



CISPA

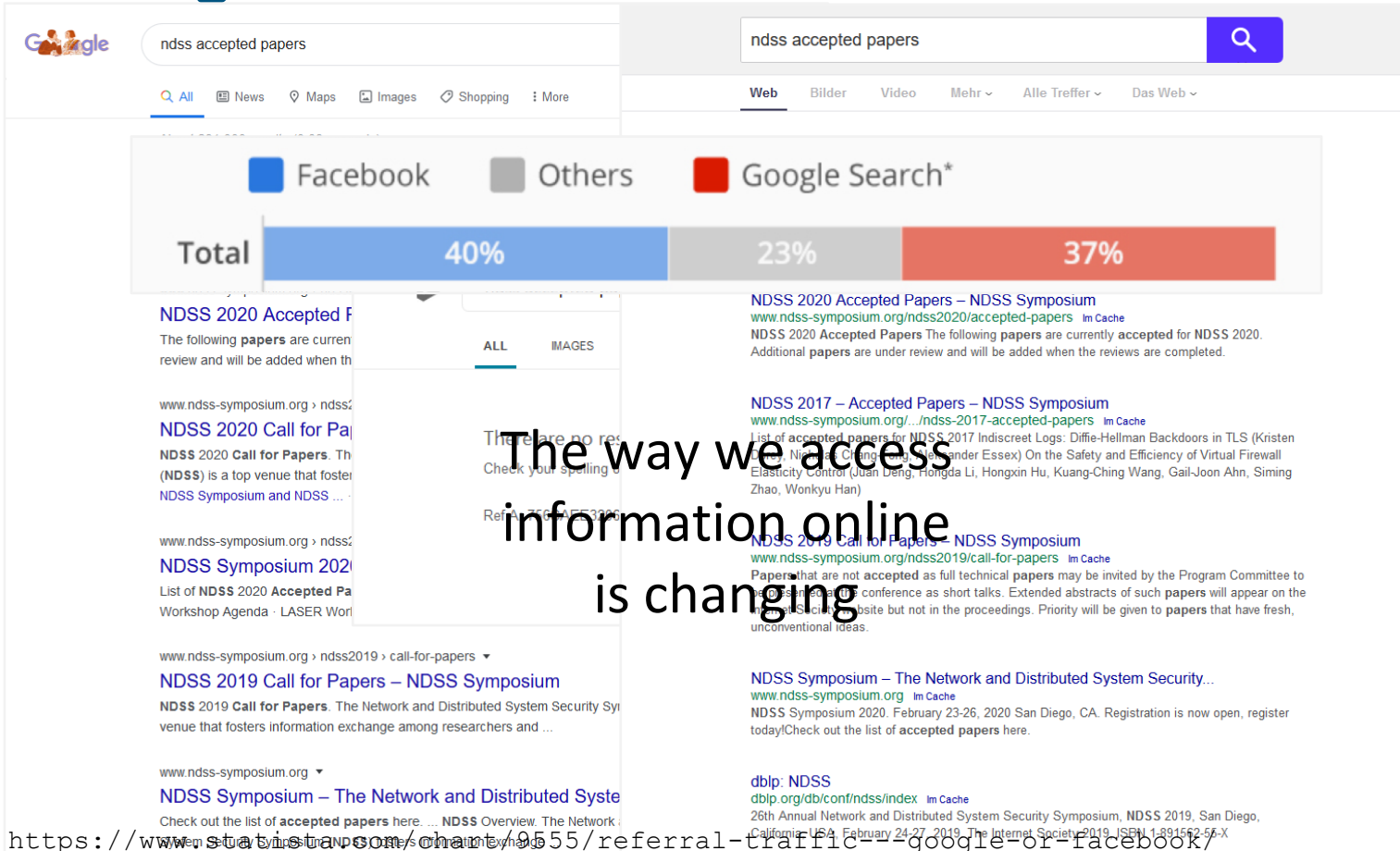
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

Deceptive Previews: A Study of the Link Preview Trustworthiness in Social Platforms

Giada Stivala and Giancarlo Pellegrino
giada.stivala@cispa.saarland

NDSS 2020 – San Diego, California, USA

Accessing information online



The screenshot shows a Google search for "ndss accepted papers". At the top, a search bar contains the query. Below it, a referral traffic chart displays the following data:

