IDN Homographs

ASCII Look-alikes vs IDN Homographs

- ASCII Look-alike: One of two or more **ASCII** strings that appear identical or very similar
- Solutions exist for detecting some ASCII look-alikes that do not exist for IDN Homographs

acme.example

acrne.example

IDN Homographic Attacks

- Humans are really good at pattern recognition
- Many glyphs originating from the Unicode repertoire look similar or even identical to others depending on the font
- So… register an IDN that is a homograph of a well-known (usually non-internationalized) domain name
- Extort, camp, cash-park, phish, distribute malware, or do other antisocial things by using the IDN in a URL
- ???
- Profit

Examples

Real Site	Homograph	A-label
easyjet.com.	easyjeț.com.	xn--easyje-n17b.com.
delta.com.	de|ta.com.	xn--deta-1kb.com.
ryanair.com.	ryanaiṛ.com.	xn--ryanai-1x7b.com.
poloniex.com.	polonìex.com.	xn--polonex-3ya.com.
bittrex.com.	bītt’rex.com.	xn--btrex-m3a12b.com.
linkedin.com.	lìnkedin.com.	xn--lnkedin-zya.com.

Courtesy of
Mike Schiffman,
Farsight Security

Observed via Passive DNS

ƒacebook.com. ƒaceboọk.com.
ƒacebook.tk. ƒɑcebook.com.
f̈acebook.com. fácebook.com.
fàcebook.com. fâcebook.com.
fåcebook.com. fäcebook.com.
fãcebook.com. fȧcebook.com.
fącebook.com. fācebook.com.
fạcebook.com. fạcebook.com.
fàćebook.com. faĉebook.com.
fačebook.com. faċebook.com.
façebook.com. facȩbook.com.
facébook.com.

applе.com. applė.com.
âpplê.cf. ápple.com.
ăpple.com. åpple.com.
äpple.com. ąpple.com.
apṗle.com. appĺe.com.
applé.com. applè.com.
àpplè.com. applĕ.com.
ăpplĕ.com. ápplê.com.
àpplê.com. âpplê.com.
applĕ.com. applë.com.
äpplë.com. applė.com.
åpplė.com.

ñetflix.com.
n̨etflix.com.
nétflix.com.
nėtflix.com.
neṭflix.com.
netflíx.com.
netflìx.com.
netflîx.com.
netflïx.com.
netfl̨ix.com.
netflıx.com.
netƒlix.com.

ġoogle.xyz. goôgle.com.
ĝoogle.com. googĺe.com.
gọọglē.com. googlè.tk.
googlę.com. googlè.com.
googlé.com. ġoogle.com.
goơgle.com. googlè.com.
googlé.com. goơgle.com.
gooĝle.com. gooĝle.com.
gooĝle.com. gooĝle.com.
gooĝle.com. gooĝle.com.
gooĝle.com. gooĝle.com.
google.com.

bankofamerica.com. baŋkofamerica.com.
baŋkofamerica.net. bąnkofamerica.com.
bankôfamerica.com. banköfamerica.com.
bankofamerîca.com. bänkofämericä.com.
banĸofamerica.com. banĸofamerica.net.
bankofamerica.com.

wėllsfargo.com.
welŀsfargo.com.
wellsfárgo.com.
wellsfårgo.com.
wellsfargó.com.
wellsfargọ.com.
wellsfargo.com.

çhase.com.
chàse.com.
chäse.com.
chasé.com.
chasë.com.
chɑse.com.
chase.com.

Courtesy of
Mike Schiffman,
Farsight Security

Observed in the Wild

- 1,936 impersonation domains observed in a review of Certificate Transparency logs (2017) [1]
- Farsight January 2018 research [2]
  - Examined 125 brand names
  - In a 3 month period observed 116,113 homographs
  - Discovered 10+ live phishing sites
  - 382 impersonation domains reported from Passive DNS logs

[1]: https://github.com/CyberMonitor/defcon-25-Packet-Hacking-Village/blob/master/YOU'RE%20GOING%20TO%20CONNECT%20TO%20THE%20WRONG%20DOMAIN%20NAME%20phv2017-serb.pdf
[2]: https://www.farsightsecurity.com/2018/01/17/mschiffm-touched_by_an_idn/

