

Certified Phishing

Taking a Look at Public Key Certificates of Phishing Websites

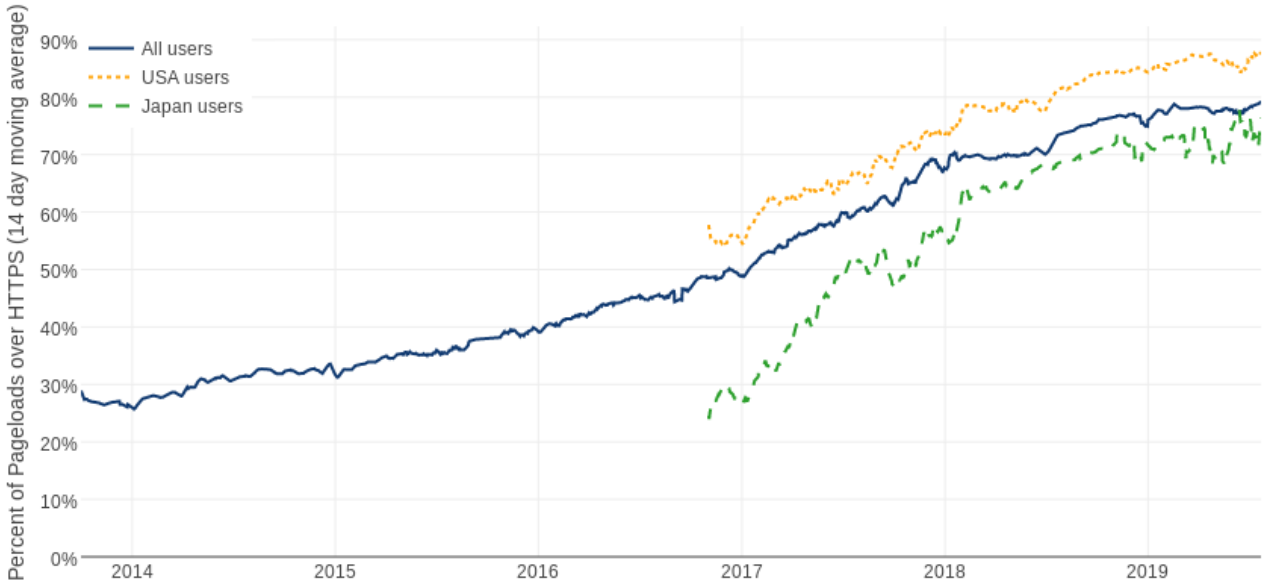
Monday, August 12

Vincent Drury, Ulrike Meyer
RWTH Aachen University
Research Group IT-Security

IT SEC Research Group IT-Security | RWTH AACHEN UNIVERSITY

Why look at Certificates?

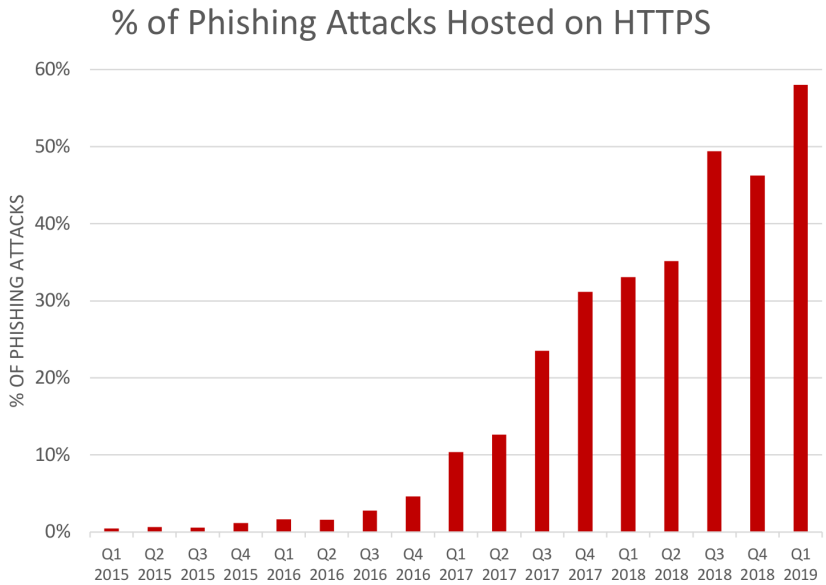
Increasing number of websites with HTTPS



Source: Let's Encrypt, https://letsencrypt.org/stats/. Online, accessed Aug 01, 2019.

