Linchpins of the Dark Web

Authors: J. Zhang et al.
Presented by: Chris Moran

Roadmap

- Background
- Methodology
- Web Structure
- Experiments
- Interpreting the Data
- TDS
- DIscussion

Malicious Attacks

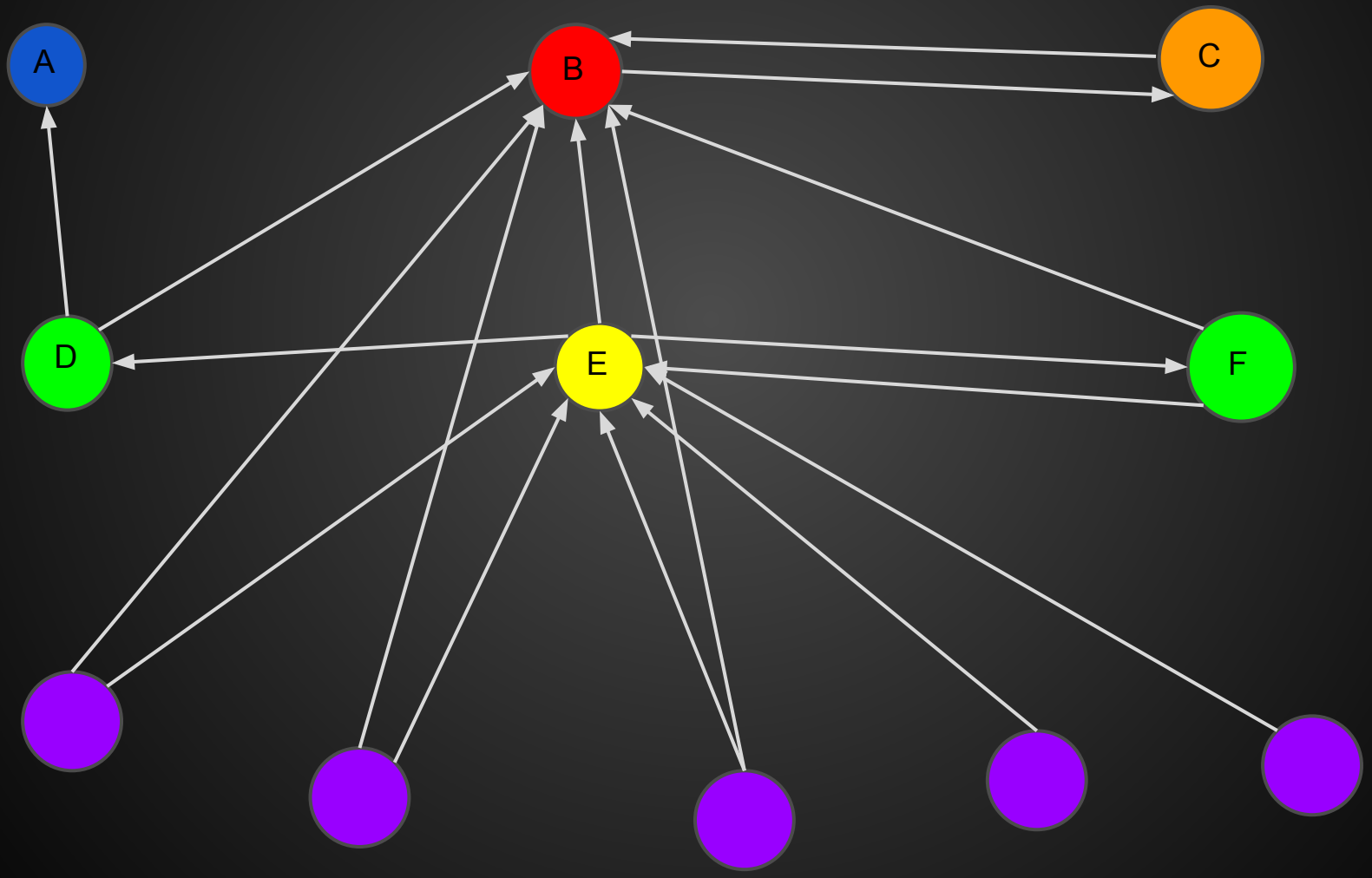
- Popularity = platform for malicious attacks
- Previous research focus on detection of attacks
  - Spam filters
  - Url blacklists
    - Drive by downloads
    - Phishing

What does the underlying architecture look like?