Source	Percentage
Facebook	40%
Others	23%
Google Search*	37%

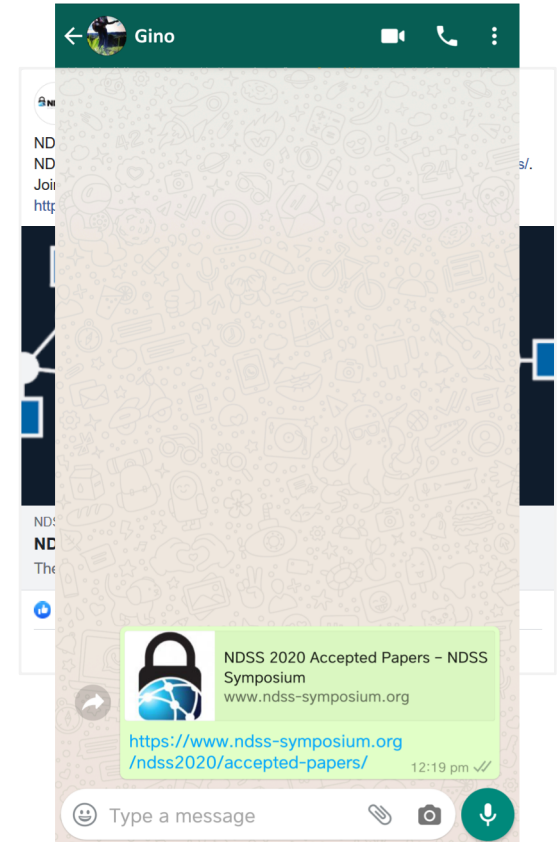
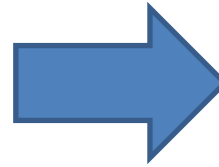
The search results include several links to NDSS 2020 and 2019 call for papers and accepted papers pages. A large text overlay is present in the center of the image:

The way we access information online is changing

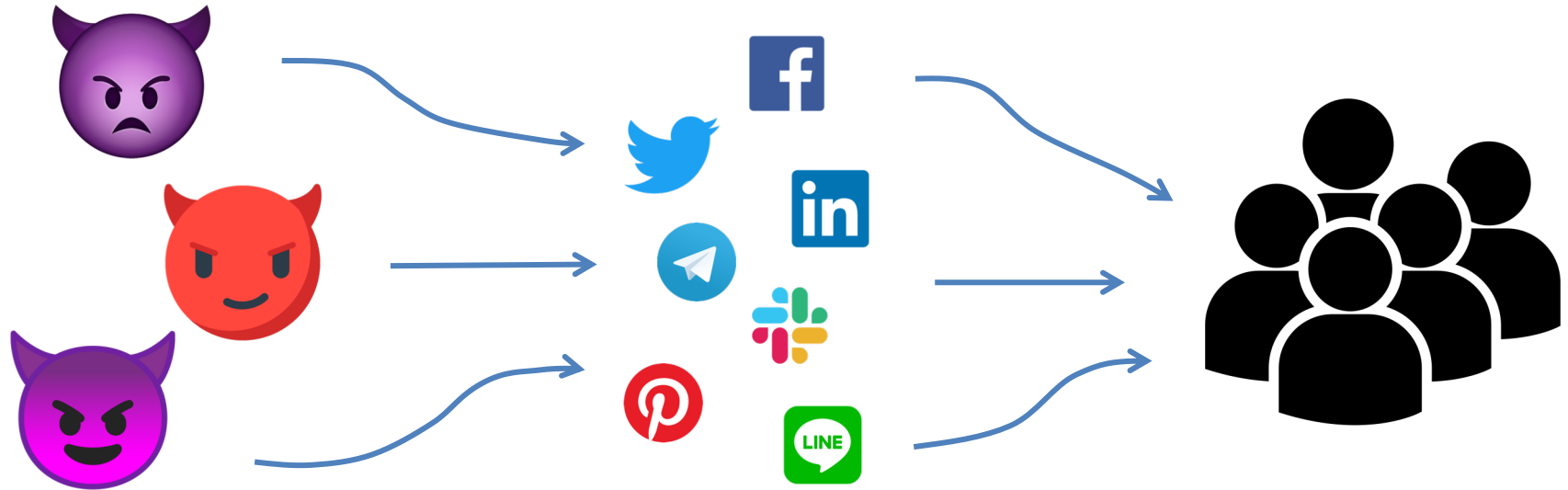
Source: <https://www.statista.com/chart/9555/referral-traffic--google-or-facebook/>

What are Link Previews?

`https://www.ndss-symposium.org/
ndss2020/accepted-papers/`



Security Risks

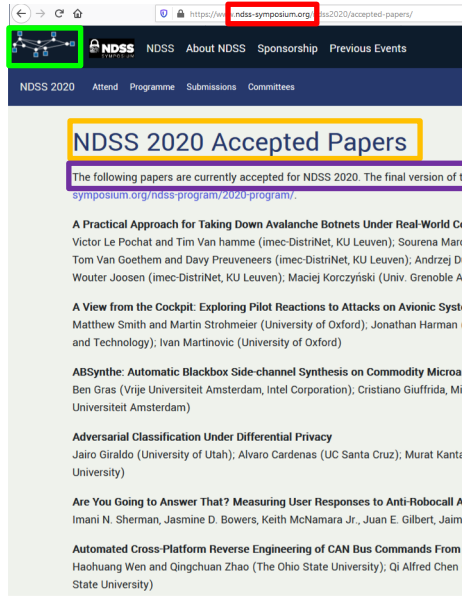


[1] Stringhini, Gianluca, Christopher Kruegel, and Giovanni Vigna. "Detecting spammers on social networks."

