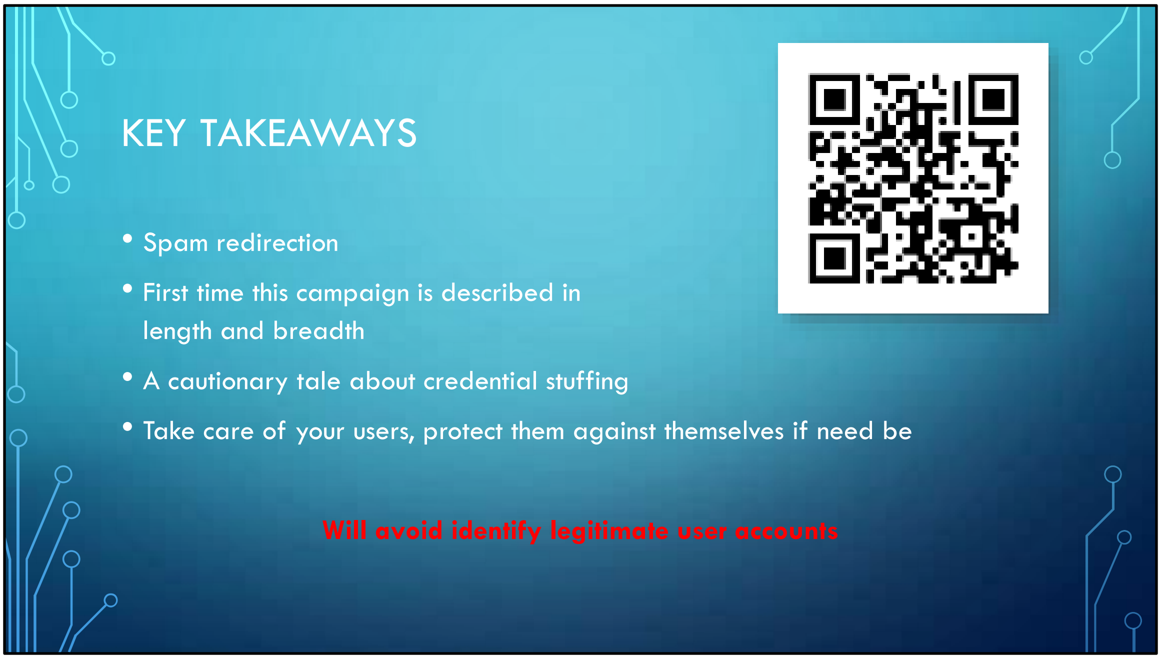
THE POD PEOPLE: DRIVING USER TRAFFIC VIA SOCIAL NETWORKS

COURTNEY FALK

WHO AM I?

- 15+ years information security experience
  - Spread across government, academia, and private industry
- CERIAS Ph.D.
- Principal software engineer at GoDaddy
- (All research for this report was done independently)



KEY TAKEAWAYS

- Spam redirection
- First time this campaign is described in length and breadth
- A cautionary tale about credential stuffing
- Take care of your users, protect them against themselves if need be

Will avoid identify legitimate user accounts

POD PEOPLE

- Threat hunting
  - 1 man
  - 0 dollars
  - Little to no cooperation
- First time assembling multiple pieces
  - DeviantArt users identified a portion
  - Some indicators floating around in threat intel databases

Donald Sutherland in Invasion of the Body Snatchers (1978).

DISCOVERING THE PROBLEM

Notifications

[redacted] [illegible]

[redacted] [redacted] [illegible]

[redacted] [illegible]

[redacted] [illegible]

[redacted] [illegible]

[redacted] [illegible]

[illegible]

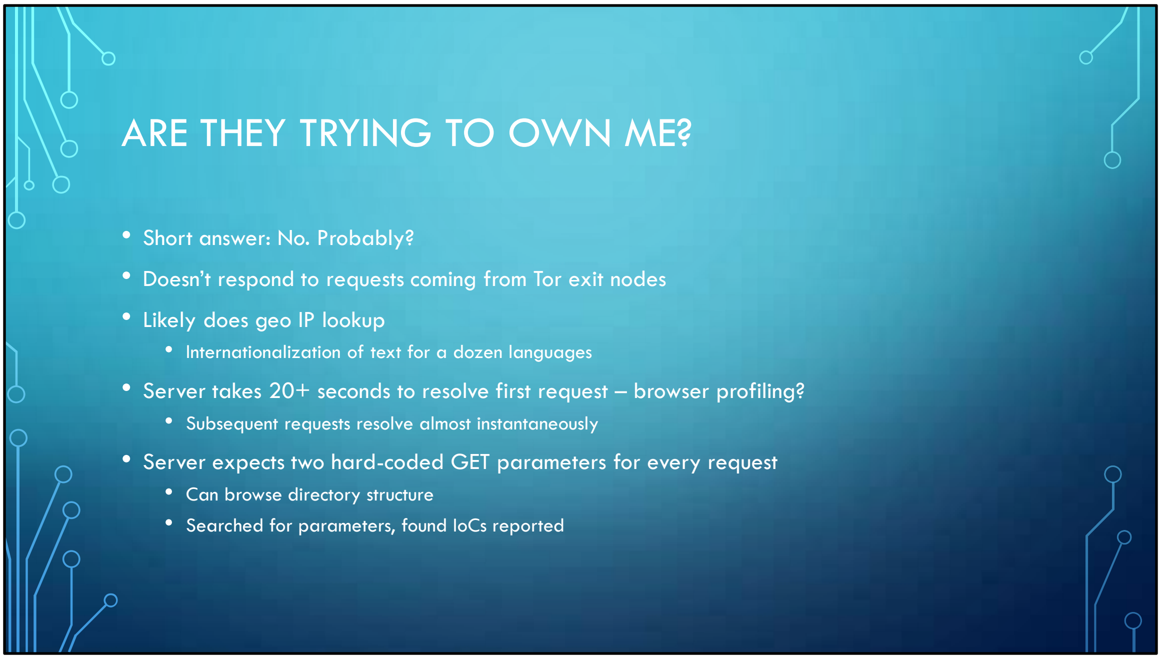
- Browsing Goodreads
- A stranger liked one of my status updates
- Then another stranger liked another update
- My interest was piqued

QUESTION #1: BOTS OR HUMANS?

- Are these bots? Trolls? Legit users?
  - Could be sold for profit
- Wide variety of data in the affected profiles
  - Too much work to backstop
- Conclusion: These were legitimate user accounts taken over and used for bots

The red boxes censor the same text string in two locations. One location is as a part of the user profile URL for Goodreads, and the other is as the subdomain to okkl[.]ru.

I attempted to contact this user and others to get more detailed information. No one responded.

