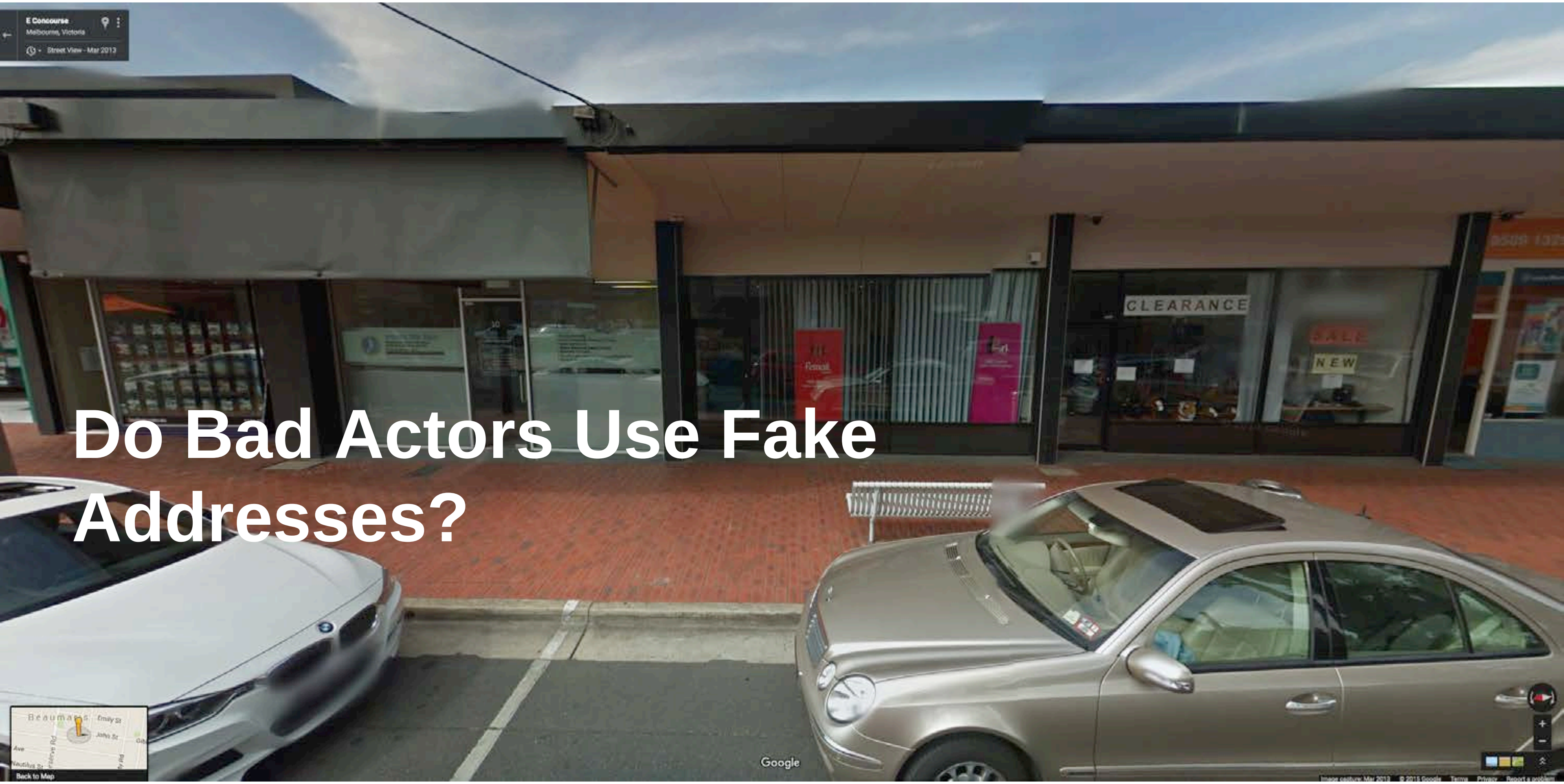
Using Domain Name Registrant Information To Identify Malicious Domains

Mark Langston

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Do Bad Actors Use Fake Addresses?