[2] Canali, Davide, and Davide Balzarotti. "Behind the scenes of online attacks: an analysis of exploitation behaviors on the web."

[3] Garera, Sujata, Niels Provos, Monica Chew, and Aviel D. Rubin. "A framework for detection and measurement of phishing attacks."

Link Previews



https://www.ndss-symposium.org/2020/accepted-papers/

NDSS 2020 Accepted Papers

The following papers are currently accepted for NDSS 2020. The final version of the papers will be available at <https://www.ndss-symposium.org/ndss-program/2020-program/>.

A Practical Approach for Taking Down Avalanche Botnets Under Real-World Conditions
Victor Le Pochat and Tim Van hamme (imec-DistriNet, KU Leuven); Sourena Marc Tom Van Goethem and Davy Preuveneers (imec-DistriNet, KU Leuven); Andrzej D. Wouter Joosen (imec-DistriNet, KU Leuven); Maciej Korczyński (Univ. Grenoble Alpes)

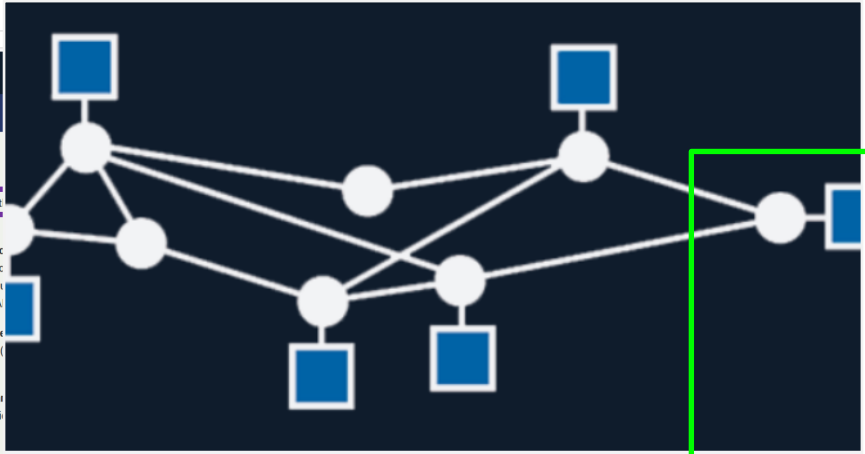
A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems
Matthew Smith and Martin Strohmeier (University of Oxford); Jonathan Harman (University of Oxford); Ivan Martinovic (University of Oxford)

ABSynthe: Automatic Blackbox Side-channel Synthesis on Commodity Microprocessors
Ben Gras (Vrije Universiteit Amsterdam, Intel Corporation); Cristiano Giuffrida, Mihai Andrusca (Vrije Universiteit Amsterdam)

Adversarial Classification Under Differential Privacy
Jairo Giraldo (University of Utah); Alvaro Cardenas (UC Santa Cruz); Murat Kanta Kurt (University of Utah)

Are You Going to Answer That? Measuring User Responses to Anti-Robocall Applications
Imani N. Sherman, Jasmine D. Bowers, Keith McNamara Jr., Juan E. Gilbert, Jaime Blazquez (University of California, Irvine)

Automated Cross-Platform Reverse Engineering of CAN Bus Commands From
Haichuang Wen and Qingchuan Zhao (The Ohio State University); Qi Alfred Chen (University of California, Irvine); Zhiqiang Lin (The Ohio State University)



NDSS-SYMPOSIUM.ORG

NDSS 2020 Accepted Papers – NDSS Symposium

The following papers are currently accepted for NDSS 2020. Additional

Misuse of Link Previews

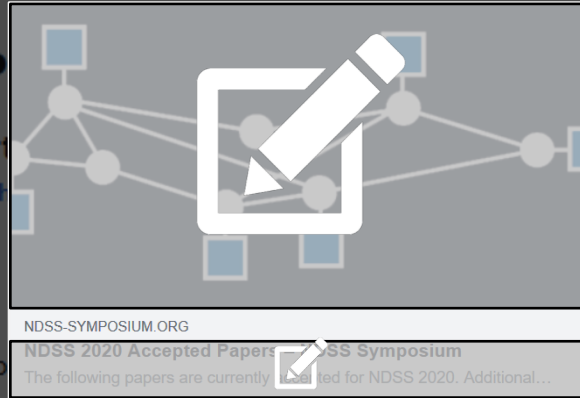
Modifying Link P



Matthew Robert

Business Tools · Publish

June 28, 2017



As part of our continuing effort

earlier this year at F8 we announced an important change to our Graph API: Graph API version 2.9 includes a 90 day deprecation of the ability to edit previews attached to link posts. We'd like to share more details on the coming change.