Observed in the Wild (cont)

- Farsight October 2018 research [3]
  - Examined 509 brand names
  - In a 20 month period observed 11,766 unique IDN homographs
  - In same period observed 61,443 total IDNs
    - 20% in banking/finance
    - 52% in .com
    - 68% geolocate to the USA
    - 93% using IPv4

Data courtesy of Mike Schiffman, Farsight Security

What We've Seen: All The IDNs

161,935,465 total IDN observations

34,460,574 total unique IDNs

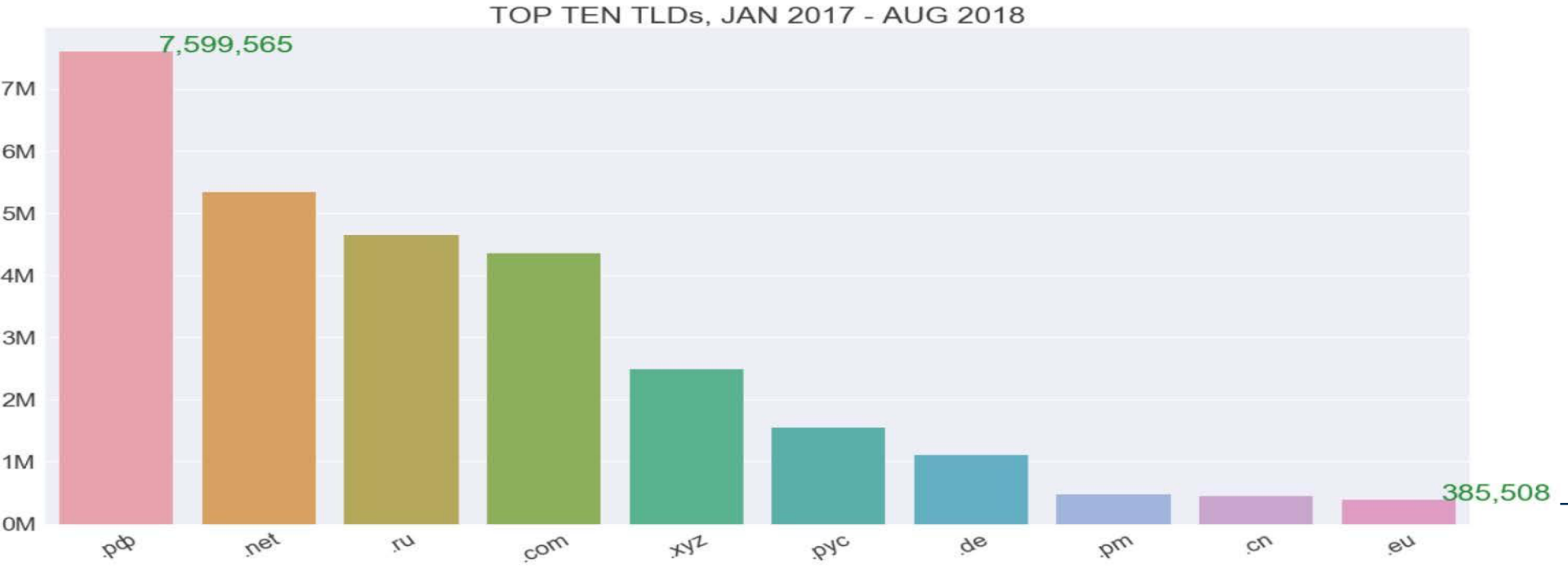
Summer vacation?