Why look at Certificates?

Trend also observable in phishing websites



Source: APWG Phishing Activity Trends Report 1st Quarter 2019, https://apwg.org/trendsreports/.

Phishing: Terms and Process



Attacker

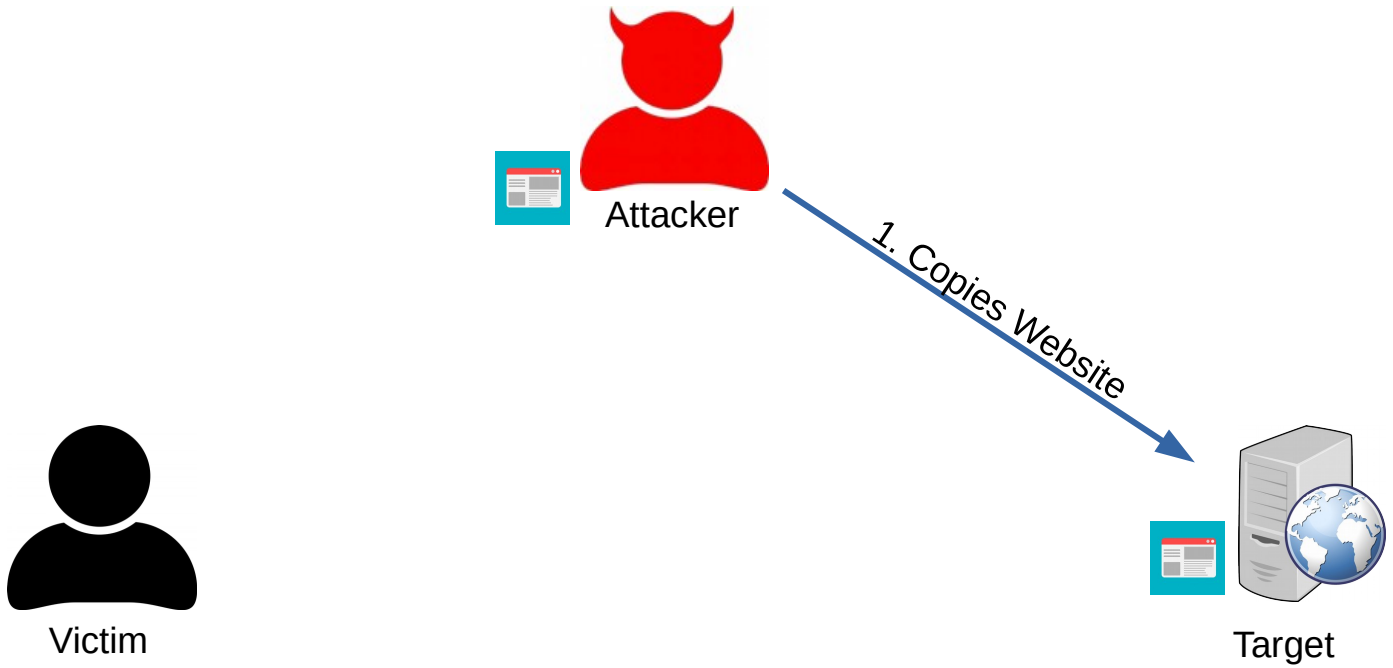


