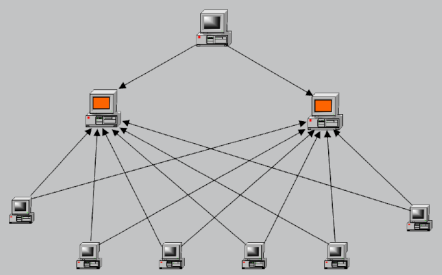
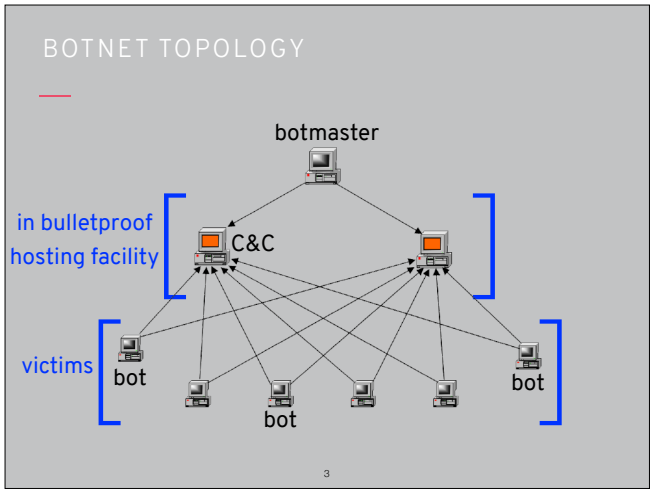
SECURITY (COMP0141): BOTNETS

UCL

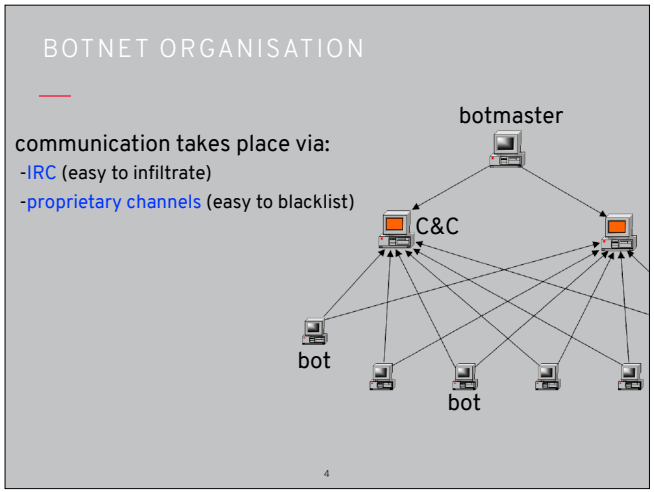
BOTNETS



Botnets are just large networks of compromised machines



Bots are victims that are not in on the scheme. Command and control (C&C) servers are hosted in bulletproof facilities, and many botmasters are in places like Russia



-IRC is like a chat room, this approach is easy to set up but too public so law enforcement can easily infiltrate and see the commands being issued
-Proprietary channels use some form of encryption, harder to spy on but there's a single C&C server they communicate with so it's easy to blacklist that fixed location

HONEYPOTS


A honeypot is designed to be highly attractive to an attacker

- unlocked car with keys in the ignition
- computer with unpatched OS, old browser version, etc.

Operated to find out more information about them (IP address, location, etc.) or provide enough evidence to report

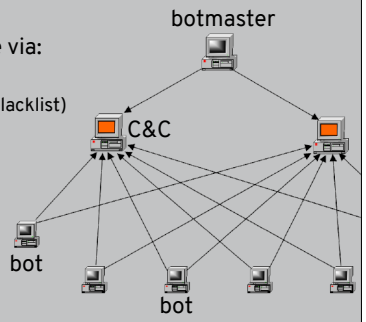
5

Honeypots are a common way for law enforcement or researchers to infiltrate a botnet

BOTNET ORGANISATION

communication takes place via:
-IRC (easy to infiltrate)
-proprietary channels (easy to blacklist)

structure uses:
-multiple tiers (expensive)
-p2p (easy to infiltrate)
-fast flux/domain flux (hard!)