false news on our platform,

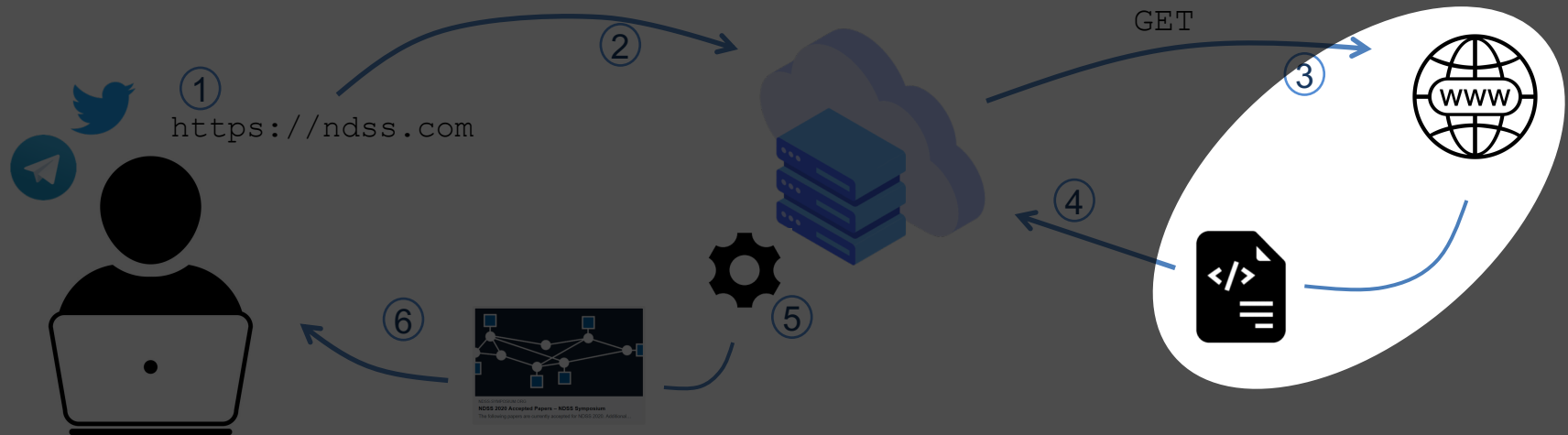
By removing the ability to customize link metadata (i.e. headline, description, image) from all link sharing entry points on Facebook, we are eliminating a channel that has been abused to post false news. We also understand that many publishers have workflows that rely on overwriting link preview metadata to customize how their content appears to audiences on Facebook. We're committed to a solution that supports them.

<https://developers.facebook.com/blog/post/2017/06/27/API-Change-Log-Modifying-Link-Previews>

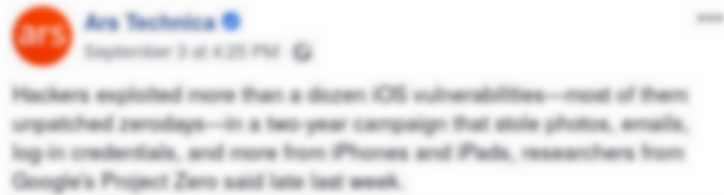
1. First comprehensive study of the link preview creation process of 20 social platforms
2. Identified 14 different link preview templates
3. Experimented with link preview creation in an adversarial setting
4. Performed experiments for active or passive malicious content spread prevention
5. Present seven recommendations towards more robust and trustworthy previews

Link Preview Creation

- Link previews are usually created server-side because of the SOP
- A series of processes takes place to retrieve link-associated resources and build the preview



Designing Link Previews



The Open Graph and Twitter Cards mark-up languages define the content of each field of a link preview

```
<meta property="og:site_name"
  content="(1)" />
```

```
<meta property="og:title"
  content="(2)" />
```

```
<meta property="og:image"
  content="(3)" />
```

1

3

2

Experimental Setup

- Case studies
 - 10 Social Networks
 - 10 Instant Messaging applications
- Performed a set of controlled experiments
- Set up a server, registered accounts (two mobile phones/social network accounts)

