Fast Flux Hosting and DNS

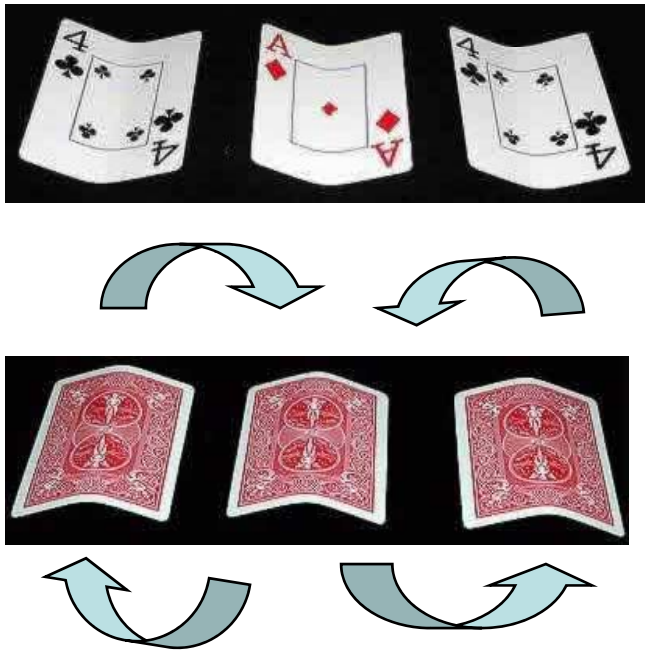
ICANN SSAC

What is Fast Flux Hosting?

- An evasion technique
- Goal of all fast flux variants
  - Avoid detection and take down of web sites used for illegal purposes
- Technique
  - Host illegal content at many web sites
  - Send phishing email with links to web site's domain name
  - Rapidly change the locations of the web site so that no one site is used long enough to isolate and shut down

e-version of age-old scam

- 3 card monte, a classic street corner scam



Bet on which card is the Ace of Diamonds!