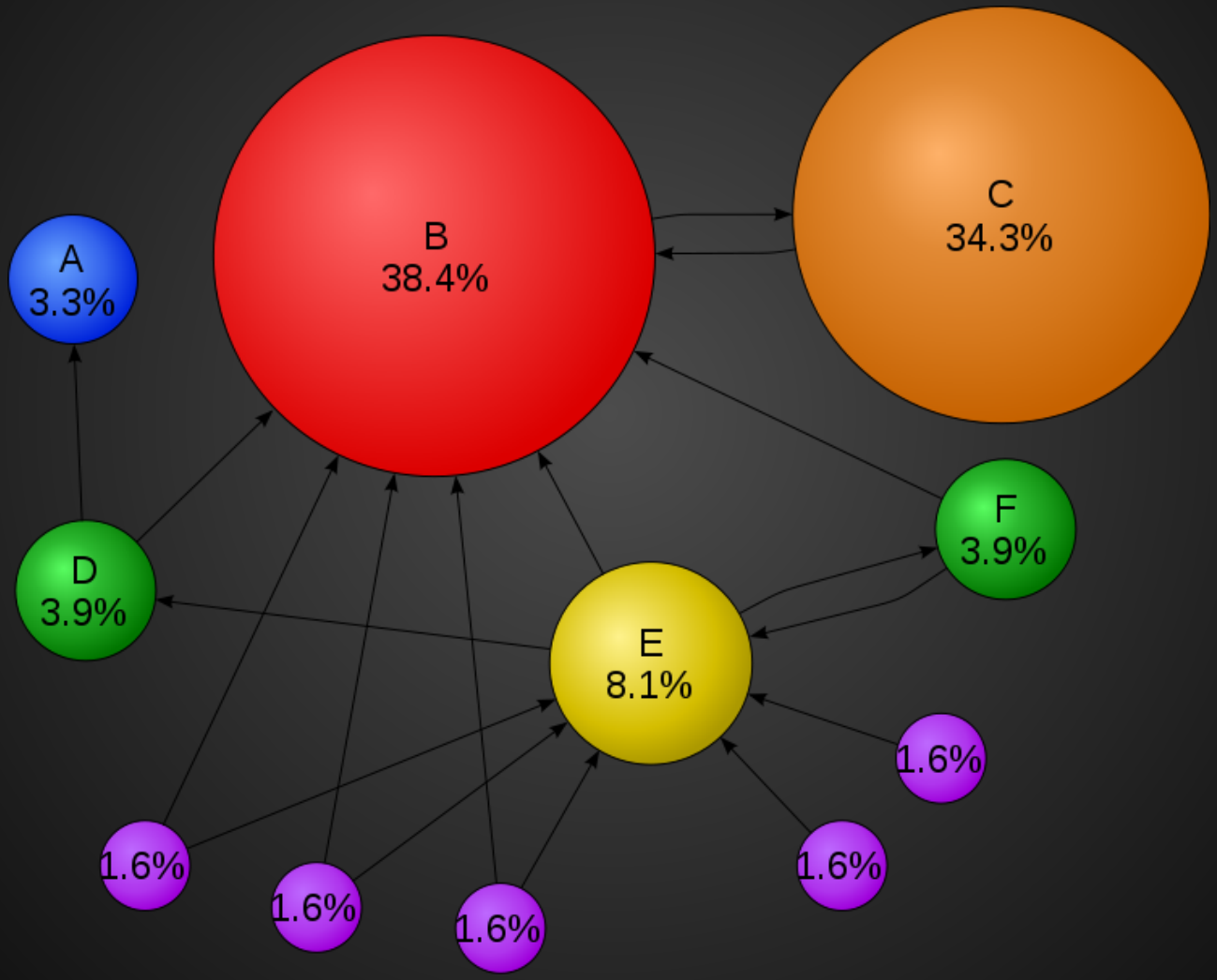
PageRank

- Google's starting point
  - Stanford paper
- Idea
  - Quality of page p is proportional to aggregate quality of the pages linking to it
  - PageRank(p) = probability a person clicking on links at random will land on your page
    - Crawler picks random start page
    - Follows links, jumps at random to avoid loops
    - PageRank(p) = proportion of visits