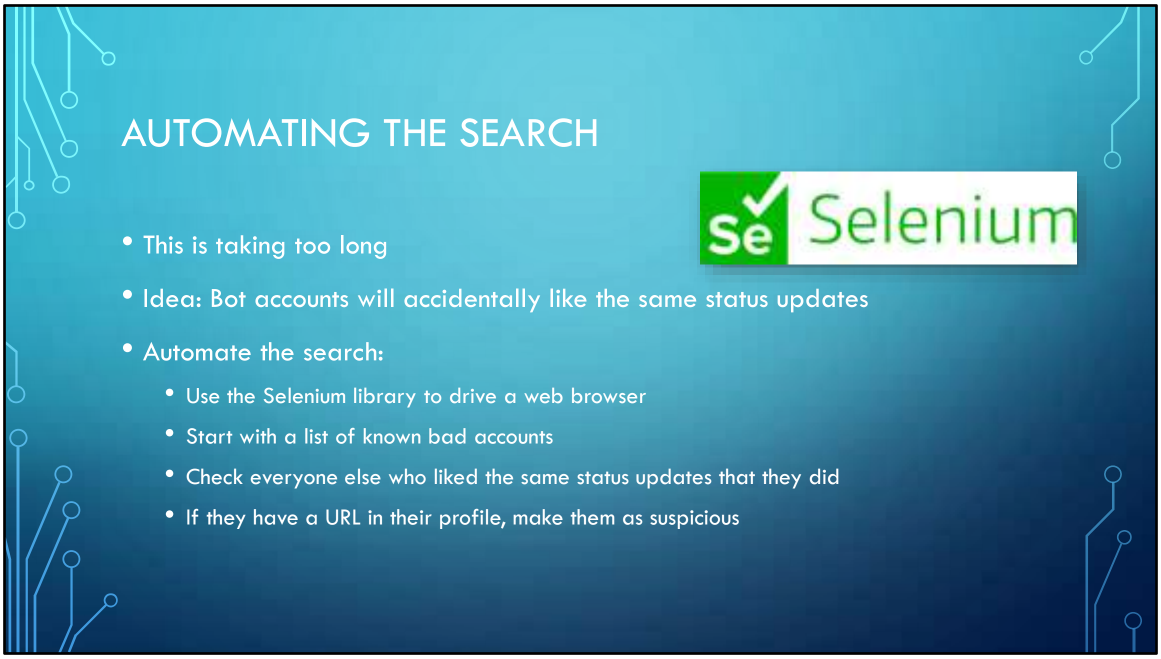


ARE THEY TRYING TO OWN ME?

- Short answer: No. Probably?
- Doesn’t respond to requests coming from Tor exit nodes
- Likely does geo IP lookup
  - Internationalization of text for a dozen languages
- Server takes 20+ seconds to resolve first request – browser profiling?
  - Subsequent requests resolve almost instantaneously
- Server expects two hard-coded GET parameters for every request
  - Can browse directory structure
  - Searched for parameters, found IoCs reported

Thanks to the Any.Run tool for testing the web page in a secure and free manner.

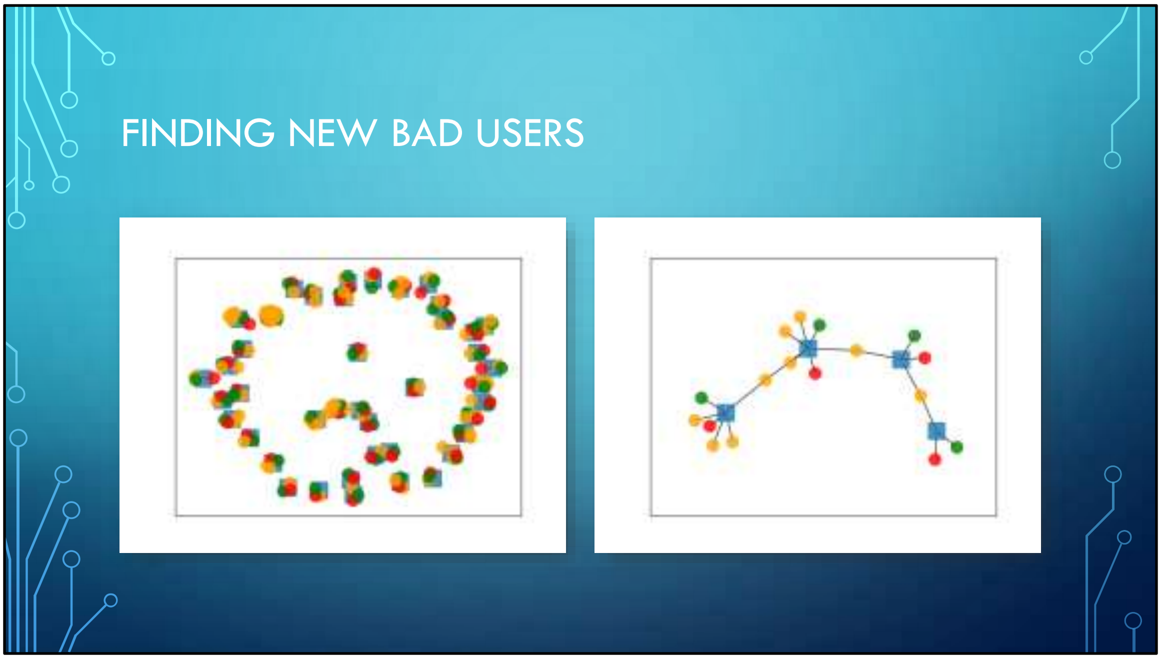
Originally redirect to your-datingspace2[.]com, which labeled itself as “DirtyTinder”.



AUTOMATING THE SEARCH

Se Selenium

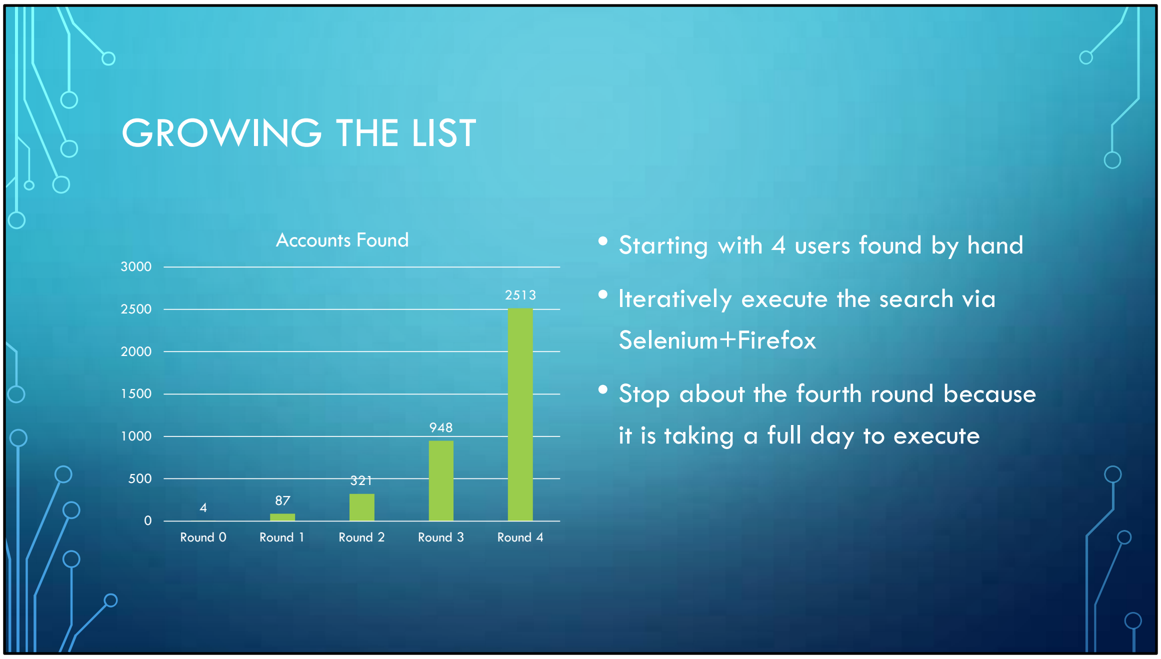
- This is taking too long
- Idea: Bot accounts will accidentally like the same status updates
- Automate the search:
  - Use the Selenium library to drive a web browser
  - Start with a list of known bad accounts
  - Check everyone else who liked the same status updates that they did
  - If they have a URL in their profile, make them as suspicious