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003089

Secrecy, and Finding What’s Hidden

“Secrecy is a way of organizing institutions and human activity to render them invisible.”

“Secrecy is self-contradictory; because what is made secret exists in the world, it is visible.”

Trevor Paglen, artist (“Six Landscapes”. Chaos Communication Congress, 2013)

The Problem With WHOIS Data

- Not all in one place.
- Whois API, LLC
- Not all ccTLDs
- Not all TLDs (e.g., .edu, .mil)
- 162 million records
- 2015, Q2
- 238GB

What Constitutes a Bad Actor?

- Phishing domain blacklist
- June 2015
- Hosts-file.net (Malwarebytes)
- 734,428 unique fully-qualified domain names
- 103,658 unique domains

The Address That Started It All

Gazetny Lane Bldg. 1 17 9 125009 Moscu Rusia
125009 RUSSIAN FEDERATION
petrdeitalia@post.cz Petr Abandonato

The Address That Stoked The Flames

Ilyinka Street 23, Moscow 103132, RUSSIAN FEDERATION
the.malware.cabal@gmail.com, Spy Eye

Diving in!

- Hadoop, Spark (PySpark)
- Only 58% of phishing domains found in WHOIS data
- Half of the remaining are in TLDs for which there was no data
- Three most frequent: .tk (4,612), .ru (4,384), .co.uk (2,716)
- Leaving 20,309 that just weren’t found.

Diving in! Registrars!

- GoDaddy the most frequent registrar (23.9%)
- eNom (13.4%)
- Network Solutions (5.3%)
- Publicdomainregistry.com, name.com, Tucows, Soluciones Corporativas IP (12.1%)

Then…

…things started to go wrong.

Privacy Services

- 17,551 domains used some form of privacy protection.
- Another 2,960 had no registrant information.
- Rendering opaque 34% of the domains for which we have data.

Repossession

- 625 domains (mostly GoDaddy) were listed as “Repossessed”.
- Another 217 (all eNom) were in a “reactivation period”.

Repossession (cont.)

- 395 domains registered to gbclaw.net.
- Another 963 registered to MarkMonitor
- 52 registered to Stephen Gaffigan
- 34 to CitizenHawk

Resellers

- 181 registered to Frank Schilling/Name Administration Inc BVI.
- 408 to New Ventures Services Corp.

Rogue Registrars

- 204 only info is BIZCN.COM, INC
- Linked to illegal internet pharmacies (Huffington Post, 11/7/14; Wall Street Journal, October 27, 2014)
- Found in breach of ICANN accreditation agreement May 8, 2014

Rypo…er, Typosquatters

- 415 registered to Nadeem Qadir (e.g., travelasity.com)
- 325 Bladimir Boyiko (e.g., wwwpbs.org)
- Both use 2006.nip.net email address

Other Suspicious Activity

- 220 registered to GDS Licensing
- Associated with illegal import of fake cancer drug Avastin in 2013
- Several domains checked with legitscript.com listed as “rogue” pharmacies.

More Suspicious Activity

- Harjanti Chandra
- 1,321 unique domains
- All in the .info gTLD
- Appear related to popular mobile app downloads
- Websites hosted in Hanoi, Vietnam
- Registrant in Indonesia

Conclusions

Conclusions

- Registrant information mining is difficult – no standards for field entries, even within an entity
- WHOIS Privacy services present a barrier to analysis
- There are entities whose names may be worthy of a priori filtering – but identifying those entities is time-consuming, often subjective, and largely manual
- The legal aspect of domain name ownership does not always keep pace with usage – malicious activity may extend beyond ownership changes, or begin before legal proceedings can start
- Fake address “watering holes” do not seem to be prevalent, or even common.

Contact Information

Presenter / Point of Contact

Mark Langston

Member of Technical Staff

Telephone: +1 412.268.1942

Email: mclangston@sei.cmu.edu