Example

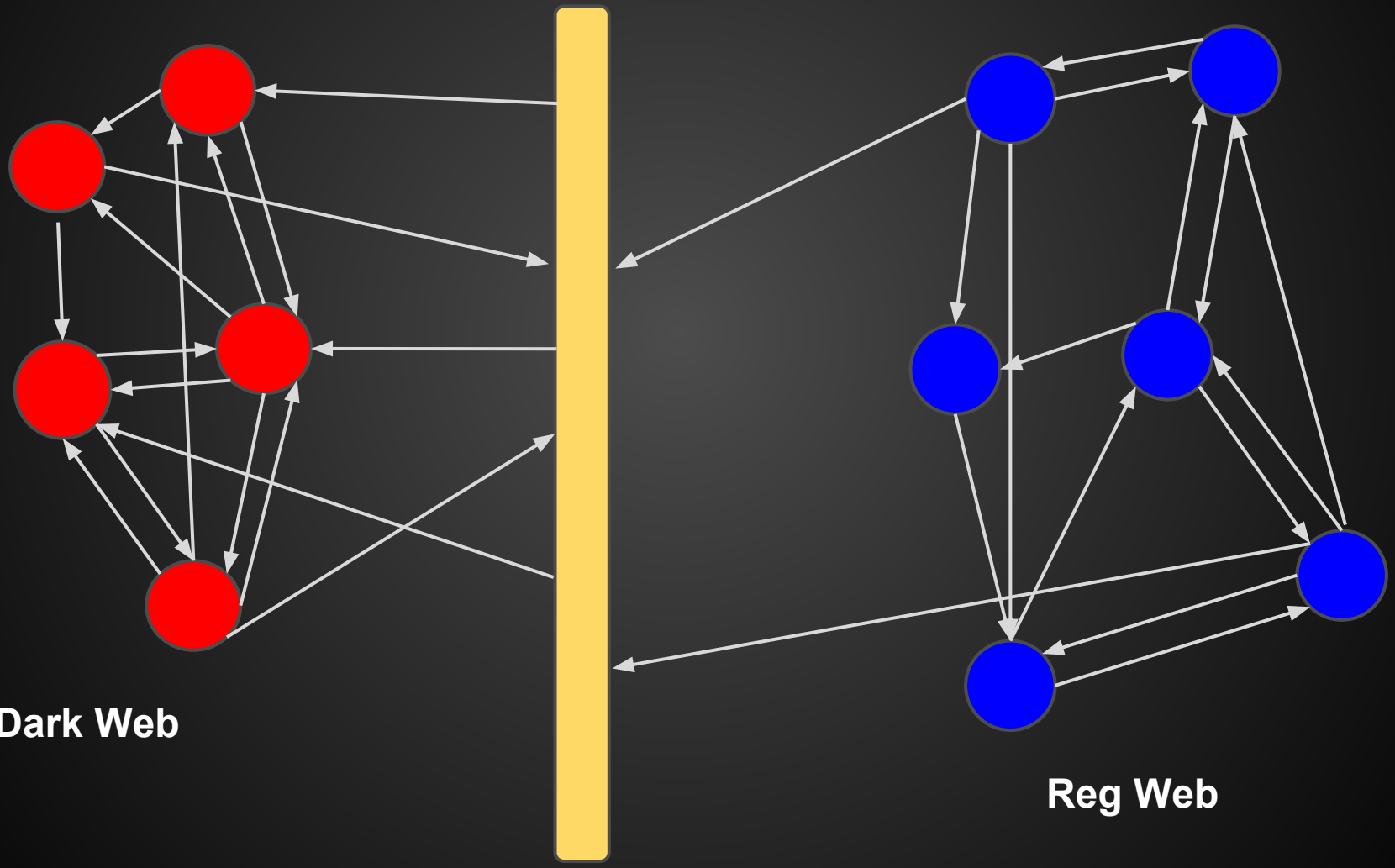


Probabilities



Maybe we can apply this to detect malicious sites?

Malicious Topology Hypothesis



Data Collection

- Crawled set of sites, tracking redirections
  - Drive-by-Download - 1.5 mil URLs
  - Warningbird feed - 300K twitter spam URLs
  - Twitter - 1.6 mil gather from twitter trending terms
  - Alexa - 2 mil URLs
- Labels
  - Malicious - Anti-Virus scanner detects a virus in contents
  - Suspicious - Any path the traverses a route with a known malicious site
  - Benign - EasyList, EasyPrivacy, and by hand
  - ~80% unlabeled

Hostname-IP Cluster

- Based on previous work
- Group hosts based on IP and Whois info
- Steps
  - Unique HIC to every hostname
  - Iteratively inspect HICs
    - Compute overlap of IPs using Jaccard distance
    - If overlap larger than threshold, merge if whois registrar is the same
- Results
  - ~2 Million HICs
  - ~15K solely malicious, aka dedicated HICs
  - Mix known as non-dedicated HICs