Social Networks

Facebook	Tumblr
Twitter	Medium
VK	Xing
LinkedIn	Plurk
Pinterest	MeWe

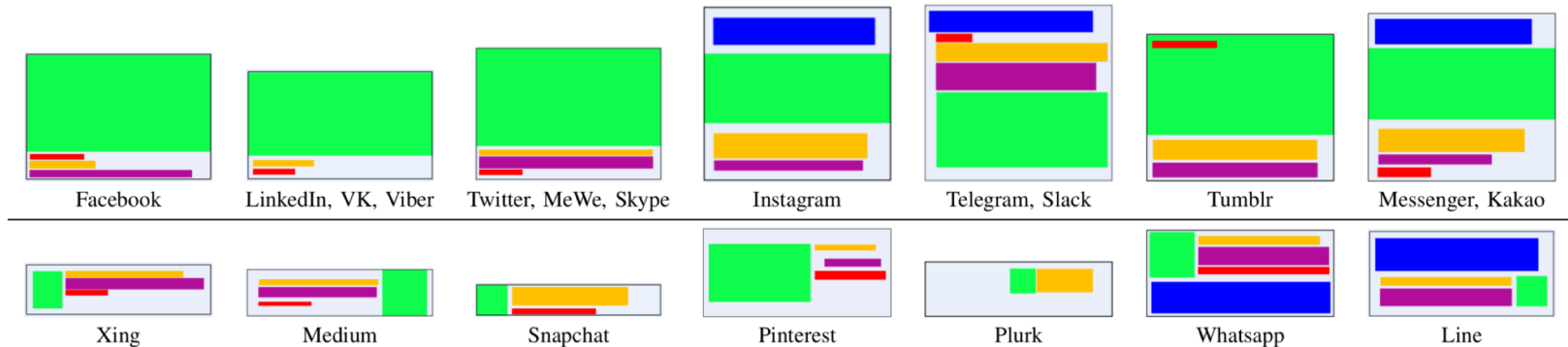
Instant Messaging Apps

Instagram	Line
Messenger	Viber
Skype	KakaoTalk
Snapchat	Telegram
WhatsApp	Slack

Dissecting Link Preview Generation

Comprehensive study of the link preview generation:

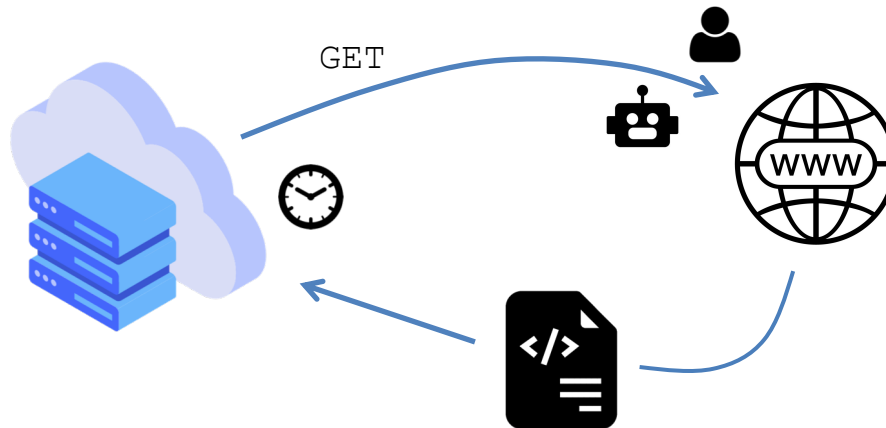
- Displayed fields: title (16/20), domain (14/20), image (11/20), desc. (5/20)
- Position fields: 14 different link preview patterns



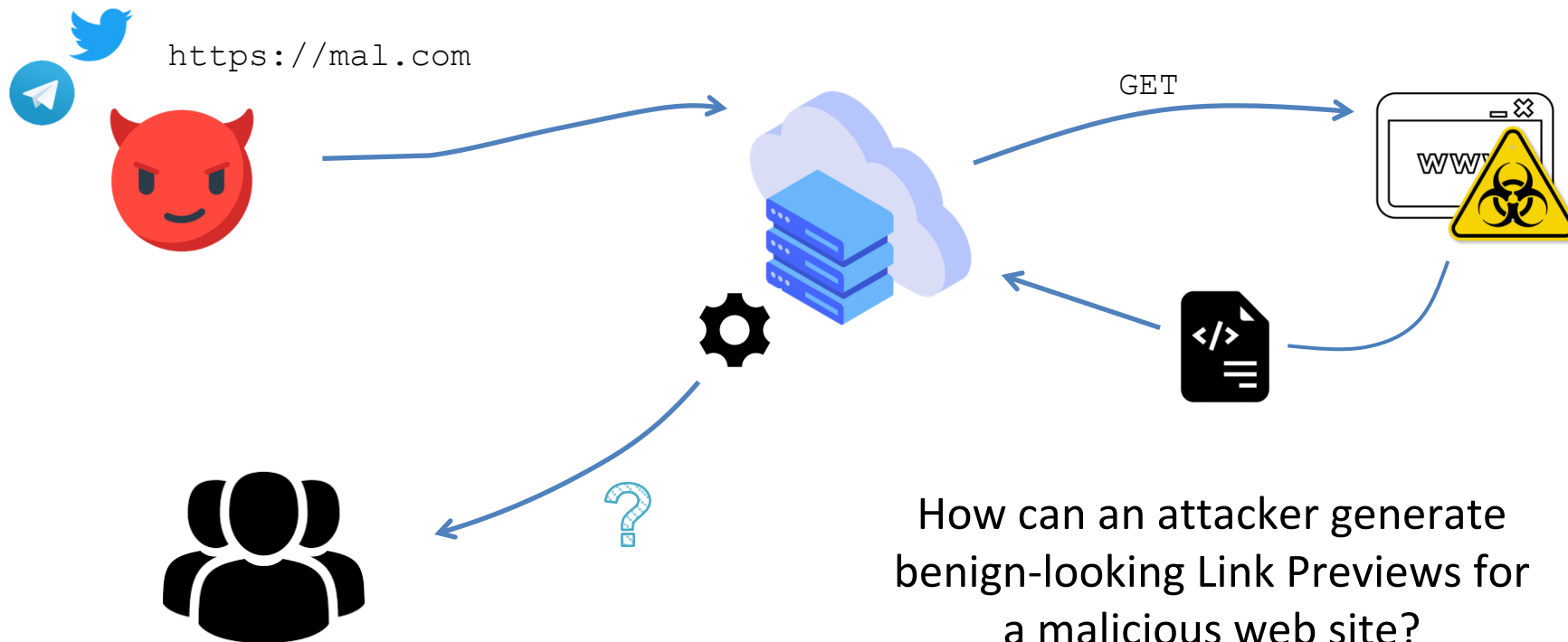
Dissecting Link Preview Generation

Comprehensive study of the link preview generation:

- Network signatures: 35 bot UAs, 18 browser UAs, 23 social platform networks and 3 residential networks
- Caching behavior (14 days): rarely preview update (8/10 only at submission time)



Link Previews in an Adversarial Setting

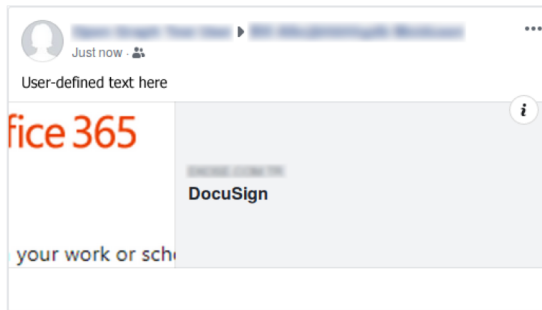


Link Preview Generation (Adversarial Sett.)

Name	Crafted Fields					
	Site title	Site descr.	Image	Host	Shared URL	
Facebook						←
Twitter						
VK						
LinkedIn						
Pinterest						
Tumblr						
Medium						
Xing						←
Plurk						←
MeWe						
Instagram						
Messenger						
Snapchat						
WhatsApp						
Skype						
Line						
Viber						
KakaoTalk						
Telegram						
Slack						←

Preview of External Reference via og:url

Name	Crafted Fields				
	Site title	Site descr.	Image	Host	Shared URL
Facebook	◆	◆	◆	◆	-
Twitter	◆	◆	◆	◇	-
VK	◆	-	◆	◇	-
LinkedIn	◆	◆	◆	◇	-
Pinterest	-	-	◆	◇	-
Tumblr	◆	◆	◆	◇	-
Medium	◆	◆	◆	◇	-
Xing	◆	◆	◆	◆	-
Plurk	◆	-	◆	-	-
MeWe	◆	◆	◆	◇	-
Instagram	◆	◆	◆	-	◇
Messenger	◆	◆	◆	◆	◇
Snapchat	◆	-	◆	◇	-
WhatsApp	◆	◆	◆	◆	◇
Skype	◆	◆	◆	◇	-
Line	◆	◆	◆	-	◇
Viber	◆	-	◆	◇	-
KakaoTalk	◆	◆	◆	◇	◇
Telegram	◆	◆	◆	◇	◇
Slack	◆	◆	◆	◆	◆



```
<meta property="og:url"
content="youtube.com/XZ"/>
```

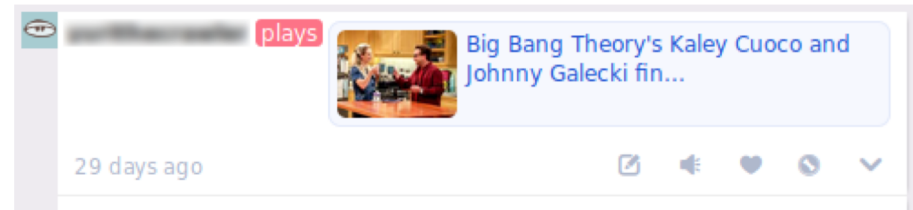


Link Previews without Domain Name

Name	Crafted Fields				
	Site title	Site descr.	Image	Host	Shared URL
Facebook	◆	◆	◆	◆	-
Twitter	◆	◆	◆	◇	-
VK	◆	-	◆	◇	-
LinkedIn	◆	-	◆	◇	-
Pinterest	-	-	◆	◇	-
Tumblr	◆	◆	◆	◇	-
Medium	◆	◆	◆	◇	-
Xing	◆	◆	◆	◆	-
Plurk	◆	-	◆	-	-
MeWe	◆	◆	◆	◇	-
Instagram	◆	◆	◆	-	◇
Messenger	◆	◆	◆	◆	◇
Snapchat	◆	-	◆	◇	-
WhatsApp	◆	◆	◆	◆	◇
Skype	◆	◆	◆	◇	-
Line	◆	◆	◆	-	◇
Viber	◆	-	◆	◇	-
KakaoTalk	◆	◆	◆	◇	◇
Telegram	◆	◆	◆	◇	◇
Slack	◆	◆	◆	◆	◆