Victim

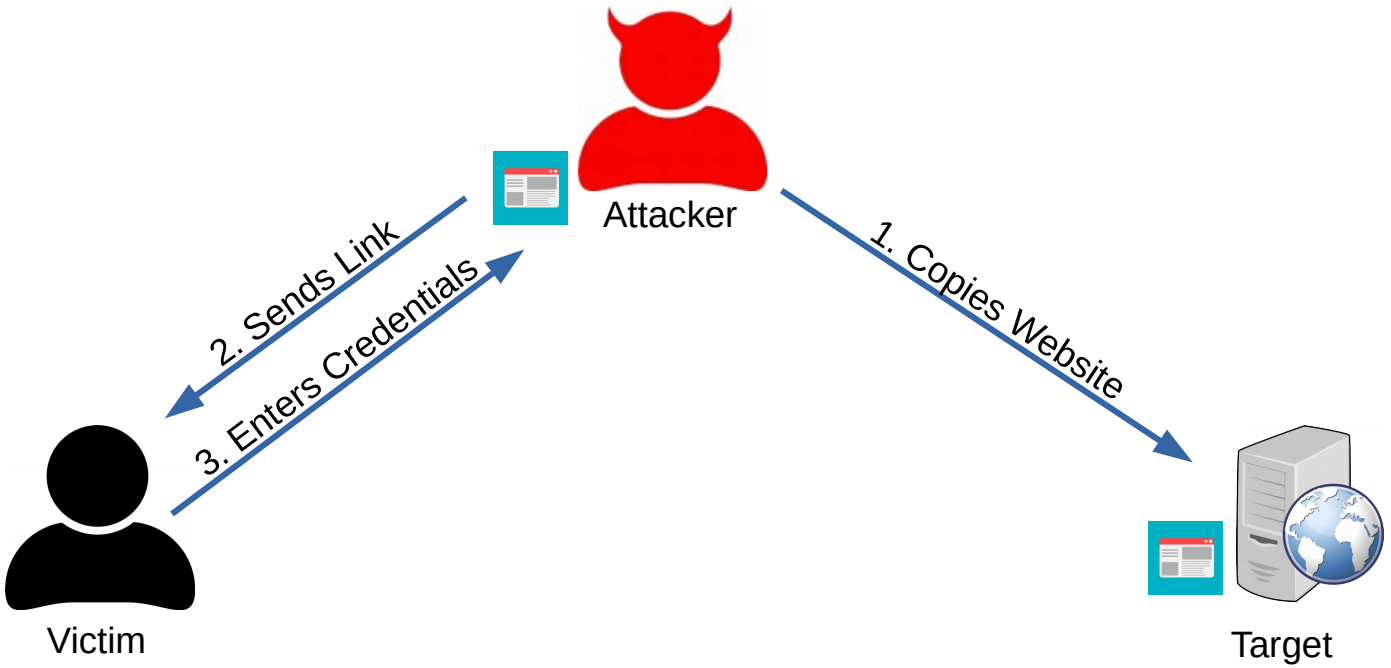


Target

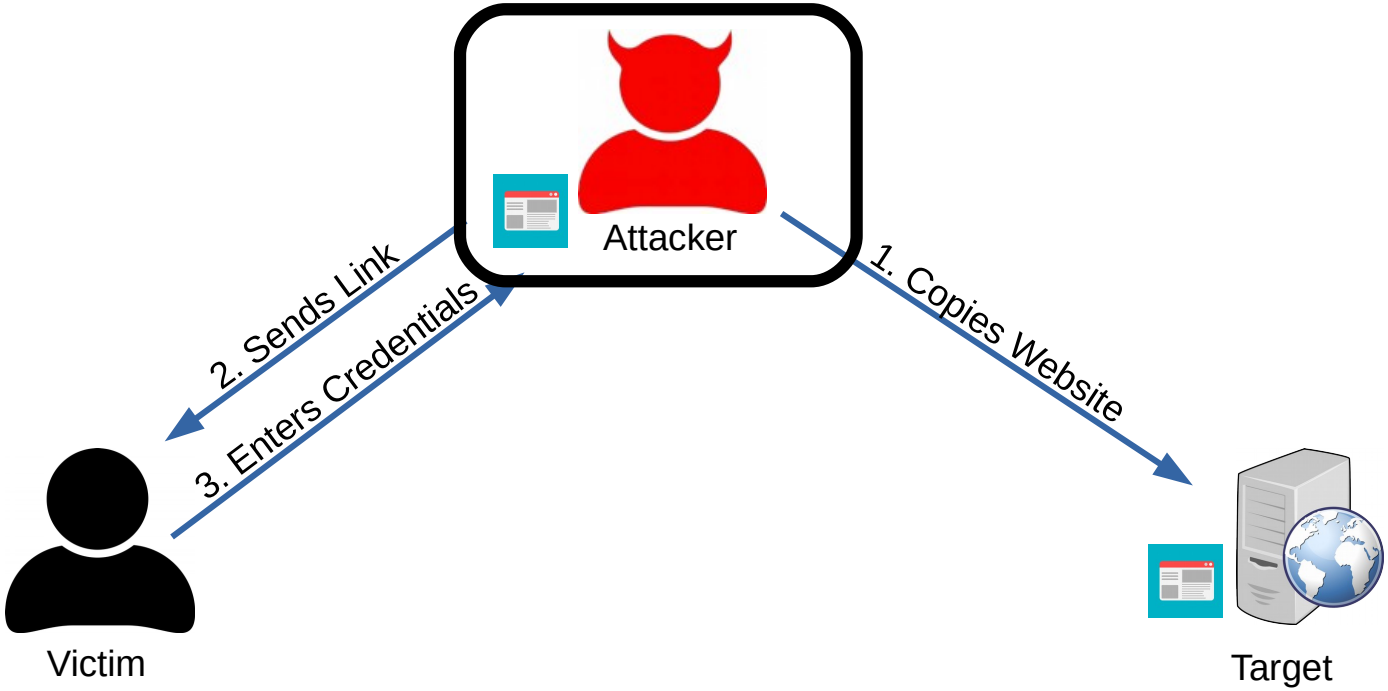
Phishing: Terms and Process



Phishing: Terms and Process



Phishing: Terms and Process



Certificates and CAs



Certificate Authority (CA)