Example HIC generation

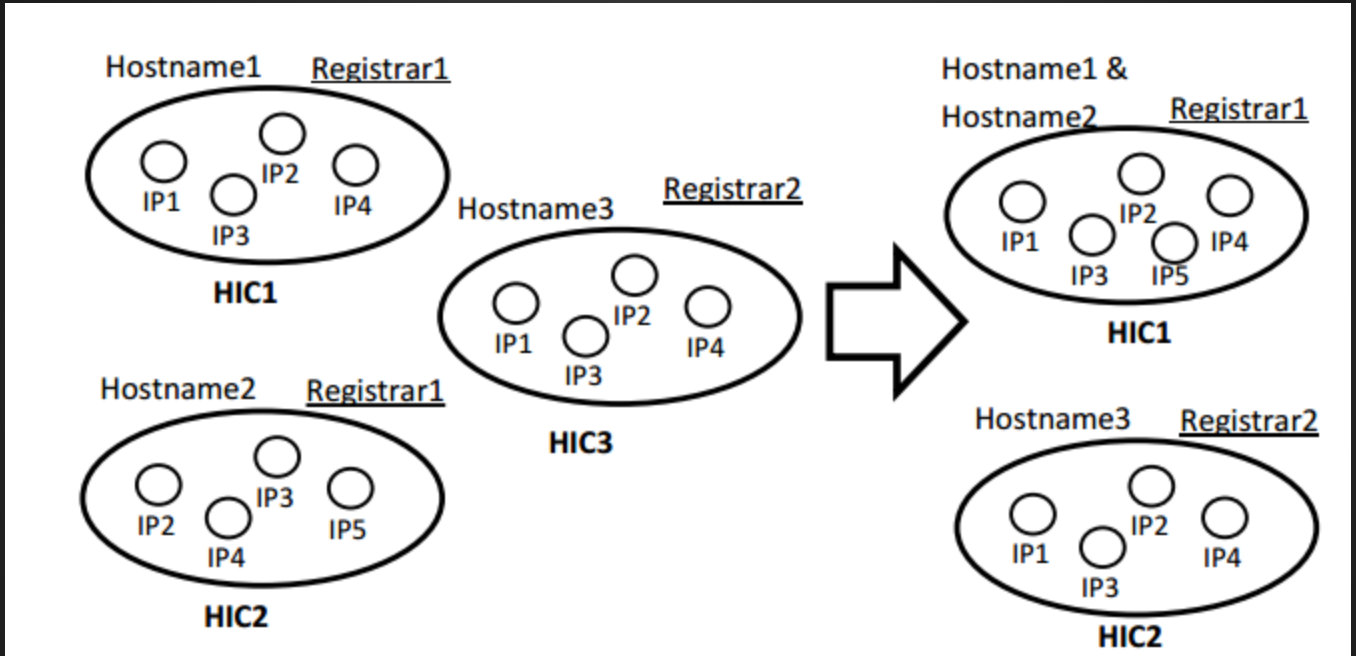


Figure 2. HIC generation process.

Graph Properties

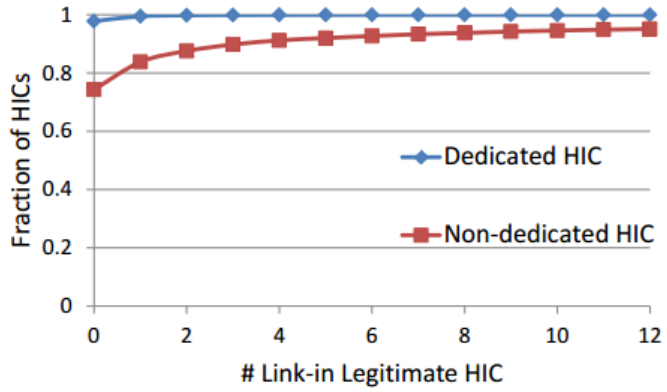


Figure 3. CDF of the number of Legitimate Link-in HIC between Dedicated HICs and Non-dedicated HICs

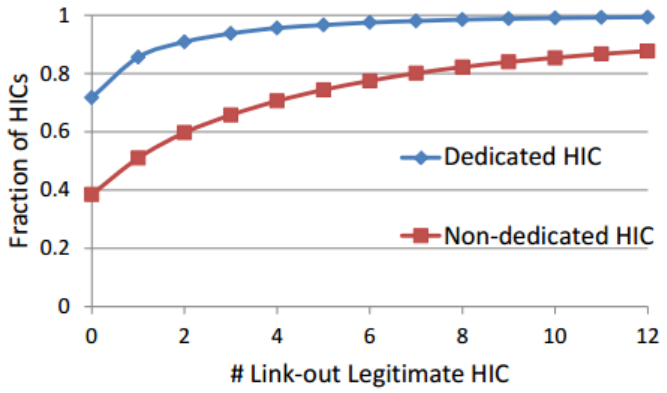


Figure 4. CDF of the number of Legitimate Link-out HIC between Dedicated HICs and Non-dedicated HICs

Topology perfect for Page Rank!

Page Rank Detection

- Each HIC maintains pair of scores
  - Good to model popularity among benign hosts
  - Bad to model popularity among known malicious hosts
- Iteratively apply algorithm to completion
  - If bad above threshold α and ratio of good/bad is below threshold β HIC considered malicious
- Requires initial seeding of values in graph