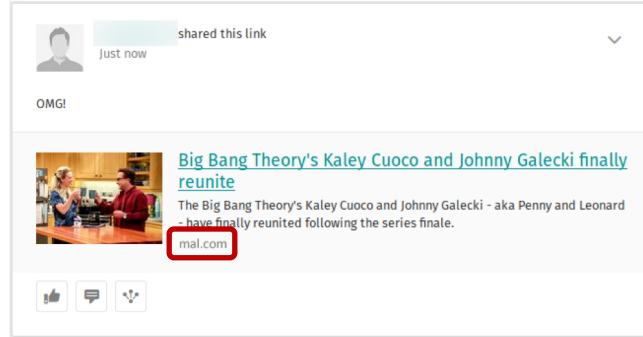
```
<meta property="og:title"
content="Big Bang Theory..." />
```

```
<meta property="og:image"
content="benign-img.jpg" />
```



Replacing Domain using og:site_name

Name	Crafted Fields				
	Site title	Site descr.	Image	Host	Shared URL
Facebook	◆	◆	◆	◆	-
Twitter	◆	◆	◆	◇	-
VK	◆	-	◆	◇	-
LinkedIn	◆	-	◆	◇	-
Pinterest	-	-	◆	◇	-
Tumblr	◆	◆	◆	◇	-
Medium	◆	◆	◆	◇	-
Xing	◆	◆	◆	◆	-
Plurk	◆	-	◆	-	-
MeWe	◆	◆	◆	◇	-
Instagram	◆	◆	◆	-	◇
Messenger	◆	◆	◆	◆	◇
Snapchat	◆	-	◆	◇	-
WhatsApp	◆	◆	◆	◆	◇
Skype	◆	◆	◆	◇	-
Line	◆	◆	◆	-	◇
Viber	◆	-	◆	◇	-
KakaoTalk	◆	◆	◆	◇	◇
Telegram	◆	◆	◆	◇	◇
Slack	◆	◆	◆	◆	◆

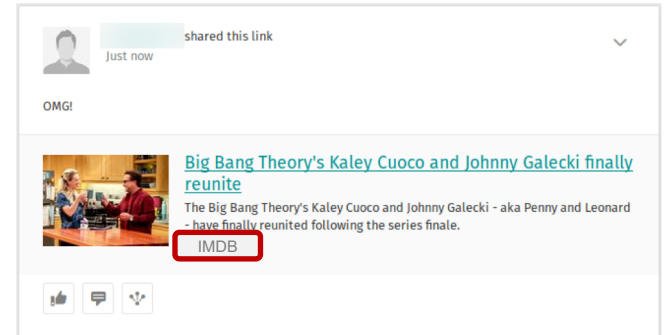


```
<meta property="og:title"
content="Big Bang Theory's..." />
```

```
<meta property="og:image"
content="benign-img.jpg" />
```

```
<meta property="og:description"
content="The Big Bang Theory..." />
```

```
<meta property="og:site_name"
content="IMDB" />
```



Removing Shared URL

Name	Crafted Fields				Shared URL
	Site title	Site descr.	Image	Host	
Facebook	◆	◆	◆	◆	-
Twitter	◆	◆	◆	◇	-
VK	◆	-	◆	◇	-
LinkedIn	◆	-	◆	◇	-
Pinterest	-	-	◆	◇	-
Tumblr	◆	◆	◆	◇	-
Medium	◆	◆	◆	◇	-
Xing	◆	◆	◆	◆	-
Plurk	◆	-	-	-	-
MeWe	◆	◆	◆	◇	-
Instagram	◆	◆	◆	-	◇
Messenger	◆	◆	◆	◆	◇
Snapchat	◆	-	◆	◇	-
WhatsApp	◆	◆	◆	◆	◇
Skype	◆	◆	◆	◇	-
Line	◆	◆	◆	-	◇
Viber	◆	-	◆	◇	-
KakaoTalk	◆	◆	◆	◇	◇
Telegram	◆	◆	◆	◆	◇
Slack	◆	◆	◆	◆	◆

<https://mal.com>

Digital Spy

Big Bang Theory's Kaley Cuoco and Johnny Galecki finally reunite

The Big Bang Theory's Kaley Cuoco and Johnny Galecki - aka Penny and Leonard - have finally reunited following the series finale.



[I should be working now](#) (edited)

Digital Spy

Big Bang Theory's Kaley Cuoco and Johnny Galecki finally reunite

The Big Bang Theory's Kaley Cuoco and Johnny Galecki - aka Penny and Leonard - have finally reunited following the series finale.

