BRIDE OF POD PEOPLE

COURTNEY FALK, PODPEOPLE <AT> INFINITE-MACHINES <DOT> COM

CIRCLECITYCON 2023

INTRODUCTION

WHAT IS ANY OF US DOING HERE?

PII DISCLAIMER

- No personally identifiable information attributed to users will be disclosed
  - User names, actual names, email addresses, profile page URLs
- No threat actor PII is disclosed either
- This information was all found via open source searches
  - **DO NOT BE A JERK**

WHO AM I?

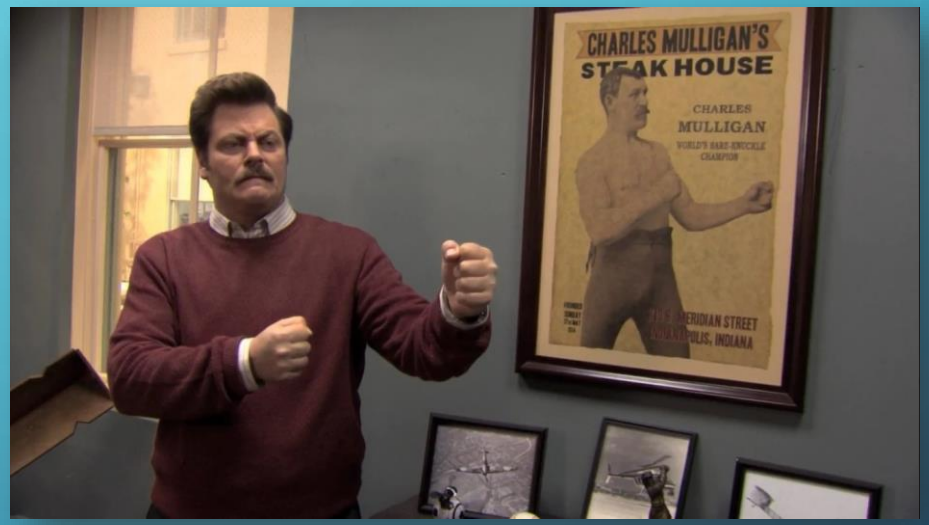
- Doctor of information security
- 15+years of experience in government, academia, and private industry
- Moderately skilled Magic player, low-skill Star Wars: Armada player
- Available for hire!
  - Must be security-focused
  - Preference for threat intelligence

AGENDA

- Pod People review
- Steps of the spam SEO
- Blogg and MySpace data analyses
- Cut for time:
  - Use of URL shorteners
  - One-off WordPress accounts
    - Same TTP (cloaking domains and text lures)
    - No validation required to create accounts
  - Viruses and other malware
    - There are other campaigns that exploit user machines and redirect them to the same CPA network