Score Propagation

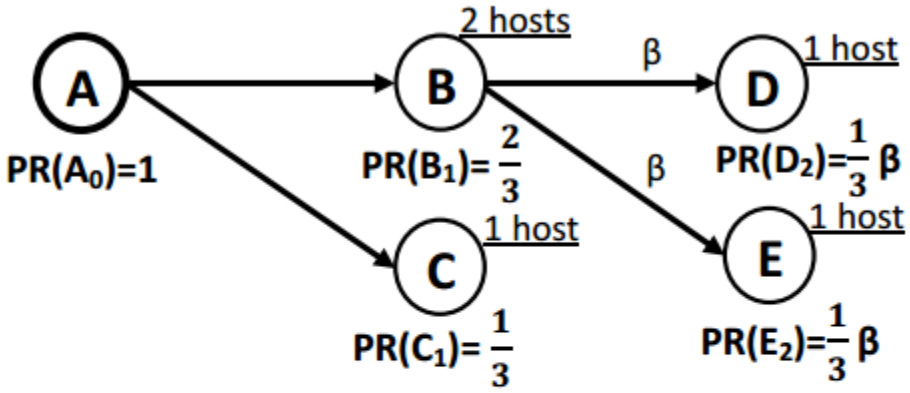
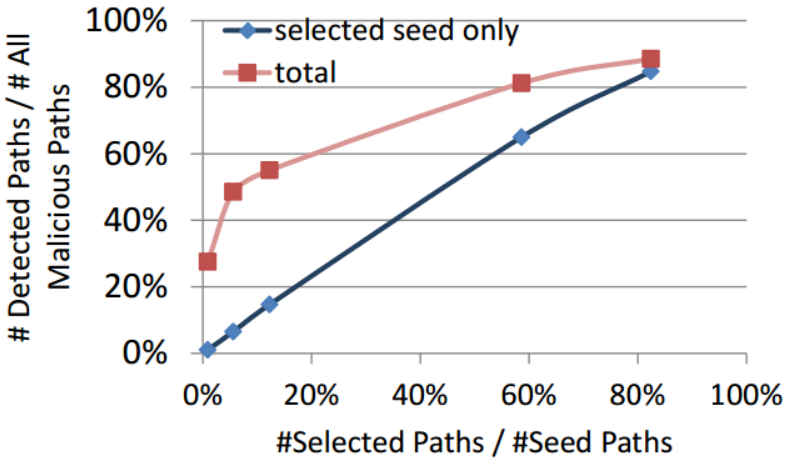


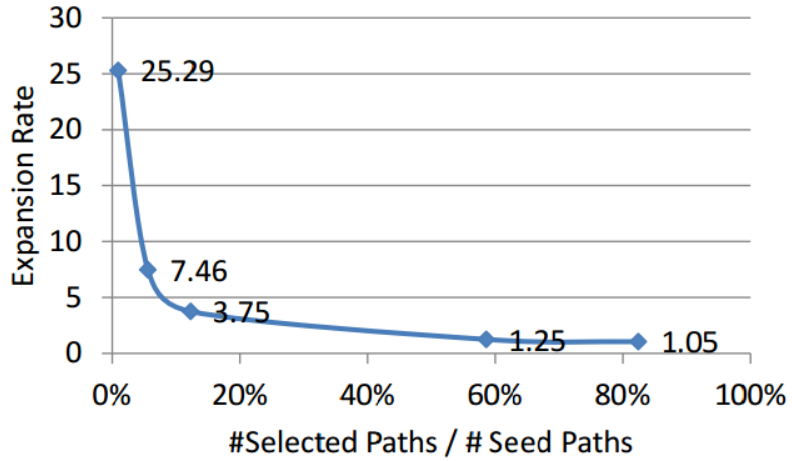
Figure 5. Score propagation. Assuming A has initial score 1, child B will receive score $\frac{2}{3}$ and child C will receive score $\frac{1}{3}$, as the number of hostnames within B is two times as within C. In the second round, B's children D and E will receive score $\frac{1}{3}\beta$ under score dampening.