Certificates and CAs



Certificate Authority (CA)

Domain Validation (DV)

Issued To

Common Name (CN)	www.letsencrypt.org
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

https://letsencrypt.org

Certificates and CAs



Certificate Authority (CA)

Domain Validation (DV)

Issued To

Common Name (CN)	www.letsencrypt.org
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

https://letsencrypt.org

Organization Validation (OV)

Issued To

Common Name (CN)	www.google.com
Organization (O)	Google LLC
Organizational Unit (OU)	<Not Part Of Certificate>

https://www.google.com

Certificates and CAs



Certificate Authority (CA)

Domain Validation (DV)

Issued To

Common Name (CN)	www.letsencrypt.org
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

https://letsencrypt.org

Organization Validation (OV)

Issued To

Common Name (CN)	www.google.com
Organization (O)	Google LLC
Organizational Unit (OU)	<Not Part Of Certificate>

https://www.google.com

Extended Validation (EV)

Issued To

Common Name (CN)	www.paypal.com
Organization (O)	PayPal, Inc.
Organizational Unit (OU)	CDN Support

PayPal, Inc. (US) | https://www.

Research Questions

Are there **general differences** between certificates of phishing and benign websites?



Research Questions

Are there **general differences** between certificates of phishing and benign websites?

Are there differences in comparison to a **specific target**?

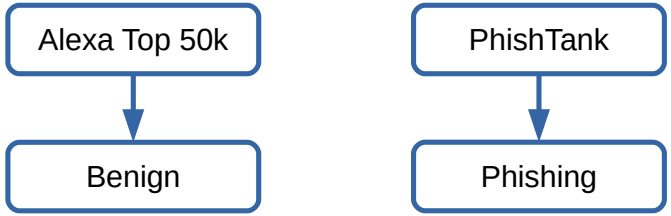


Collection Process Overview



Collection Process Overview

- 50.000 benign URLs from Alexa
- 31.264 phishing URLs from PhishTank (53 days)

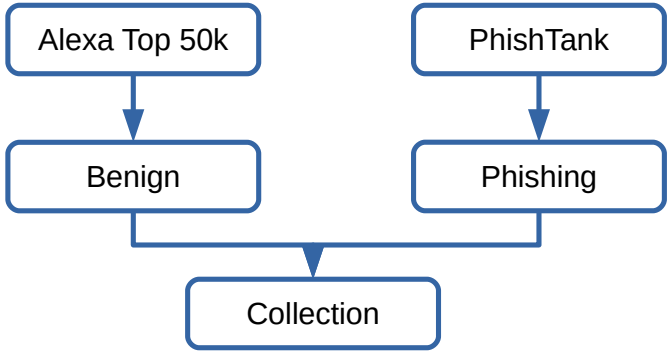


Collection Process Overview

- 50.000 benign URLs from Alexa
- 31.264 phishing URLs from PhishTank (53 days)

Certificates	Benign	Phishing
Collected	43.018	25777
Duplicates	-698	-11.712
Invalid	-2.842	-4.586
Final	**39.478**	**9.479**

