Characterising the threat of unintended URLs on social media

• • •

By
Beliz Kaleli, Brian Kondracki, Manuel Egele,
Nick Nikiforakis, Gianluca Stringhinini

Research article 8
Oliver Chamberlain

Introduction

●●●

Background and motivations

Tpyos are reelly comman!

- Easy to make
- How many of us have sent something with typos without checking?
- Even come from the highest offices
- **Sometimes they result in URLs being in social media posts**

You might not think this is bad

- But opportunists WILL exploit this.

Donald J. Trump ✔
@realDonaldTrump

Despite the constant negative press covfefe

5/31/17, 12:06 AM
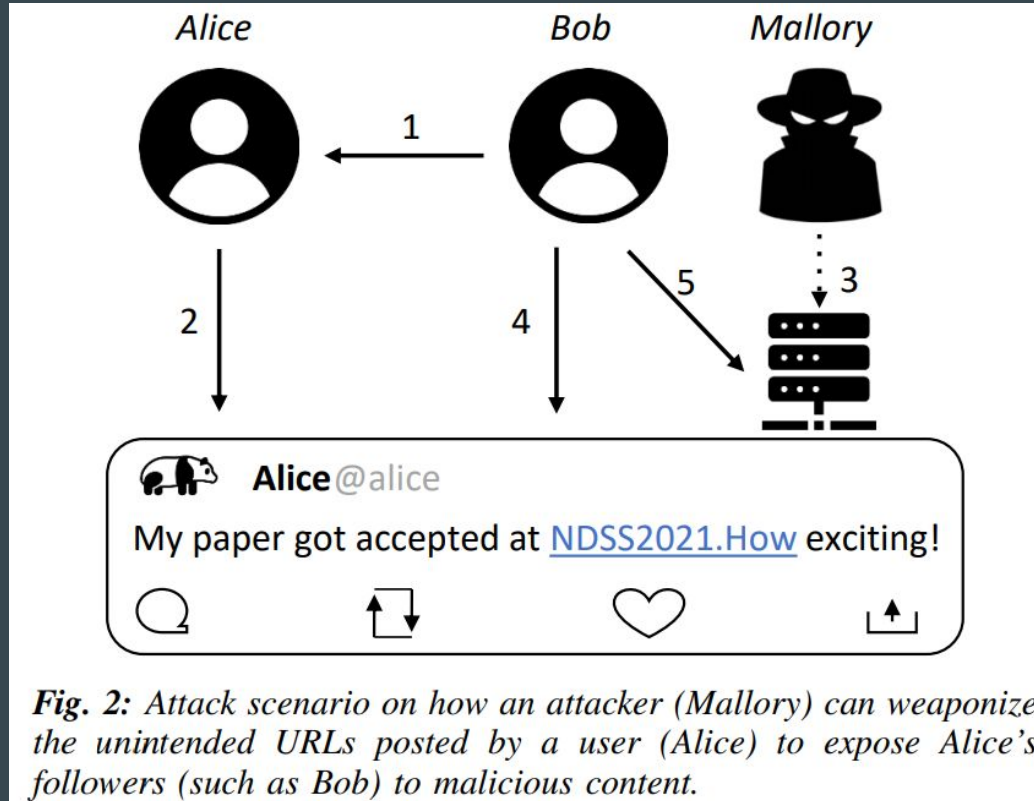
84K RETWEETS 105K LIKES

Background

- Social media platforms becoming primary form of information and communication.
- Popularity makes them perfect for malicious attacks.
- One attack vector involves the way URLs are rendered on such platforms.

Unintended URL

Any string that is typed by a user on an online service rendered to be clickable *without the user intending it to be a URL*.

Mechanics of an attack

Fig. 2: Attack scenario on how an attacker (Mallory) can weaponize the unintended URLs posted by a user (Alice) to expose Alice's followers (such as Bob) to malicious content.

From the paper

Link rendering behaviour of platforms

- User Friendliness
- Automatically render URLs
- How this happens for each site was not known
- Tested 9 popular media sites and observed rendering with 23 types of test case.

NX Test URLs	X Test URLs	Linkedin	Twitter Snapchat Whatsapp Web	Slack Facebook Whatsapp Mobile	Telegram	Skype Google Hangouts
notdomain.net	php.net	C	C	C	C	U
notdomain.Net	php.Net	C	C	C	U	U
notdomain.dev	web.dev	C	C	U	C	U
notdomain.Dev	web.Dev	C	C	U	U	U
sub.notdomain.net	windows.php.net	C	C	C	C	U
sub.Notdomain.Net	windows.Php.Net	C	C	C	U	U
sub.notdomain.dev	auth.web.dev	C	C	U	C	U
sub.Notdomain.Dev	auth.Web.Dev	C	C	U	U	U
5.net	123.net	C	C	C	C	U
5.dev	1.dev	C	C	U	C	U
www.notdomain.dev	www.web.dev	C	C	C	C	C
notdomain.notatld	-	C	U	U	U	U

TABLE I: *Unintended URL test results on different social media and messaging platforms. "U" depicts test URL is not clickable after posting whereas "C" depicts test URL is clickable after posting on the particular platform.*

From the paper

Researchers focussed on Twitter.