Initial Experiments

- Seeds
  - ~61K benign HICs
  - ~53K malicious HICs
  - Vary subset of malicious seeds - 1,5,10,50,90%
    - Beta dependent on # of seeds used
- Run 20 iterations of PageRank
  - Interesting to see how results narrow as algorithm progresses

Initial Results



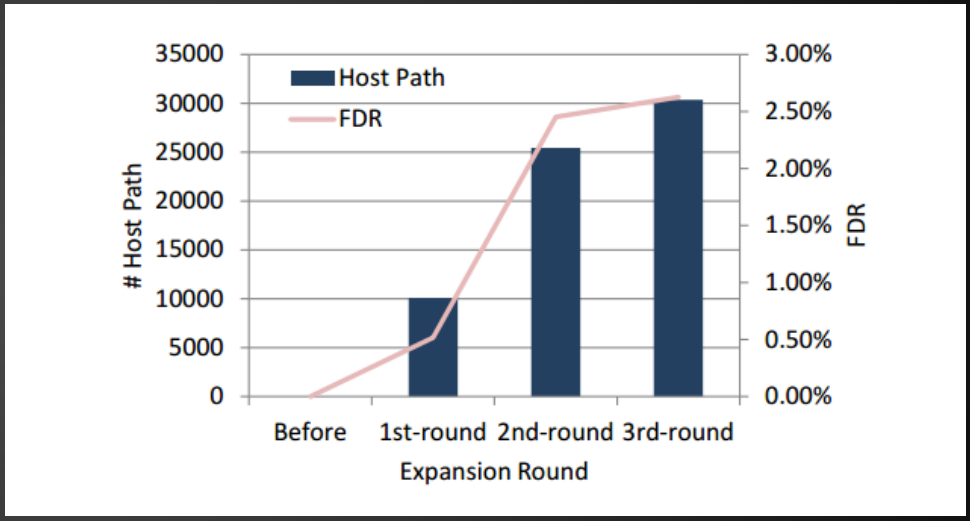


Very good!

- High expansion rate for lower percentages
- Low error rates
  - > 0.025% false positives (malicious as benign)