FINDING NEW BAD USERS

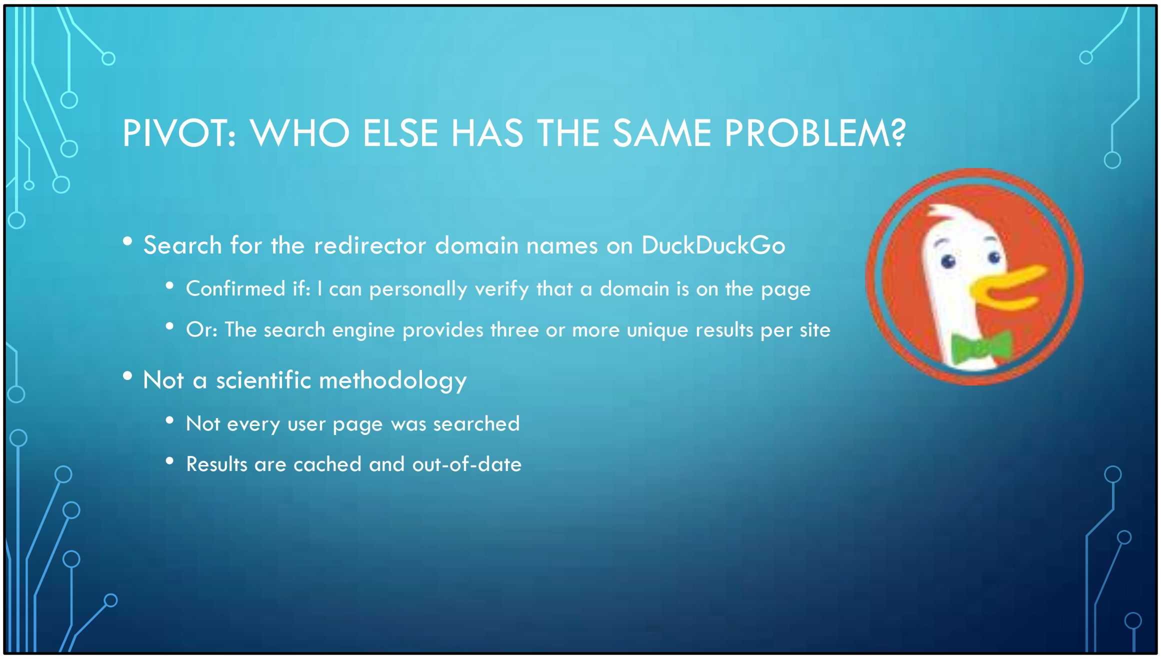
Legend:

- Blue square: Status update
- Green circle: Known good user (status poster)
- Red circle: Known bad user (redirection link found)
- Yellow circle: Suspect user



GROWING THE LIST

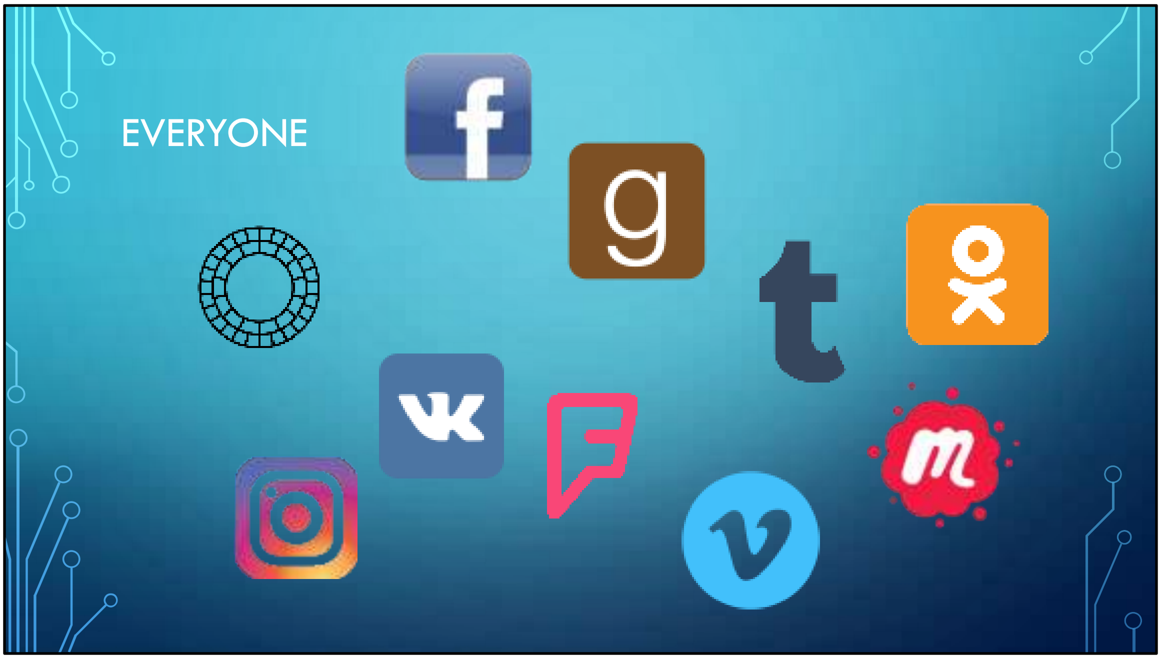
- Starting with 4 users found by hand
- Iteratively execute the search via Selenium+Firefox
- Stop about the fourth round because it is taking a full day to execute



PIVOT: WHO ELSE HAS THE SAME PROBLEM?