THE INVESTIGATION

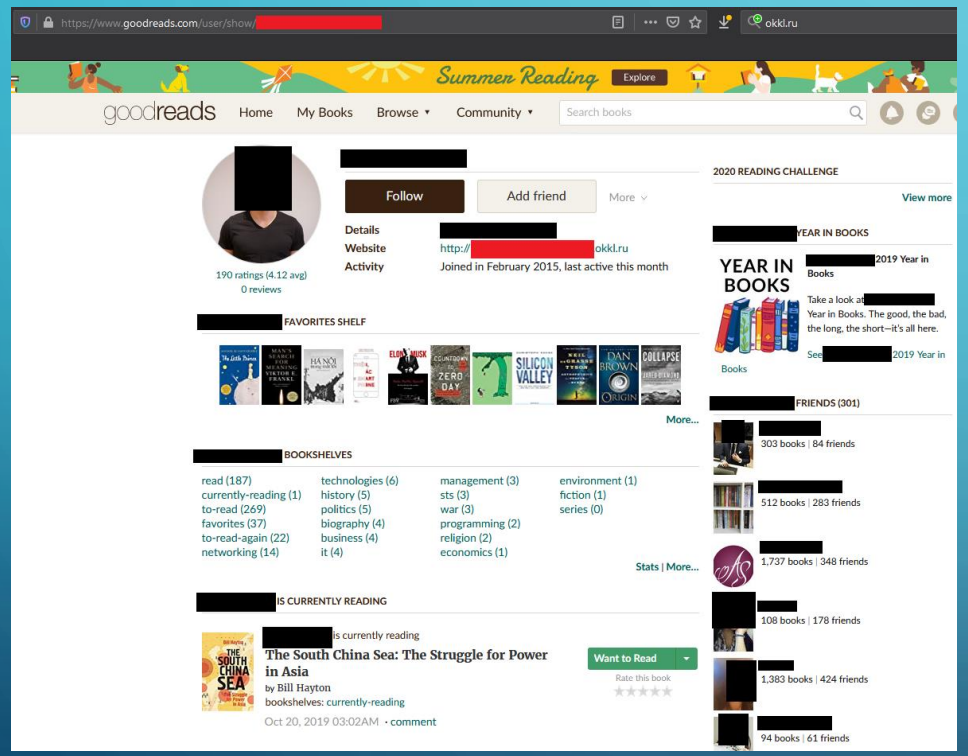
THE MEAT AND POTATOES OF THE MATTER



HISTORY

- Started in 2020 with the Pod People Campaign
- Noticed IoC overlap with older/concurrent WordPress multi-tenant site compromises
- Novelty
  - Some IoCs scattered singly around the Internet (AlienVault, Joe Sandbox, etc.)
  - Largest IoC collection in one place
  - First attempts to describe TTP, timelines, threat actors
  - Why no reporting? Not sexy enough
- Spent $0 on the investigation

THE ORIGINAL POD PEOPLE



- First noticed on Goodreads
- Custom spam domain that includes the user name
- Lived-in accounts that were stolen
- Automated botnet liking activity
- Connections to other sites

STEP 1: COMPROMISE USER ACCOUNTS

- Null hypothesis:
  - H_0: This is normal
- Alternate hypotheses:
  - H_1: Exploit to gain access to the target site
    - \- A very low infection rate (perhaps 1%)
    - \- Expensive and site-specific
  - H_2: Credential stuffing to steal individual user accounts
    - \+ Old accounts with 1-2 years gap in activity
    - ? Where do the credentials come from?
  - H_3: Cultivated accounts
    - \- Lengthy, highly diverse posting history (lived in)
- Average of 2 years between last legitimate post and first spam post

STEP 2: CLOAKING SERVICE

- Decouple the traffic source and sink
  - Legitimate uses for non-criminal affiliate programs
- Basically a reverse proxy
- Create a unique subdomain per compromised account
  - Often use the compromised user account name as the subdomain
  - Domains are heavily reused across social networks sites
  - Unanswered question: Does the threat actor record HTTP referrer data? (Tracking where the activity originates from)

CLOAKING SERVICE OBFUSCATION (RED BOOLEAN)

First five domains were never registered (will not resolve)

```
function re() {
    var url = 'https://www.capha-auditor.ru/?u=63fkp0n&o=uh7pmz8';
    document.location.href = url;
}

function red() {
    var url = 'https://posholhahuybot.com/?u=63fkp0n&o=uh7pmz8';
    document.location.href = url;
}

function redb() {
    var url = 'https://brasileprofit.or/?u=63fkp0n&o=uh7pmz8';
    document.location.href = url;
}

function redbo() {
    var url = 'https://leprikon.in/?u=63fkp0n&o=uh7pmz8';
    document.location.href = url;
}

function redboo() {
    var url = 'https://www.tomaslide.life/?u=63fkp0n&o=uh7pmz8';
    document.location.href = url;
}

function redbool() {
    var url = 'https://takeyourpresent.life/?u=63fkp0n&o=uh7pmz8';
    document.location.href = url;
}

redbool();
```