  - 2.4% false negatives (benign as malicious)
    - Grows with seed %
- Can process be improved?

Seed Rolling

- Feed set of detected nodes and re-run PageRank
- For 5% seeds, jump from ~50% to ~75%, with low FDR



In Degree Approach

- Assume that if site receives traffic from other malicious sites, it is also malicious
- Results in high false detection rates
- Trouble detecting malicious HICs with small in-degrees

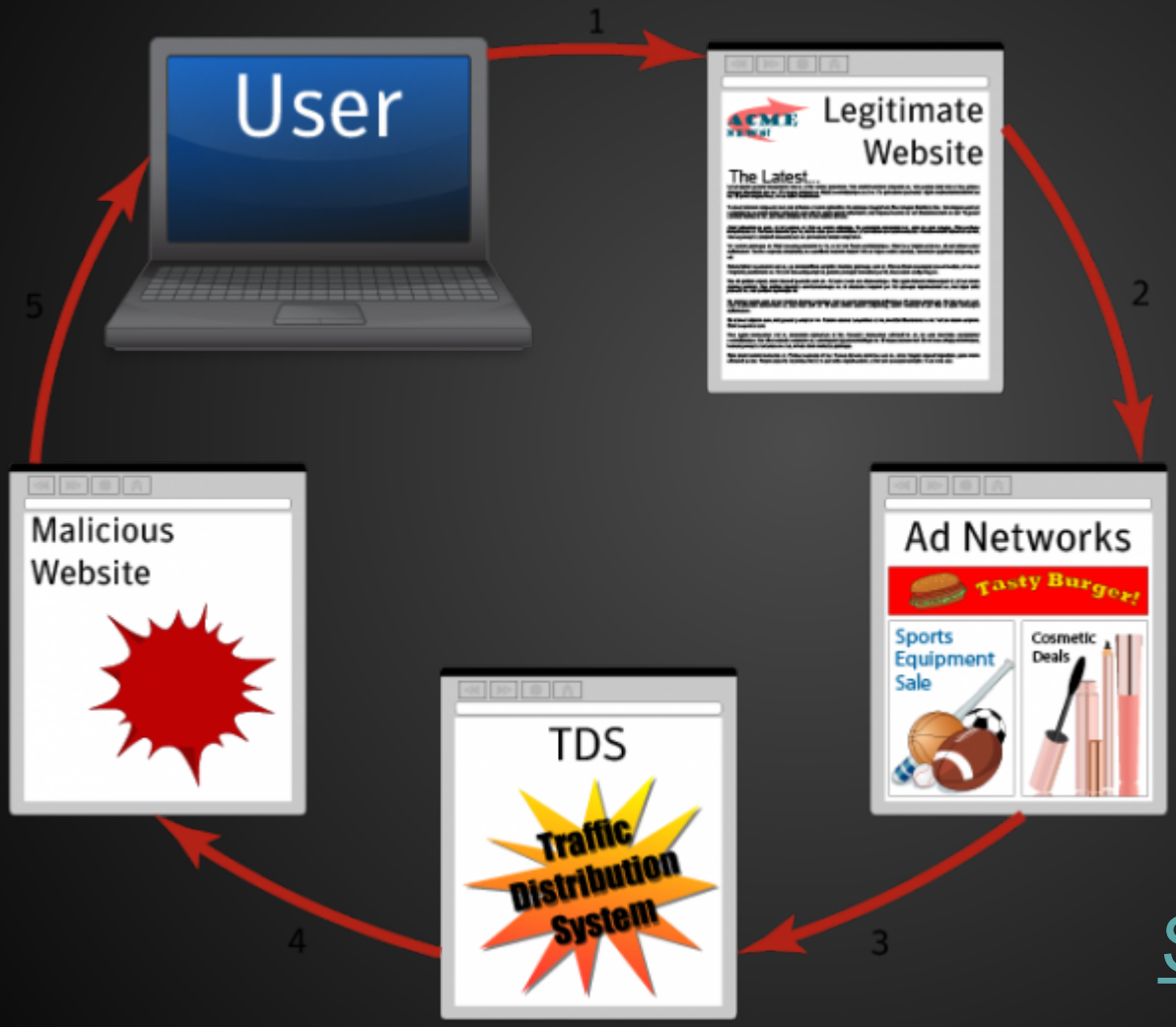
What attacks are detected?

