hello world! ;-)
6

Back to top ↑

Abuse Department 2015-12-02 12:12:01

Dear Customer,

This abuse ticket requires your immediate attention. Please correct the matter and reply to this ticket with resolution within the next 48 hours to ensure uninterrupted service. Overwhelming evidence of violation/compromise may result in VPS suspension prior to the 48 hour deadline to protect system and additional customer resources.

-- Complaint Response Team --

2015-12-02 12:03:26

Abuse Team,
A malware email campaign directs to an IP address and port on your network for Command & Control (C2). Please take appropriate action to investigate and remediate any malicious files.
IP:port contacted by malware file:
104.238.174.49:443
Malware appears to be:
Dridex
Thank you for your immediate attention and action. Please contact us as soon as you receive this and stay in contact until the issue has been resolved.
Regards,

Abuse Team

P Please - consider the environment before printing this e-mail.

Dridex 1 – Sev 1

1/67	2016-04-07 17:17:25	https://45.127.92.175:8143/sudosev
1/67	2016-02-18 15:06:22	http://45.127.92.175:8143/sudosev
1/66	2016-01-20 02:55:06	https://45.127.92.175/sudosev
1/66	2016-01-19 23:36:03	http://45.127.92.175/sudosev
1/66	2016-01-12 14:54:19	http://45.127.92.175/sudose

The Components

- Loader – Downloads core modules & node list to join the botnet
- Core – Very bad stuff!
- VNC – Why drop a RAT when we can just VNC?
- Backconnect – You too can be a C2!

Sophistication?

- Obfuscated code everywhere!
  - Not really sophistication.
- VM detection
  - IsVirtualPCPresent()
  - Case sBuffer Like “*VIRTUAL*” IsVirtualPCPresent = 1
  - Case sBuffer Like “*VMWARE*” IsVirtualPCPresent = 2
  - Case sBuffer Like “*VBOX*” IsVirtualPCPresent = 3
- Sandbox detection
  - Anubis
  - SandBoxie
- Windows – XP, Vista, 7, 8, 8.1, 10, Server 2003, Server 2008, Server 2012
- Reused code
  - Copied from a Spanish hacking forum