In *basic* fast flux attacks, the web site is the Ace of Diamonds

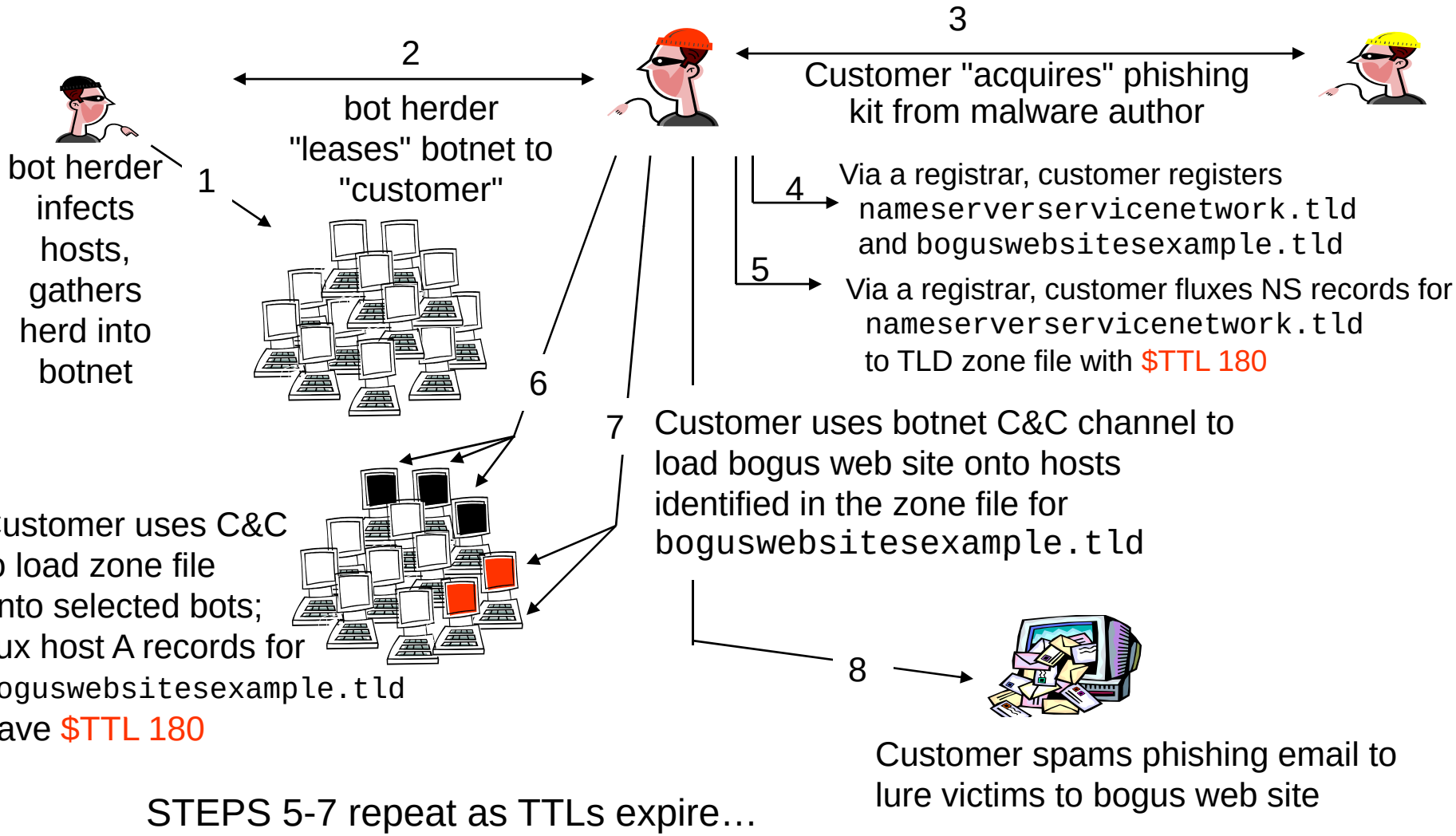
Eluding the beat cop

- In the brick-and-mortar world, 3 card Monte is run on a street corner
- Lookouts warn the scam artist when the beat cop is approaching
- The scam artist packs up his game and moved to another corner
- In the e-world, scammers alter the DNS to "change corners"
  - This is called Name Server Fluxing
  - Double flux combines basic and name server fluxing

Variations on a theme…

- Basic fast flux hosting
  - IP addresses of illegal web sites are fluxed
- Name Server (NS) fluxing
  - IP addresses of DNS name servers are fluxed
- Double flux
  - IP addresses of web sites *and* name servers are fluxed

Anatomy of an attack



STEPS 5-7 repeat as TTLs expire…

Mitigation Alternatives

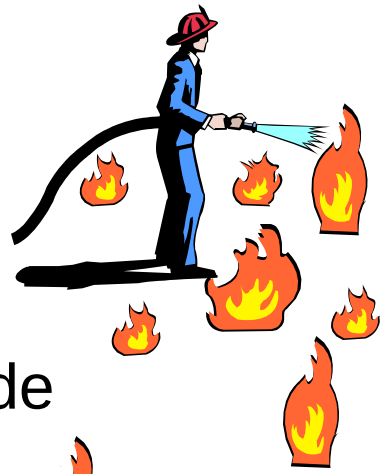
1. Shut down the bots (botnets) that host fast flux

2. Shut down the fast flux hosts

3. Remove domains used in fast flux hosting from service

Can we shut down the bots?

- Bots number in the 100,000s or 1Ms
- Current mitigation techniques
  - Anti-malware on desktops and at gateways
  - Education and awareness
  - Current efforts not close to stemming the tide
- Possible additional techniques include
  - Process and executable white listing
  - Network access/admission controls for private networks and public Internet service
  - Inclusion of bot detection in "unified threat management" security



Can we shut down fast flux hosts?

- Today,
  - Responders and law enforcement collect information (and obtain court orders) to shut down fast flux hosts
  - The shut down process operates at a real world pace
  - Fast flux is designed to thwart these activities
  - Fast flux hosts remain operational well beyond the average illegal site lifetime of 4 days
- Possible additional measures
  - Accelerated domain name suspension procedures
  - Information sharing among responders, CERTS, LEAs
  - Accredited list of responders, acknowledged by registrars and registries

Can we remove domains used in fast flux hosting from service?

- Some domains are easier to delete than others
  - Obscure strings, WHOIS inaccuracies, rapidly changing TTLs, …
- Other domains are HARD to take down
  - Illegal sites hosted
    - on legitimate but compromised servers
    - on bulletproof hosts
    - where other "safe harbor" conditions are available
- Overly simplistic detection methods may result in false positives

Additional practices we can consider

- Practiced today (but not uniformly)
  - Authenticate contacts before allowing NS record changes
  - Rate-limit NS record changes
  - Detect and block automated NS record changes
  - Enforce a minimum TTL (e.g., 30 minutes)
    - Whitelist or exception handling for registrants with legitimate uses
  - Abuse monitoring systems to report excessive DNS configuration changes
    - Domain name quarantining (and honeypotting)
  - Prohibit use of domains and hosting services to abet illegal activities Universal Terms of Service agreements
  - Resolve suspended domains to antiphishing education page

Who is "we"?

- More than SSAC, more than ICANN
- SSAC's role
  - Publish its findings
  - Share information with antiphishing and anticrime groups
  - Make recommendations to the ICANN Board
- ICANN
  - work with registries and registrars on aspects of domain name registration and DNS that abet double flux in matters of policy and common/best practices
- Constituencies and communities
  - Education and outreach to ISPs, broadband Internet users, businesses

SSAC Findings

- Fast flux hosting exploits domain name resolution and registration services to abet illegal activities
- Fast flux hosting hampers current methods to detect and shut down illegal web sites
- Current methods to thwart fast flux hosting by detecting and dismantling botnets *are not effective*
- Frequent modifications to NS records and short TTLs in NS A records in TLD zone files can be monitored to *identify possible abuse*
- Effective countermeasures against fast flux include enforcing a minimum TTL > 30 minutes and blocking, rate-limiting, and monitoring to detect automated changes to DNS info