- Categorization Tools
  - Forefront reporting
  - Content and URL Clustering
  - Safebrowsing reporting
- Redirection key in attack path

Role	URLs	URL paths
exploit	13,216	89,019
click-fraud	5,955	36,761
scam	29,411	632,644
fakeav	1,604	1,805
other	1,031	90,962
redirector	286,275	2,479,695
unknown	69,062	526,952
total	406,553	3,088,741

Table VII
ROLES OF URLS.

Traffic Distribution Networks



Source

Why TDS?

- Attacker only needs malicious site, no longer needs to lure user
  - Specialization
- Generation of income for TDS maintainer
- TDS have longer life span
  - More difficult to detect

Landscape

- Toolkits (Sutra, Simple TDS, Advanced TDS)
- Funnel 53% of doorway traffic to TDSs
- Can perform IP filtering
  - Might resolve to different sites depending on number of visits
- Attack types
  - ~50% exploit servers
  - ~3% scam sites
  - ~60% unknown attack types

TDS Hosting

- DDNS providers, free subdomains
  - A quarter of TDSs use DDNS
- Free hosting providers
  - About 15%
- Similar IP prefixes

#	ASN#	ASN Name	Country	Number of IPs
1	16265	LEASEWEB	NL	45
2	24940	HETZNER	DE	33
3	28753	LEASEWEB-DE	DE	19
4	44050	PIN-AS	RU	13
5	21788	NOC-Network	US	10

Table XI
TOP 5 ASNS HOSTING TDSS

TDS Life Time & Parking

- Uptime median 65.21 days
  - Can live much longer
  - Not always resolving to malicious sites
- Parking good option for TDS
  - Lots of traffic funneling to IP addr for monetization
  - Redirect to ads sites like DoubleClick or BidSystem
  - Free hosting sites can take advantage of this after malicious site reported

Discussion

- What will the response of malicious site controllers be?
- How can research be used?
  - Better browser evasion tools?
  - Smarter search engines?

Thanks for listening!