GET parameters for tracking user and campaign

The only code that actually executes

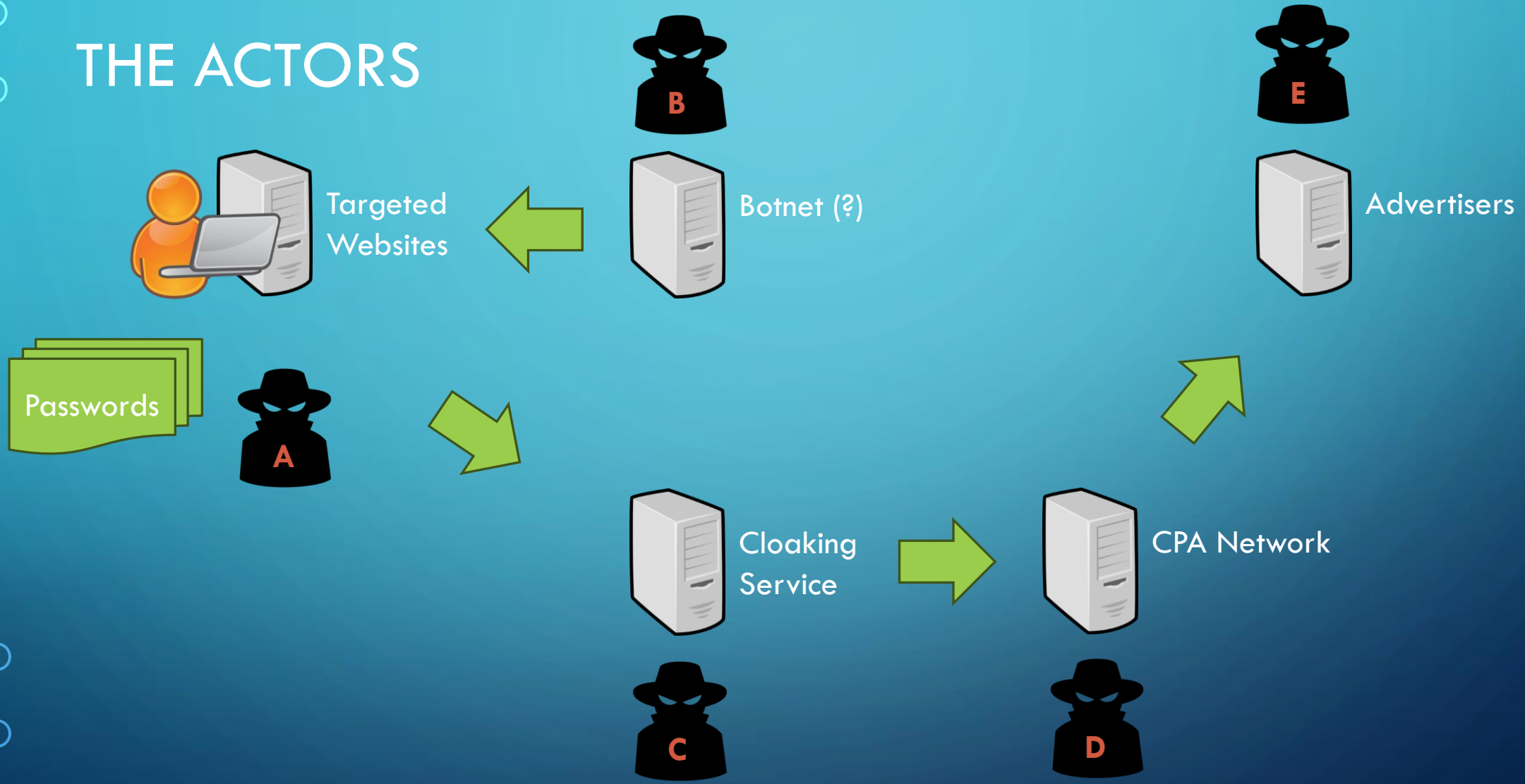
No JavaScript execution, meta redirect to Google (scanner check)

```
<meta http-equiv="refresh" content="0;url=https://www.google.com/" />
```

STEP 3: CPA AFFILIATE NETWORK

- Cost per action (CPA) model of monetizing traffic
- Tracks affiliate parameters
  - ?u=<user>&o=<campaign>
  - These parameters are common across legitimate affiliate programs
- Adds session ID parameter, cookies
- Three-word-domain.live pattern for domain names
  - Also uses three-digit subdomains
- Serves up heavily obfuscated JavaScript (not yet reversed)
- Pass users to sketchy advertisers