6

-To hide the C&C server we can set up a tiered approach so bots see proxy server rather than direct IP address of C&C server
-This is too static though, since proxy could get taken down. Could use peer-to-peer (P2P) networks where bots with better connectivity get treated as proxy servers, used to both receive and send commands. Again though anyone could act as a peer to see commands
-Even this could still be too static, so we use fast flux/domain flux (see demo) where domain names and IP addresses change quickly so no one knows where the C&C server is (or will be soon)

EXAMPLES

Grum
-shut down in 2012
-500-900K infected

ZeroAccess
-shut down in 2013
-2M infected

Cutwail
-shut down in 2010
-1.5-2M infected

Storm
-peak in 2007
-1-50M infected

7

Here are some examples of big historic botnets

BUSINESS MODEL

q: but how do booter services work? how to do it myself?
a: use a **botnet**.

q: what is the monetary point of creating a botnet?
a: DDoS as a service, **click fraud**, **spam**.

8

Aside from DDoS, what do you use a botnet for?

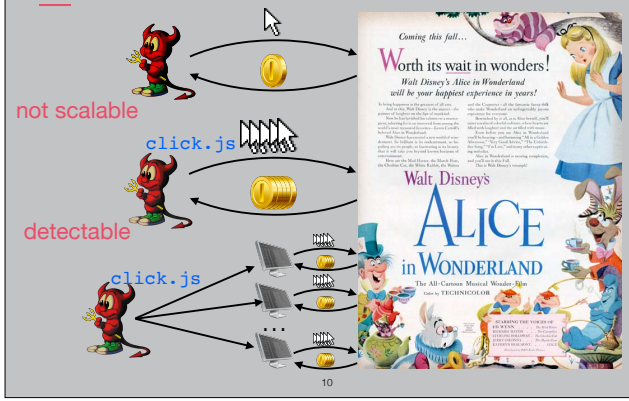
PAY PER CLICK


Pay-per-click (PPC) advertising means advertiser (Alice) pays publisher every time the ad is clicked

9

Let's consider what happens if the publisher is malicious

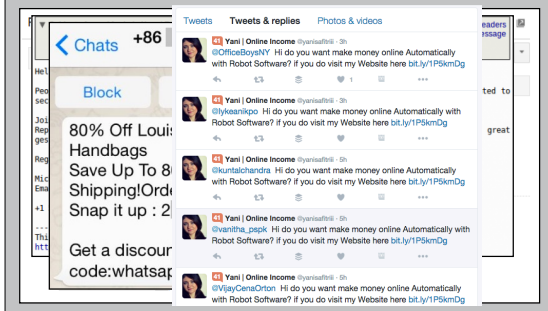
CLICK FRAUD



10

One use of a botnet is click fraud, in which the attacker repeatedly clicks on an advertisement in order to inflate their own revenue

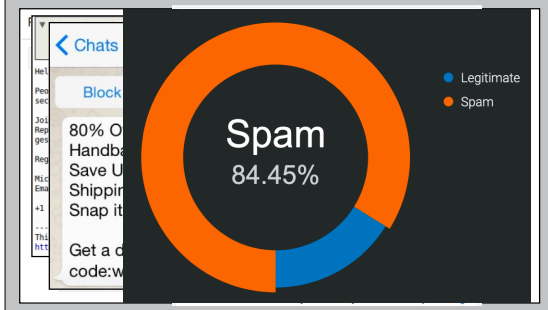
SPAM



11

More prevalent use case is spam, which we're familiar with in email but also happens via text, Twitter, etc. What percentage of all emails do you think is spam?