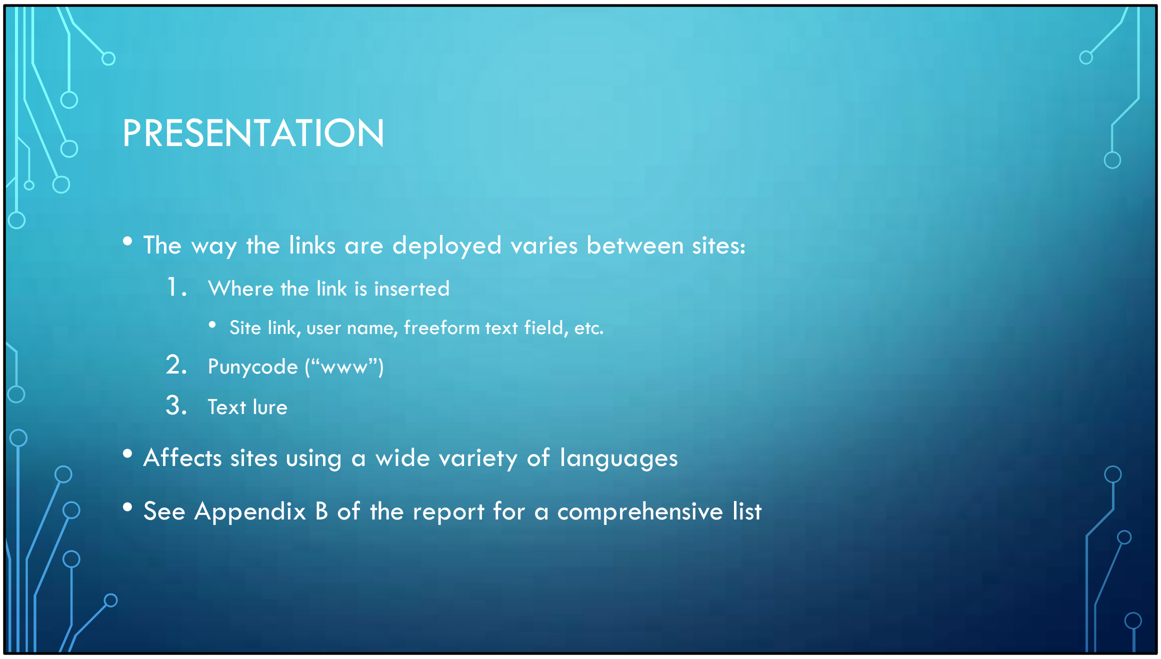
- Search for the redirector domain names on DuckDuckGo
  - Confirmed if: I can personally verify that a domain is on the page
  - Or: The search engine provides three or more unique results per site
- Not a scientific methodology
  - Not every user page was searched
  - Results are cached and out-of-date

You can also find affected accounts using unique/distinct words gathered from the text lures.



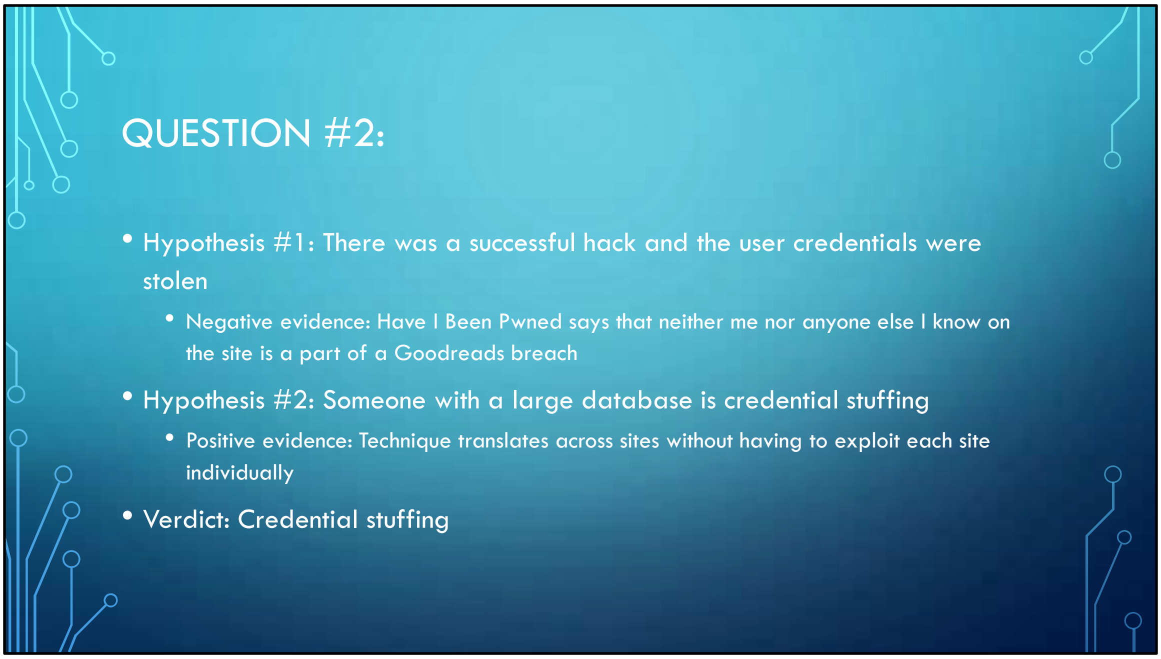
EVERYONE

Found over 70 different sites affected, not including sites that only repackage data, or WordPress blogs.



PRESENTATION

- The way the links are deployed varies between sites:
  1. Where the link is inserted
     - Site link, user name, freeform text field, etc.
  2. Punycode (“www”)
  3. Text lure
- Affects sites using a wide variety of languages
- See Appendix B of the report for a comprehensive list

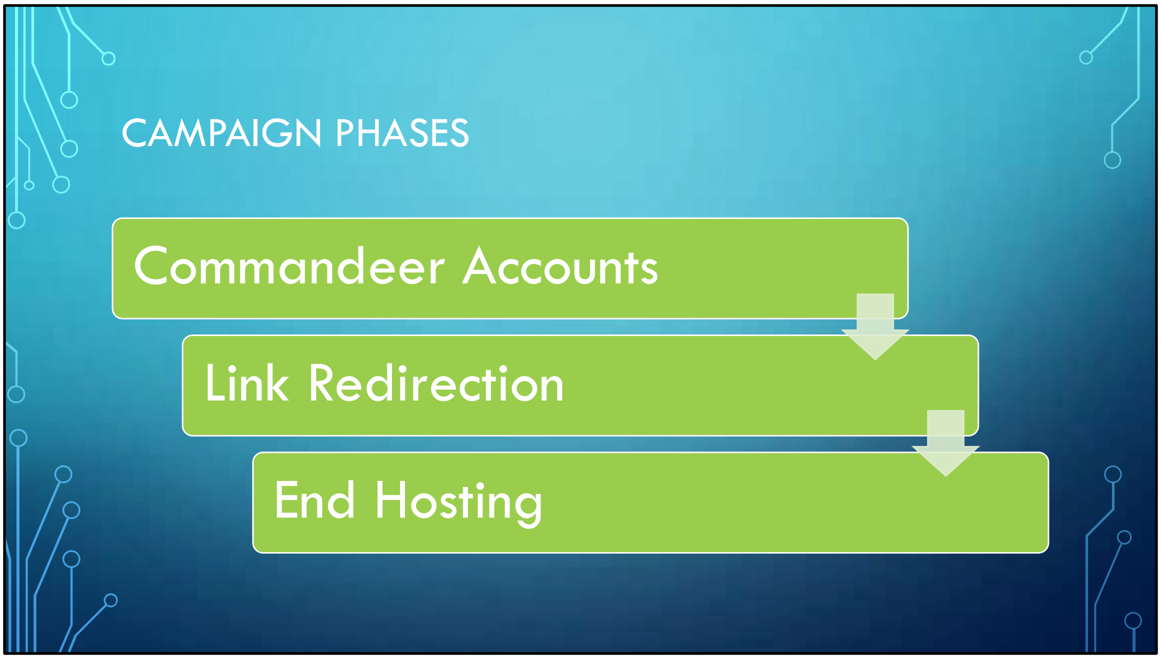


QUESTION #2:

- Hypothesis #1: There was a successful hack and the user credentials were stolen
  - Negative evidence: Have I Been Pwned says that neither me nor anyone else I know on the site is a part of a Goodreads breach
- Hypothesis #2: Someone with a large database is credential stuffing
  - Positive evidence: Technique translates across sites without having to exploit each site individually
- Verdict: Credential stuffing

Have I Been Pwned: https://haveibeenpwned.com/

Credential stuffing attacks can expect a 0.5% success rate. Goodreads has a reported 90 million users.