THE ACTORS


B
E
Targeted Websites
Botnet (?)
Advertisers
Passwords
A
Cloaking Service
CPA Network
C
D

DATA SETS

- Set 1: Blogg.se
  - Swedish WordPress multisite
- Set 2: MySpace
- Over 500 samples each
- 80+ other sites affected

SPAM LURE MESSAGES

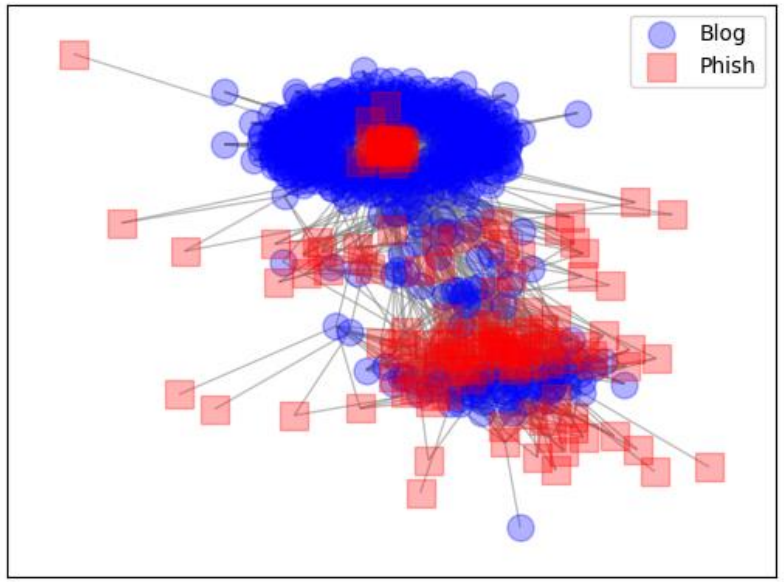

www[redacted].xxxtor.su - passionate sexy girls brighten up your loneliness and will surround you affection and love.

www[redacted].xxxtor.su - passionate sexy girls brighten up your loneliness and will surround you affection and love.

2022-11-25 @ 00:21:39 Permalink В общем-то Kommentarer (0) Trackbacks ()

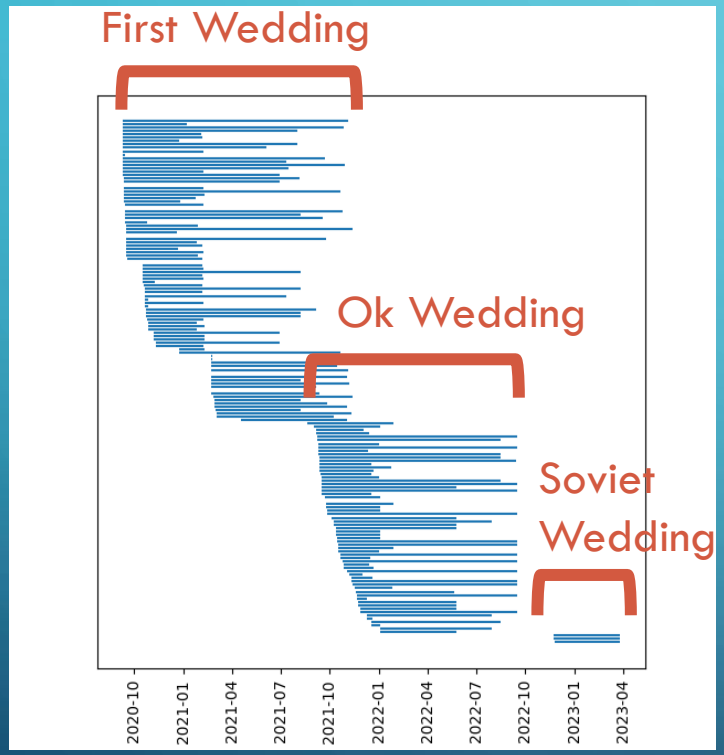
- Not universal across sites (not every site gives users the ability to post text blobs)
- Sex/female-themed
- Broken English
  - Mixed Latin and Cyrillic alphabets
  - Interjected Ukrainian/Russian words (usually sex-themed)
  - Probably generated using a pattern
- Fairly uniform distribution across posts