Diagram courtesy of Mike Schiffman, Farsight Security

What We've Seen: Top 10 IDN TLDs

1,675 total unique TLDs

Diagram courtesy of Mike Schiffman, Farsight Security

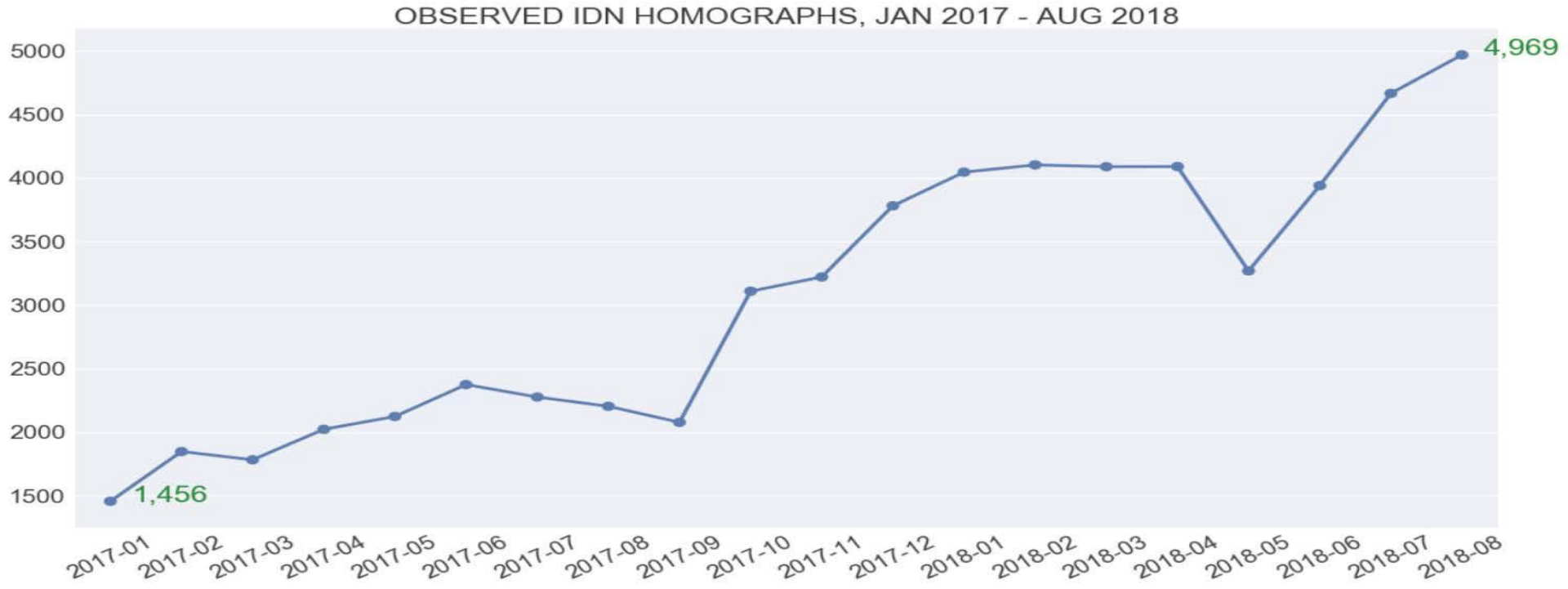


What We've Seen: IDN Homographs

61,443 total IDN homograph observations

11,766 total unique IDN homographs

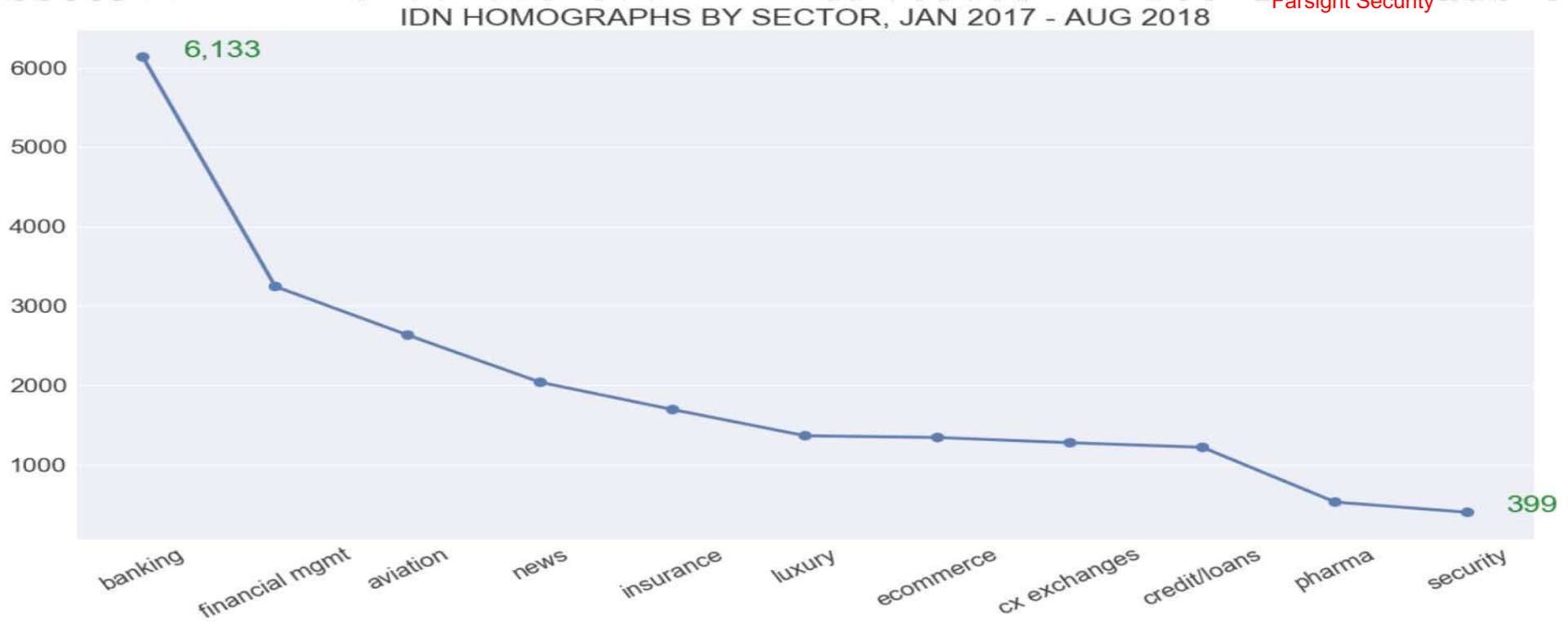
Diagram courtesy of Mike Schiffman, Farsight Security



What We've Seen: IDN Homographs by Sector

Of the 61,443 total IDN homograph observations,
20% are in banking/finance

Diagram courtesy of
Mike Schiffman,
Farsight Security



Detection and Mitigation

How to Detect Attacks

- Monitor certificate transparency logs
- Monitor DNS zone files
- Utilize passive DNS services
- Detecting IDN homographs reliably typically requires human eyes

Mitigation

- Stricter rules at registry and registrar
  - Registries and registrars implement recommendations from IDNA2008 (RFC 5890-5894, specifically RFC5894)
  - Use an inclusion based process before allowing code points
    - For example, base rules on what script a code point belongs to
  - Be extremely conservative with mixed scripts within a label, and within a domain name
  - Adapt the Label Generation Rules (LGRs)
  - Mandate homographic lookup checks
- Browsers often implement homograph preventions, but with limited success

Why is this Important?

- ICANN's mission of **Security**, Stability and Resiliency of the global unique identifiers
  - Phishing, malware, malicious email
- Affects universal acceptance
  - Failure to act may result in ad-hoc blocking or other display tricks
- Business Email Compromise (BEC) is a growing problem
  - Failure to act may result in blocking of emails that use IDNs

What Can the Community do to Help?

- Opportunity for development of tools to detect IDN Homographs
  - Visualization
  - Comparison to known homographic targets
  - Facilitate brand protection
- Awareness and outreach of the potential malicious use of IDN Homographs
  - End-user awareness
  - Implementor education
  - Service provider awareness

Relevant SSAC Publications

Relevant SSAC Publications

- https://www.icann.org/groups/ssac/documents

- SAC037: Display and usage of Internationalized Registration Data Support for characters from local languages or scripts
- SAC052: SSAC Advisory on Delegation of Single-Character IDN TLDs
- SAC084: SSAC Comments on Guidelines for the Extended Process Similarity Review Panel for the IDN ccTLD Fast Track Process
- SAC088: SSAC Response to the ccNSO evaluation of SAC084
- SAC099: SSAC Response to the ICANN Internationalized Domain Name Guidelines Working Group

Thank you