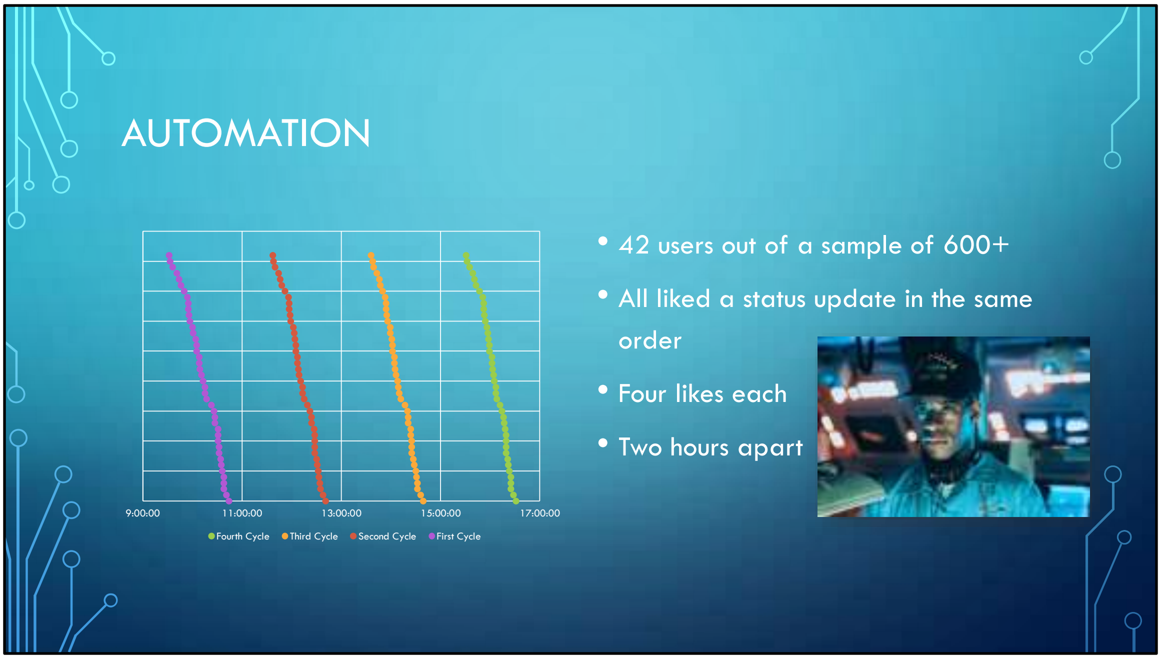
CAMPAIGN PHASES

Commandeer Accounts

Link Redirection

End Hosting

It may be safer to assume that there are three different threat actor groups operating in concert/cooperation.



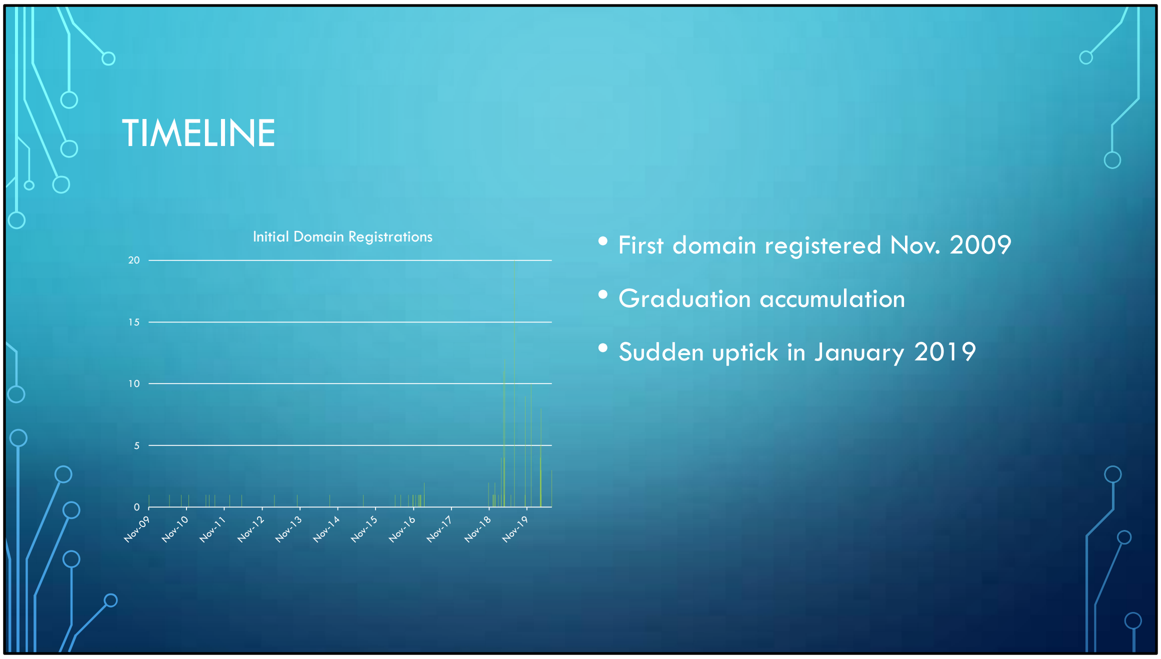
AUTOMATION

- 42 users out of a sample of 600+
- All liked a status update in the same order
- Four likes each
- Two hours apart

Found a set of 42 users whose status likes followed a strict sequence.

The vertical axis doesn’t represent anything. It is only there to demonstrate the separation between the individual events.