BLOGG USERS AND DOMAINS



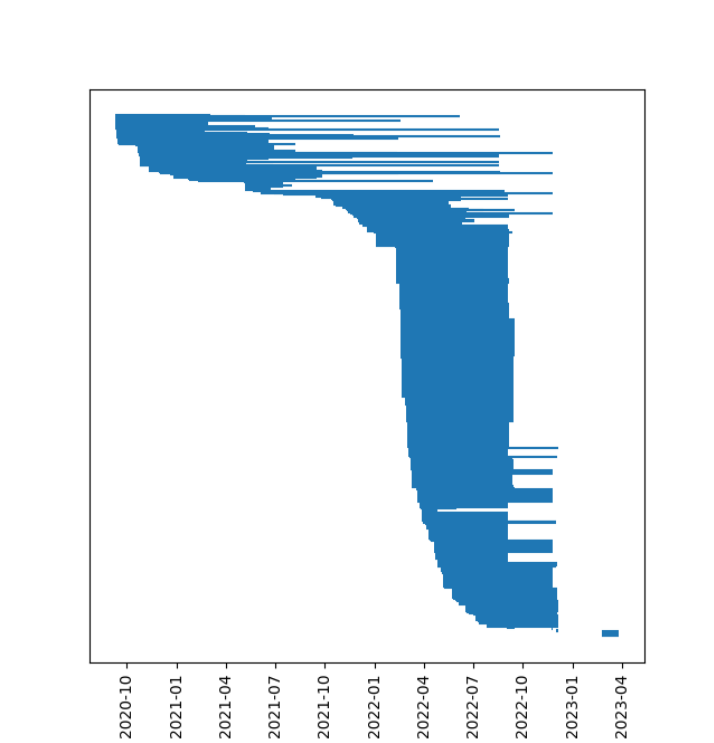
- Displays two distinct behavior patterns
  1. Blogs linking many different domains (bottom)
  2. Many blogs linking to just a few domains (top)
- Notice the overlap (middle)

BLOGG.SE CLOAKING DOMAINS OVER TIME



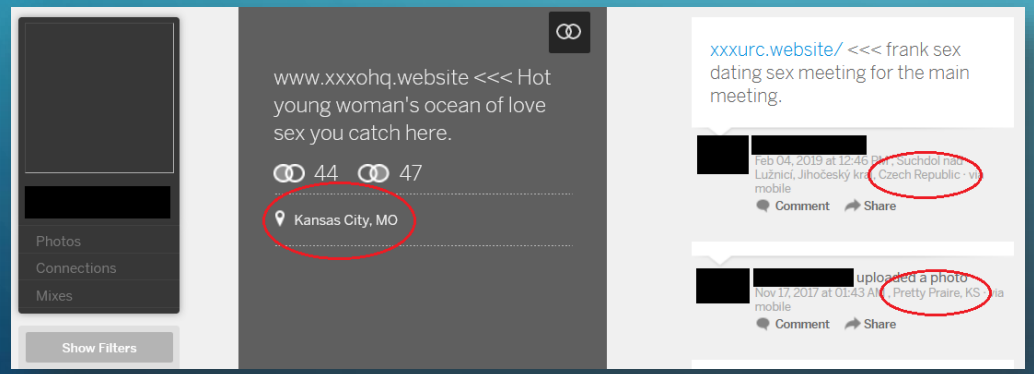
- Activity clustered by time and indicator similarity
- Three general phases:
  1. First Wedding
     - Registered with REG.RU
  2. Ok Wedding
     - Domain regex: ok[a-z]{3}\.(ru|online)
  3. Soviet Wedding
     - .su TLDs
     - Registered with Fast Engine

BLOGG USER POSTS OVER TIME



- No noticeable correlation between user account and cloaking domains utilized in lures
- The post activity shape roughly follows the cloaking domain activity