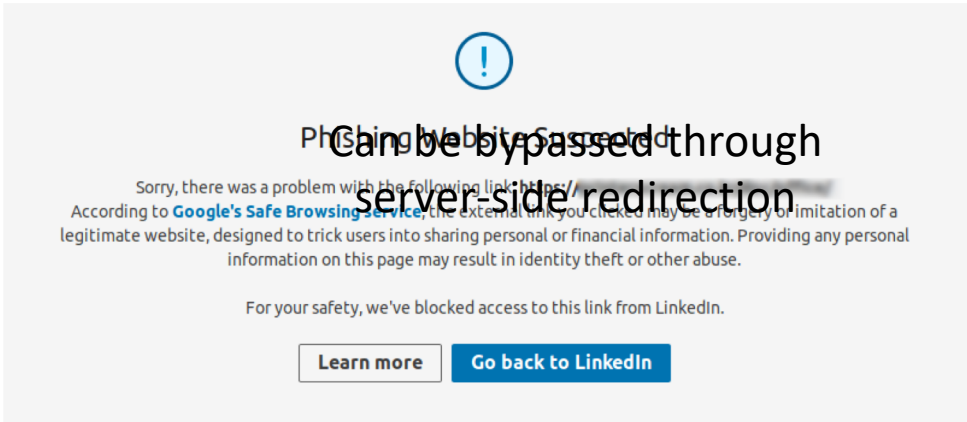


Sharing Malicious Content

Name	Crafted Fields					Tested
	Site title	Site descr.	Image	Host	Shared URL	
Facebook	◆	◆	◆	◆	-	✓
Twitter	◆	◆	◆	◇	-	✓
VK	◆	-	◆	◇	-	✓
LinkedIn	◆	-	◆	◇	-	✓
Pinterest	-	-	◆	◇	-	✓
Tumblr	◆	◆	◆	◇	-	✓
Medium	◆	◆	◆	◇	-	-
Xing	◆	◆	◆	◆	-	✓
Plurk	◆	-	◆	-	-	-
MeWe	◆	◆	◆	◇	-	✓
Instagram	◆	◆	◆	-	◇	✓
Messenger	◆	◆	◆	◆	◇	✓
Snapchat	◆	-	◆	◇	-	✓
WhatsApp	◆	◆	◆	◆	◇	✓
Skype	◆	◆	◆	◇	-	✓
Line	◆	◆	◆	-	◇	✓
Viber	◆	-	◆	◇	-	✓
KakaoTalk	◆	◆	◆	◇	◇	✓
Telegram	◆	◆	◆	◆	◇	✓
Slack	◆	◆	◆	◆	◆	✓

This request looks like it might be automated. To protect our users from spam and other malicious activity, we can't complete this action right now. Please try again later.

Can be bypassed through client-side redirection



Sharing Website Suspended

Sorry, there was a problem with the following link: <https://...>

According to [Google's Safe Browsing Service](#), the external link you clicked may be a forgery or imitation of a legitimate website, designed to trick users into sharing personal or financial information. Providing any personal information on this page may result in identity theft or other abuse.

For your safety, we've blocked access to this link from LinkedIn.

[Learn more](#) [Go back to LinkedIn](#)

Can be bypassed through server-side redirection

Recommendations

1. Introduce a standardized way of building previews
2. Show domain or URL
3. Rebuild or update Link Previews after edits
4. Create Link Previews without retrieving referred pages
5. Enforce type constraints to prevent domain overwrite
6. Do upstream URL validation (e.g., using blacklist services)
7. Inspect redirection chains



Takeaways

- First comprehensive characterization of Link Preview creation process spanning over 20 popular social platforms
 - Inconsistent use of metatags, variety and heterogeneity of templates
- Studied Link Preview creation in an adversarial setting
 - 4 platforms indistinguishable preview, 16 all fields but domain/URL
- Analysis of in-place countermeasures against spread of malicious content
 - 2 platforms do URL filtering, bypassed with server and client redirects
- Present seven recommendations

Automated Agent's Behavior (SNs)

	Facebook	Twitter	LinkedIn	Tumblr	VK	Pinterest	Xing	MeWe	Plurk	Medium
Resources requested before sharing	✓		✓	✓	✓	✓	✓	✓	✓	✓
Resources requested after sharing	✓	✓	✓	✓	✓	✓	✓	✓		✓
Parse OG tags	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Parse Tw tags		✓			✓				✓	✓
Parse HTML code	✓		✓		✓	✓		✓		✓
Follow client HTML redirection	✓		✓			✓				
_ Fetch redirector resources	✓	✓		✓	✓		✓	✓	✓	✓
Follow client JS redirection	✓						✓			
_ Fetch redirector resources	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Inspect og:url resources	✓		✓							
Follow server 303 redirect	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Follow server 307 redirect	✓	✓	✓	✓	✓	✓	✓		✓	✓

Automated Agent's Behavior (IMs)

	Instagram	Messenger	Skype	Snapchat	WhatsApp	Line	Viber	KakaoTalk	Telegram	Slack
Resources requested before sharing					✓				✓	
Resources requested after sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Parse OG tags	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Parse Tw tags		✓	✓	✓	✓	✓	✓		✓	✓
Parse HTML code	✓	✓		✓		✓	✓	✓		
Follow client HTML redirect	✓					✓			✓	
_ Fetch redirector resources	✓	✓	✓	✓	✓		✓	✓		✓
Follow client JS redirect	✓									
_ Fetch redirector resources	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Inspect og:url resources	✓				✓					
Follow server 303 redirect	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Follow server 307 redirect	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