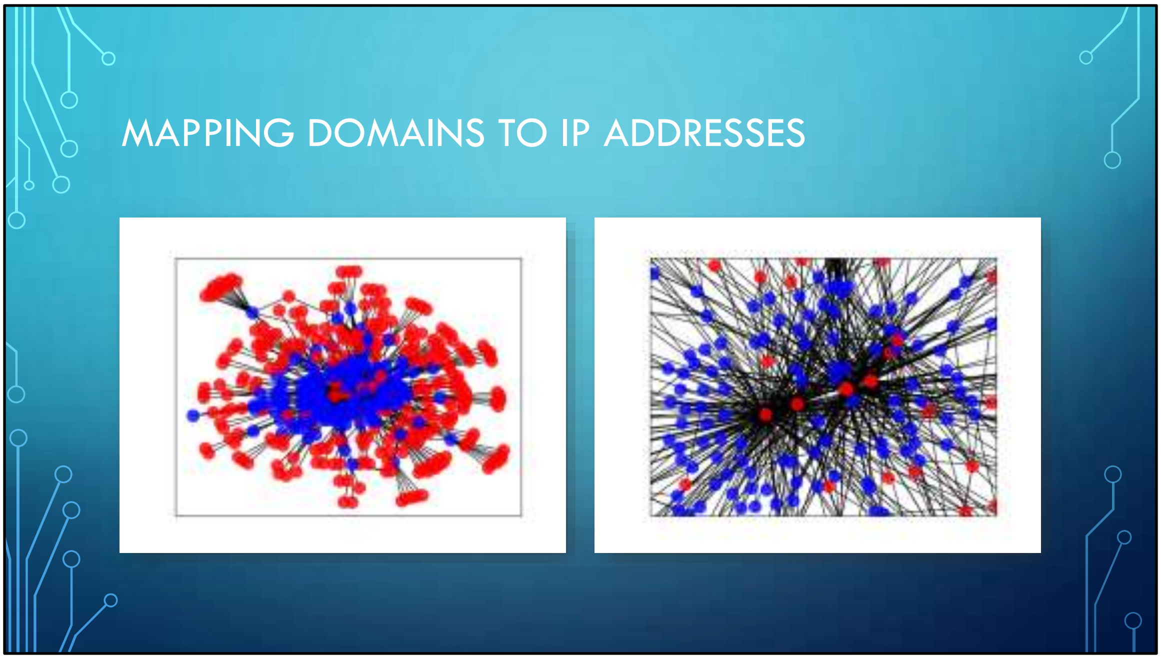
Courtney B. Vance from The Hunt for Red October (1990).



TIMELINE

- First domain registered Nov. 2009
- Graduation accumulation
- Sudden uptick in January 2019

Notice the gap from early 2017 through late 2018.



MAPPING DOMAINS TO IP ADDRESSES

Left is all mappings. Right is a focused view of the center. Blue are domain names, red are IP addresses.

Notice how some domains switch to many address, while some addresses are used by several domains.

CHANGES OVER TIME

[redacted] [redacted]

2 500 6

[redacted]のブックマーク (2)

http://[redacted] [illegible]

[redacted]

[redacted]

[illegible]

http://[redacted] [illegible]

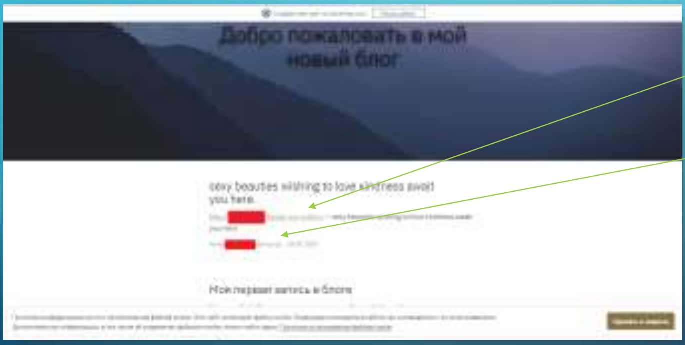
[redacted]

[redacted]

[illegible]

- Some profiles get updated/changed redirection links
- Redirection links change their target sites over time
- Some sites remediate affected accounts
- Some users appear to reclaim their accounts

MULTIPLE CAMPAIGN PHASES?



Добро пожаловать в мой новый блог

sexy beauties wishing to love kindness await you here.

[illegible] [redacted] [illegible]

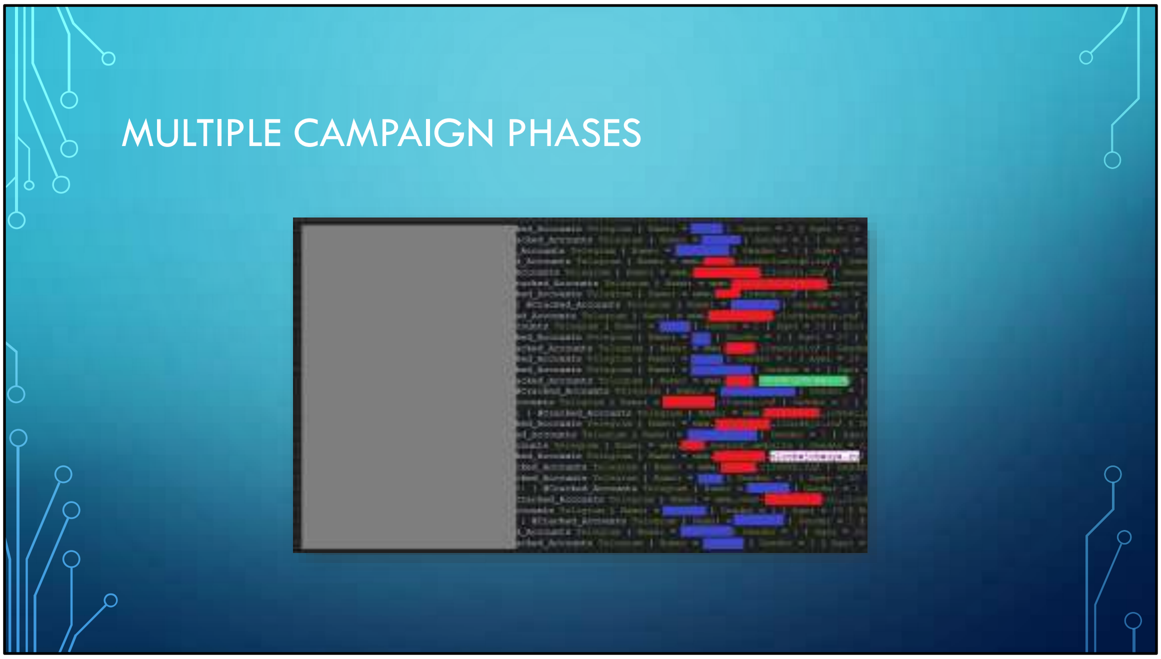
[illegible] [redacted] [illegible]