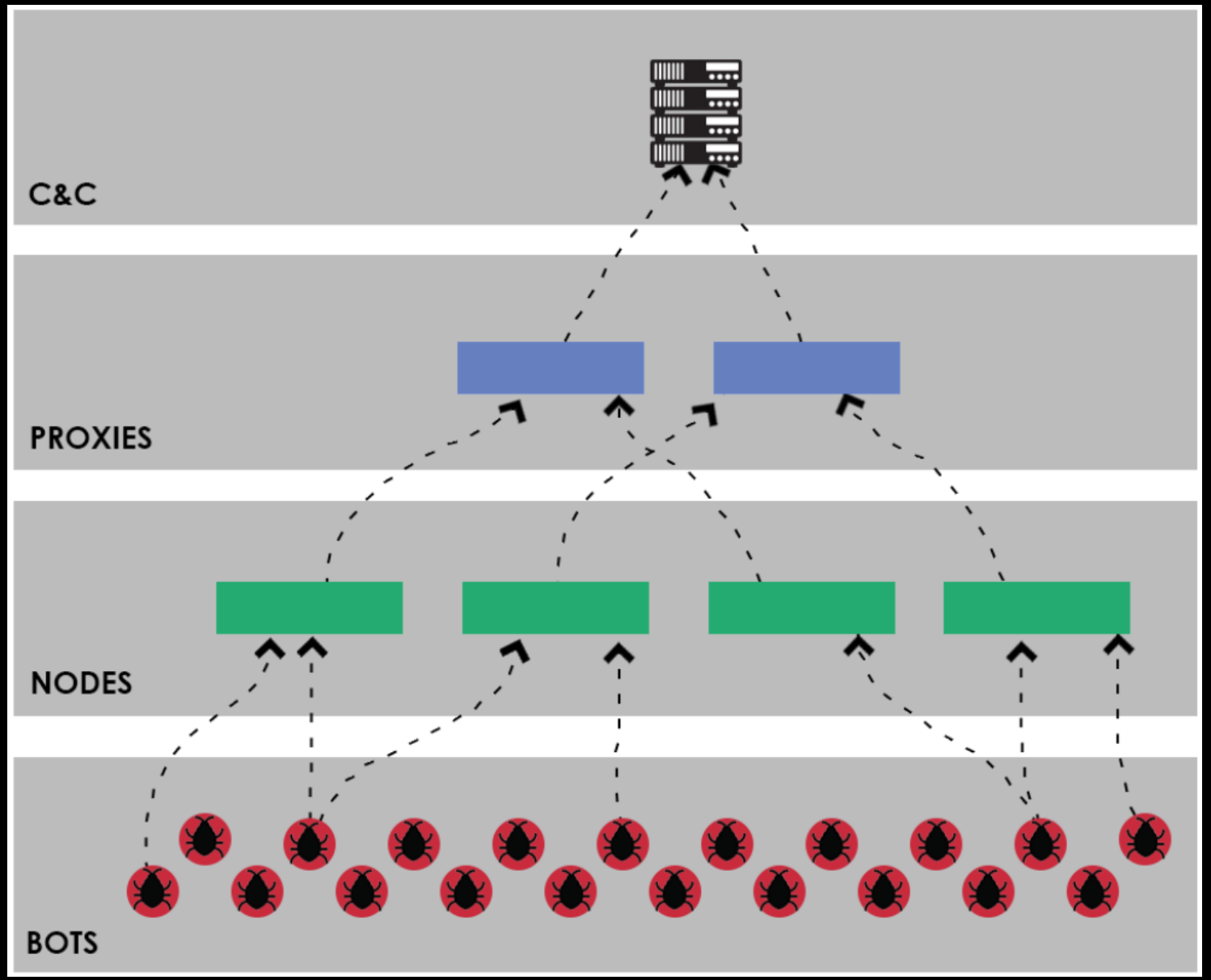
Network Infrastructure

Backend C&C, hidden.

Frontline C&Cs – Usually some sort of CMS

More infected machines with the backconnect module in use for proxying & forwarding

Infected machines, every day users



Encryption changes

- Old encryption scheme
  - No Public/Private key infrastructure
  - 2 byte XOR key (0x55AA)
  - Gzip format once decrypted
- New encryption scheme
  - RC4 key, 16 bytes, ciphered with RSA 2048
  - XOR key, 4 bytes, randomly generated

Sub-Botnets

- October 2015 - 120, 121, 122, 125, 126, 127, 200, 220, 300, 305, 310, 320, 888
- Sub-Botnet 220 seems to be king.
- Botnet 220 was seen distributing TeslaCrypt in February 2016.
- Botnet 120 spike, March 16th 2016, concurrent with Locky
- Botnet 123 spiking via new Angler EK infrastructure, early May 2016
- Botnet 124 observed recently targeting Swiss financial institutions (May 31st 2016)

File distribution

- Mostly weaponized office documents
- Botnet 222 used .js downloaders
- RockLoader Voicemail emails, April 2016
- XXXXXX.exe where X = any alphanumeric value

File Name	File Size	File Type	Mu
DHL Exception ID GB00-1852228843147209.zip	2739		
DHL Case ID GB00-4749102640523899.zip	2684	ZIP	
Mark as Read _Xoom ID542-_65215658_51_.js	6805	JS	
Mark as Read _Xoom ID542-_65215658_70_.js	7211	JS	
Mark as Read _Xoom ID542-_65215658_53_.js	6621	JS	
Mark as Read _Xoom ID542-_65215658_56_.js	7036	JS	
Mark as Read _Xoom ID542-_65215658_46_.js	6656	JS	
DHL Exception ID GB00-7447200130309032.zip	2747	ZIP	
Mark as Read _Xoom ID542-_65215658_69_.js	6880	JS	
Mark as Read _Xoom ID542-_65215658_64_.js	6942	JS	
Mark as Read _Xoom ID542-_65215658_79_.js	7032	JS	
Mark as Read _Xoom ID542-_65215658_47_.js	6845	JS	
Mark as Read _Xoom ID542-_65215658_90_.js	6834	JS	
Mark as Read _Xoom ID542-_65215658_82_.js	7194	JS	
DHL_2566770483.pdf.original.js	7052	JS	
85.93.31.[143]/dhl/track.php	180224	EXE	
DHL Case ID GB00-0918767627966213.zip	2594	ZIP	
DHL_7285767975.pdf.original.js	6943	JS	
DHL_5923535894.pdf.original.js	6637	JS	

www.tracker.h3x.eu

Locky

- Delivered via weaponized office documents and exploit kits
- Files encrypted with AES-128 CTR mode
- RSA-2048 key generated remotely
- Deletes shadow copies of files
- Autostart persistence via registry
- Enumerates network shares and infects if possible

The ‘this literally just happened so I had no time to add it properly’ slide

- June 2nd, a revised version of Dridex started to appear.
- Mostly targeting US banks (56.7%)
- With China and Brazil in close second.
- Now paired with Certuli to evade detection even further

Takeaway

- Can we pick a name for the Dridex/Locky distribution network?
- These campaigns are not perfect (ATS flaw, protocol vulnerabilities, exposed admin panels etc).
- Dridex is still one of the most lucrative and prevalent campaigns out there.
- Criminals are transitioning to ransomware and FAST.
- Ransomware has a somewhat flawless business model.

Questions?