MYSPACE



- Possibly older, more stale cloaking domains
- Three different clusters of activity:
  1. Profile, Latin-script text, no per-user sub-domain
  2. Profile, mixed-script text, per-user sub-domain
  3. User post (often doubled posts), Latin-script text, no per-user sub-domain, "<<<" separator
- Botnet activity: 60% of users are US, only 9% of posts are US

INFRASTRUCTURE COST ESTIMATES

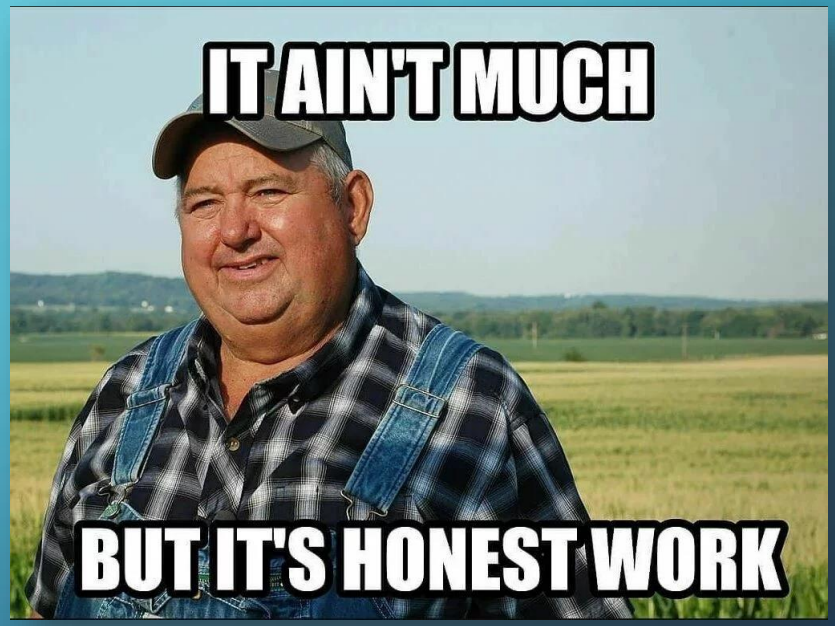
- Based just on the Blogg activity
- Older domains appear to be abandoned
- Domain registrations: over $5000
  - REG.RU and Fast Engine (both Russian)
- Virtual private servers (VPS): $160
  - Aeza @ $5.71/mo. (also Russian)

DENOUEMENT

WHAT DID WE LEARN?

CONCLUSIONS

- Not the most thrilling campaign on record
- Some remediation on the part of web sites (+1 to FourSquare)
- Not safe to assume that it will always stay as spam SEO
- Unanswered questions:
  - Threat actor attribution
  - Identification of the botnet in use
  - The software used in the cloaking server



SUGGESTED REMEDIATIONS

- Users:
  - Use strong passwords, don't reuse passwords across sites, consider a password manager
  - Deactivate/delete old, unused accounts
  - Be ware of new TLDs
- Social media sites:
  - Scan for these IoCs
  - Share log data (ISACs, InfraGard, etc.)
  - Deactivate/delete old, unused accounts
  - Use password compromise sharing services to screen user passwords
  - Monitor/moderate/curate user-created content
  - Validate user account creation

IOCS ON GITHUB

- https://www.github.com/podpeople/brideofpodpeople
- What's included:
  1. This presentation
  2. Domain names of cloaking service
  3. IP addresses associated with cloaking domains
  4. Domain names of CPA network sites
  5. Text lures used in spam messages
  6. YARA rules
  7. Written report (coming soon)

APPENDICES

SPECIFIC, TECHNICAL DETAILS NOT OF GENERAL INTEREST

RELEVANT TTP

MITRE ATT&CK Category	Description
T1589.001	Gather Victim Identity Information: Credentials
T1110.004	Brute Force: Credential Stuffing
T1586.001	Compromise Accounts: Social Media Accounts
T1204.001	User Execution: Malicious Link
T1090.002	Proxy: External Proxy
T1622	Debugger Evasion
T1585.001	Establish Accounts: Social Media Accounts

TOOLS USED

- OpenCTI threat intelligence platform
- DuckDuckGo (better results than Google)
- RiskIQ/Passive Total (now owned by Microsoft)
- AlienVault OTX