Моя первая запись в блоге

Redirection URL

Account Name

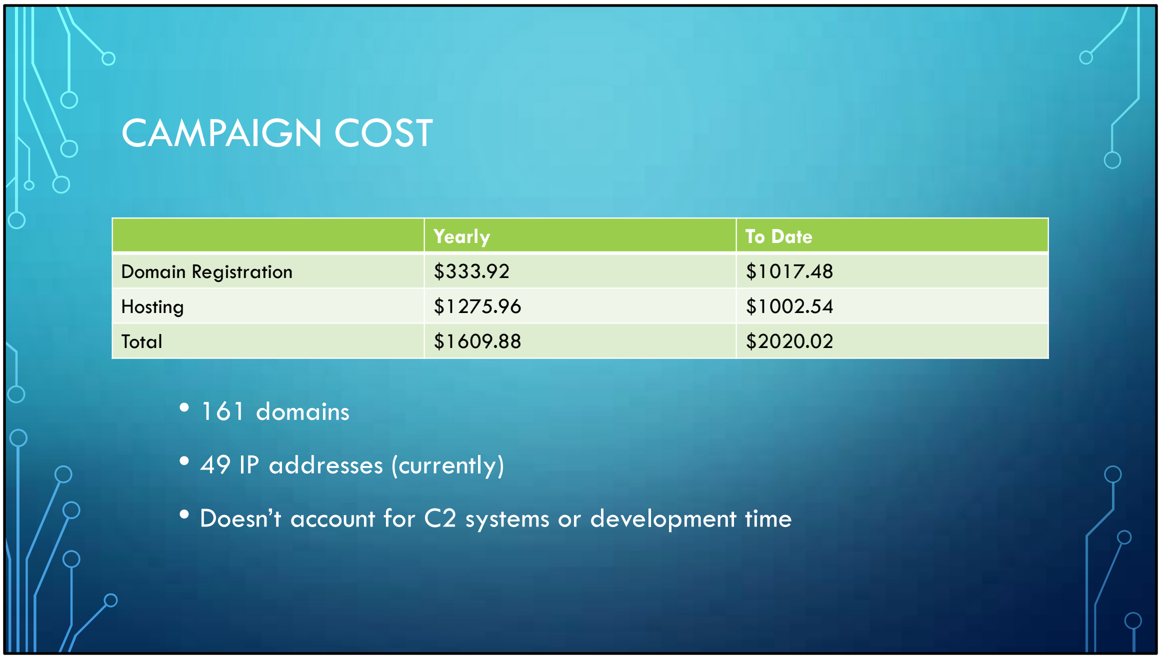
The account name is already a URL, meaning it was changed in a prior phase, re-found, then used as a new subdomain…



MULTIPLE CAMPAIGN PHASES

Telegram breaches:

- March 2020 – misconfigured third-party cloud storage
- June 2020 – software vulnerability

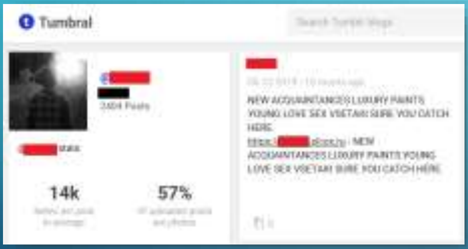


CAMPAIGN COST

	Yearly	To Date
Domain Registration	$333.92	$1017.48
Hosting	$1275.96	$1002.54
Total	$1609.88	$2020.02

- 161 domains
- 49 IP addresses (currently)
- Doesn’t account for C2 systems or development time

SITES WITHIN SITES



Tumbral

[redacted]

[redacted]

3404 Posts

[redacted]stats

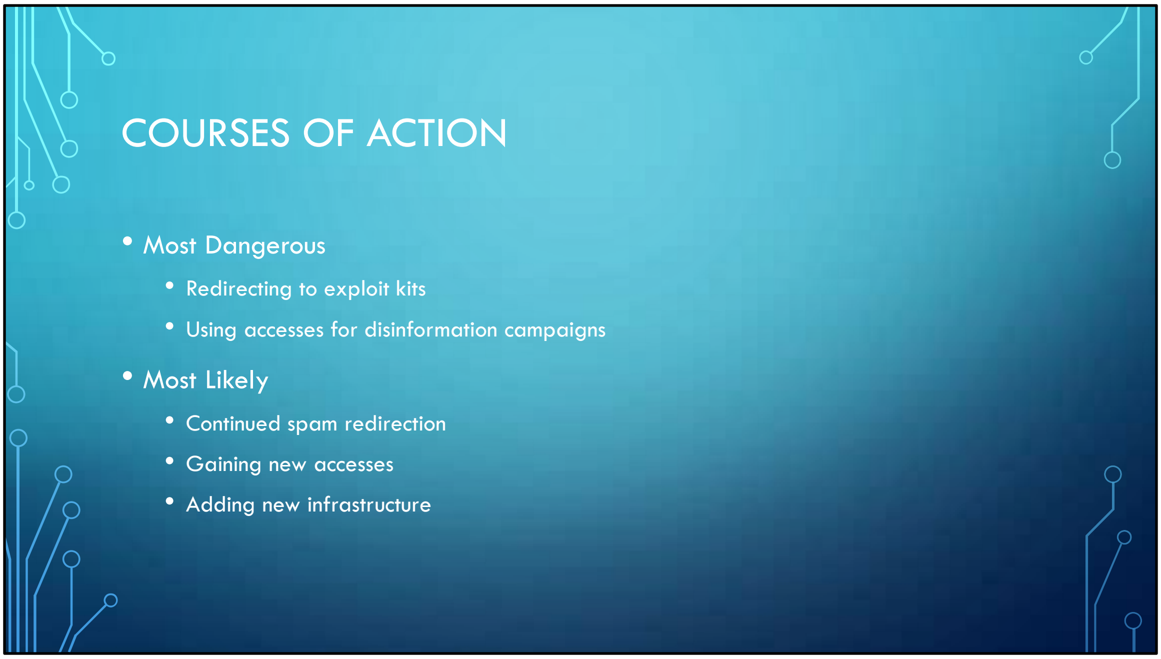
14k

57%

[redacted]

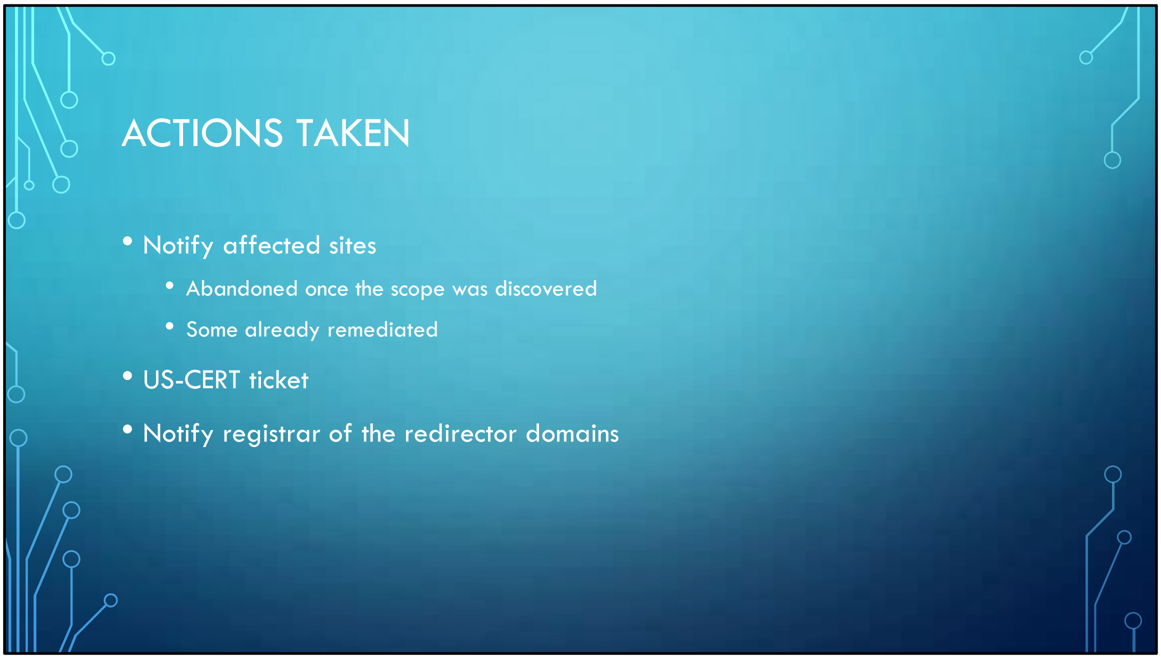
NEW ACQUAINTANCES LUXURY PAINTS YOUNG LOVE SEX VSETAKI SURE YOU CATCH HERE.
https:[redacted].ru · NEW ACQUAINTANCES LUXURY PAINTS YOUNG LOVE SEX VSETAKI SURE YOU CATCH HERE