Extremely popular

Social media pushes messages out to wider audience than instant messaging services.

Posts are public by default

Retweeting

Threat Model

- Twitter has no spell check or punctuation, and anyone can create accounts and post tweets publicly.
- 400M tweets posted daily by users
- Onus of proper spelling falls on the user so typos in tweets are far from uncommon.
- Due to retweeting, typos in tweets of unpopular users still have the potential to be viewed by millions of users (i.e. a popular user retweets it).

Reasons for typos occuring

- Forgetting spaces between sentences
- Forgetting the space in a numbered list (i.e., 1.ITEM)
- Hitting the full stop key rather than space.

- Partly down to how fast people type and post, but also partly because many users on on mobile.

Classifier

Used Twitter Streaming API, 20M tweets

Pre-filtered down to 1068 tweets

Ground truth dataset can build classifier

94%
Accuracy

- Automated pipeline ran for 7 months using this classifier.
- Found 26,596 unintended URLs

Properties of unintended URLs

72% of unintended URLs were not registered domains

- Popular Top Level Domains (TLDs)   www.something.TLD
    - TLDs that are english words
    - i.e. *.it* which is the TLD for italy.

- URL being in middle of tweet

- URLs not being registered

Impact of an attack

- Registered 45 unregistered domains
- Traffic peaked on day of tweet and then tailed off
- Received an average of 100 hits (but some were over 700)
- 20% retweeted

- All of these hits could expose people to malicious content.

	Unintended URL	Original Author	Follower Count
NX	SEE.YOU	Harry_Styles	34M
	Kobe.Osaka	Harry_Styles	34M
	c.bank	Reuters	22M
	im.mo	9GAG	16M
	kuba.black	9GAG	16M
	raminta.art	9GAG	16M
	PERMANENTLY.MORTGAGE	iamcardib	13M
	sign.Hair	iamcardib	13M
	shake.You	iamcardib	13M
	unexpected.Love	iamcardib	13M
X	thing.It	Oprah	42M
	moment.In	deepikapadukone	27M
	people.It	iamcardib	13M
	tongue.Today	iamcardib	13M
	pregnant.My	iamcardib	13M
	street.It	JKCorden	11M
	Rt.live	TechCrunch	10M
	movie.Best	dhanushkraja	8.9M
	airbnb.To	anandmahindra	7.8M
	violence.In	marcorubio	4.2M

TABLE II: *unintended URLs with highest original author follower count.*

From the paper

Proposed Solution

● ● ●

Preventing Unintended URLs

Nature of the solution

Browser Extension would be ideal

- Applies the classifier and ML model already developed
- Non-intrusive solution
- Works cross-platform (Mac or Windows)
- Does not require specific integration with Twitter
  - Researchers assumed non-compliance from Twitter ❌

Chrome Extension

- So that's exactly what they did
- Chrome extension called TypoNoMo
- Before tweet is sent it checks the links with the ML model
- Gives the user the option to edit the tweet before sending

Benefits

✅ Non-intrusive to the user

✅ Little performance overhead

✅ Effective at getting users to look at their tweets

Criticism

●●●

What do I think?

User Testing

👦👧 User testing on volunteers would be good

- Test if there are any usability issues
- Validate the solution reduces unintended URLs

Broader scope

- Look at the issue from the POV of the user clicking on the links
  - Rather than the POV of the poster.
- Extension could analyse the links on a web page and highlight ones that may be unintended.
- Could be applied to a broader scope with extension looking for any links that may typos, spoofed etc.
- This would help with related issues such as Typo Squatting.

Thank you

• • •

Questions?

Image References

Twitter logo:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.clipartmax.com%2Fmiddle%2Fm2H7K9m2i8b1m2d3_tweet-twitter-icon-icon-chirrup-icon-icon-twitter-png-format-twitter-logo%2F&psig=AOvVaw3P38aLCZRooZI-S_0NS2jD&ust=1634033498383000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCLjrlaSPwvMCFQAAAAAdAAAAABAD

Trump image:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.businessinsider.com%2Ftrump-typos-spelling-tweets-unpresidented-2017-4&psig=AOvVaw2lyGfk6KxQeJ-Q715L7Nf1&ust=1634024459879000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCKDY1c7twfMCFQAAAAAdAAAAABAD

Italy:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.shutterstock.com%2Fsearch%2Fitaly%2Bcountry%2Boutline&psig=AOvVaw2hp1gjT2h2rgo4aqfh1eBw&ust=1634121070059000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCJi3_sPVxPMCFQAAAAAdAAAAABAS

TypoNoMo:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fndss2021.how%2F&psig=AOvVaw2FGxcl0_gx_vvJpep5HxaF&ust=1634125232887000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCOCHsIblxPMCFQAAAAAdAAAAABAI