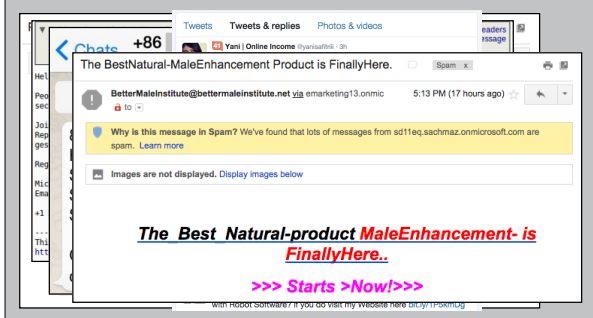
SPAM



12

Spam is incredibly prevalent (number from https://talosintelligence.com/reputation_center/email_rep#tab=1), which is why we're all likely familiar with it

SPAM

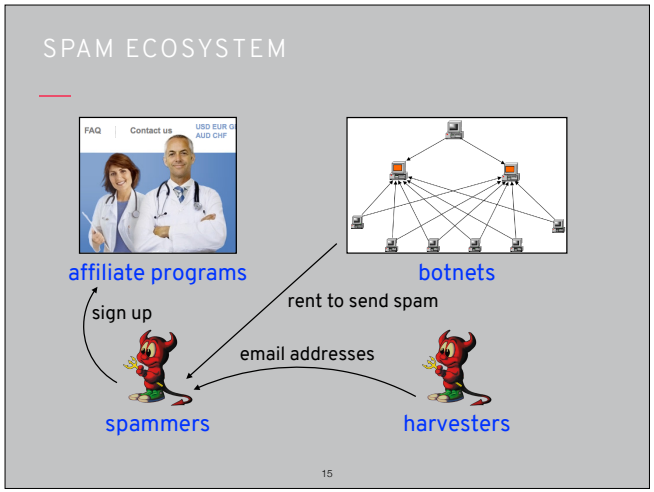


13

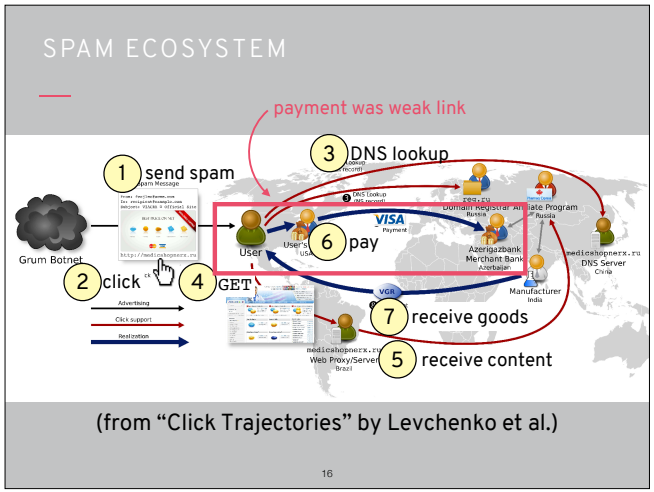
Let's focus on a "classic" type of spam, selling pharmaceuticals

AFFILIATE PROGRAMS

14



We think of spam as email, but what happens if you click on the link? Get to a website that belongs to something called an affiliate program. Affiliate program is separate from spam, spammer typically signs up with affiliate and gets a cut of the profits per customer. Spammer gets list of people to email from harvest, who scrapes websites to find email addresses. He then rents a botnet to send emails



(from “Click Trajectories” by Levchenko et al.)

This is very much a worldwide ecosystem

EXAMPLES

Grum
-shut down in 2012
-500-900K infected
-26% of spam in 2010 (40B/day)

ZeroAccess
-shut down in 2013
-2M infected
-click fraud/Bitcoin mining

Cutwail
-shut down in 2010
-1.5-2M infected
-46% of spam in 2009 (74B/day)

Storm
-peak in 2007
-1-50M infected
-20% of spam in 2008

17

These botnets were responsible for sending a significant percentage of all spam at their peaks. ZeroAccess had a different revenue model

WHERE DO BOTNETS COME FROM?

q: but how do booter services work? how to do it myself?
a: use a **botnet**.

q: what is the monetary point of creating a botnet?
a: DDoS as a service, **click fraud**, **spam**.

q: but how do I create a botnet in the first place?
a: infect computers with **malware**.

18

Botnets are formed using malware, which is also our third major threat to availability