- Some site embed data from social networks
  - Tumblr
  - FourSquare
  - Gravatar
- They inadvertently embed these attacks



COURSES OF ACTION

- Most Dangerous
  - Redirecting to exploit kits
  - Using accesses for disinformation campaigns
- Most Likely
  - Continued spam redirection
  - Gaining new accesses
  - Adding new infrastructure



ACTIONS TAKEN

- Notify affected sites
  - Abandoned once the scope was discovered
  - Some already remediated
- US-CERT ticket
- Notify registrar of the redirector domains

ATTRIBUTION

[redacted]

[redacted] .xyz

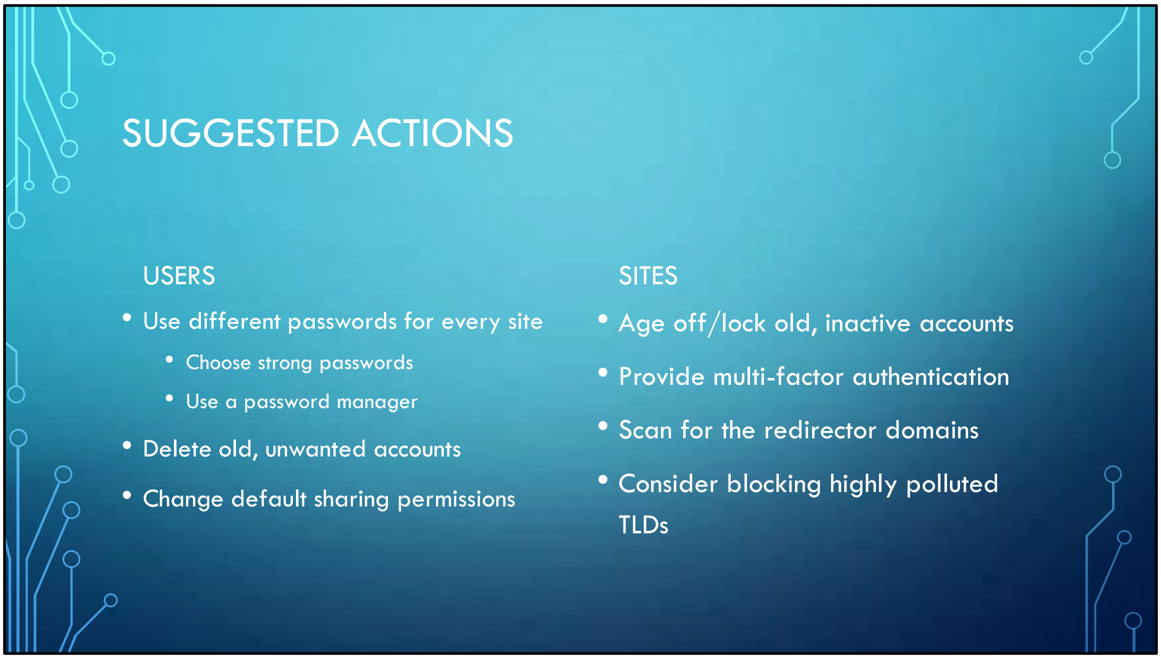
www.[redacted] .xyz – [illegible]

- HIGH: Russian language speakers
  - Use of Russian-language registrars and hosting
  - Russian language posts and Cyrillic characters
- MODERATE: Russian nationals

WORDPRESS ATTACKS

- “New” development not covered in the original report
- Attackers compromise WordPress hosting and set up redirections
  - Possibly also setting up phony WordPress sites
- Overlapping attacker infrastructure with Pod People
  - Possibly related (yet to be determined)

Look for more information in a future report.



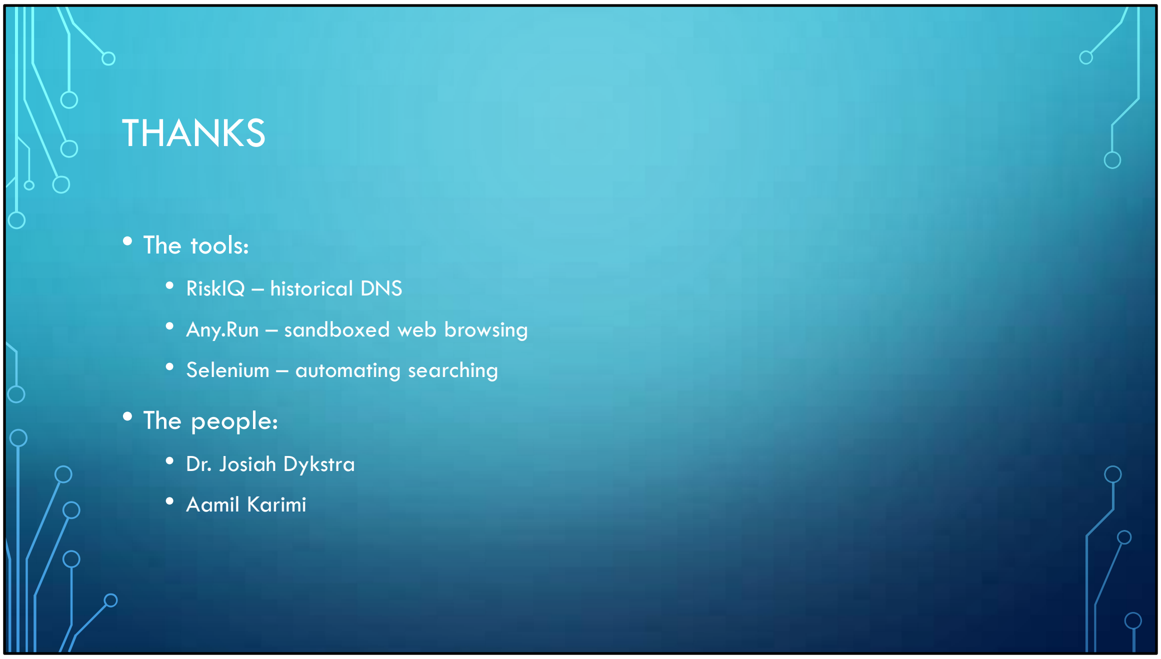
SUGGESTED ACTIONS

USERS

- Use different passwords for every site
  - Choose strong passwords
  - Use a password manager
- Delete old, unwanted accounts
- Change default sharing permissions

SITES

- Age off/lock old, inactive accounts
- Provide multi-factor authentication
- Scan for the redirector domains
- Consider blocking highly polluted TLDs



THANKS

- The tools:
  - RiskIQ – historical DNS
  - Any.Run – sandboxed web browsing
  - Selenium – automating searching
- The people:
  - Dr. Josiah Dykstra
  - Aamil Karimi

Q & A

- https://github.com/podpeople/podpeople
- podpeople <at/> infimach <dot/> com