⇒ HTTPS does not mean safe

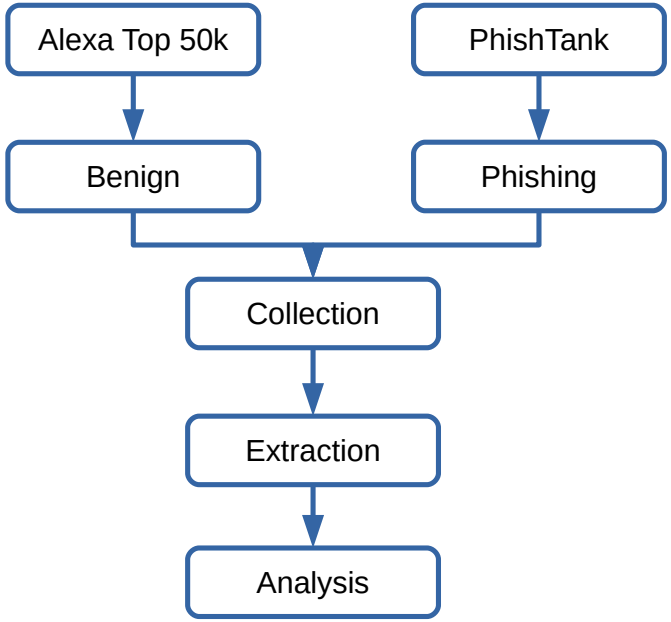


Collection Process Overview

- 50.000 benign URLs from Alexa
- 31.264 phishing URLs from PhishTank (53 days)

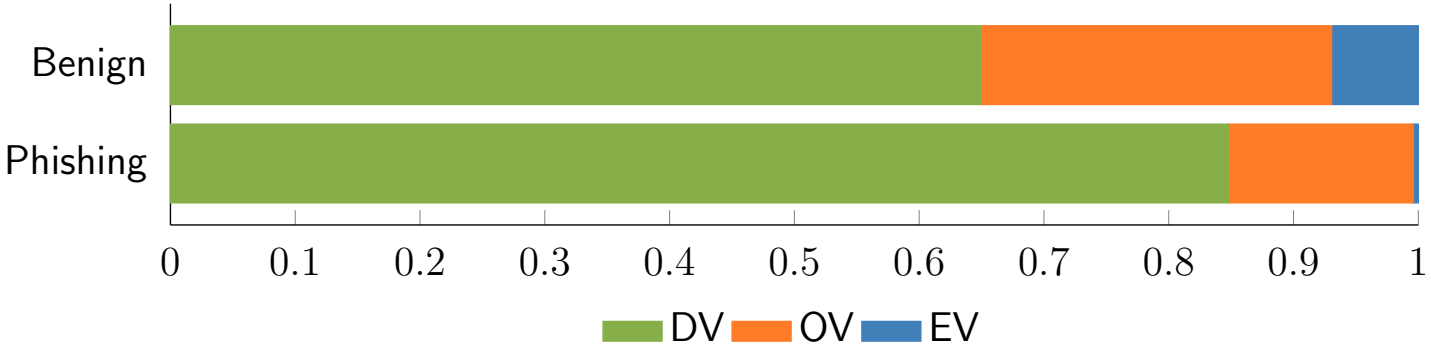
Certificates	Benign	Phishing
Collected	43.018	25777
Duplicates	-698	-11.712
Invalid	-2.842	-4.586
Final	**39.478**	**9.479**

⇒ HTTPS does not mean safe



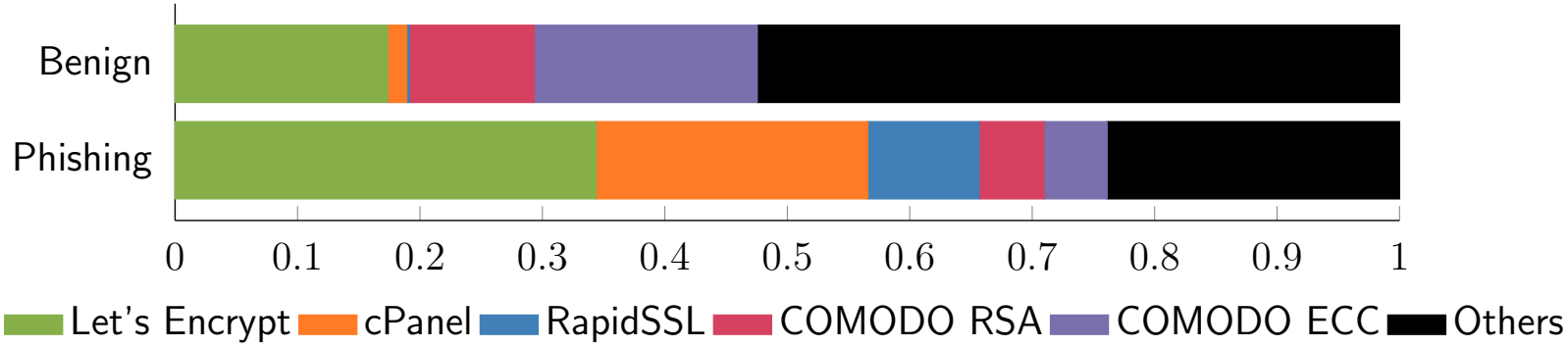
General Differences

Distribution of Validation Types:



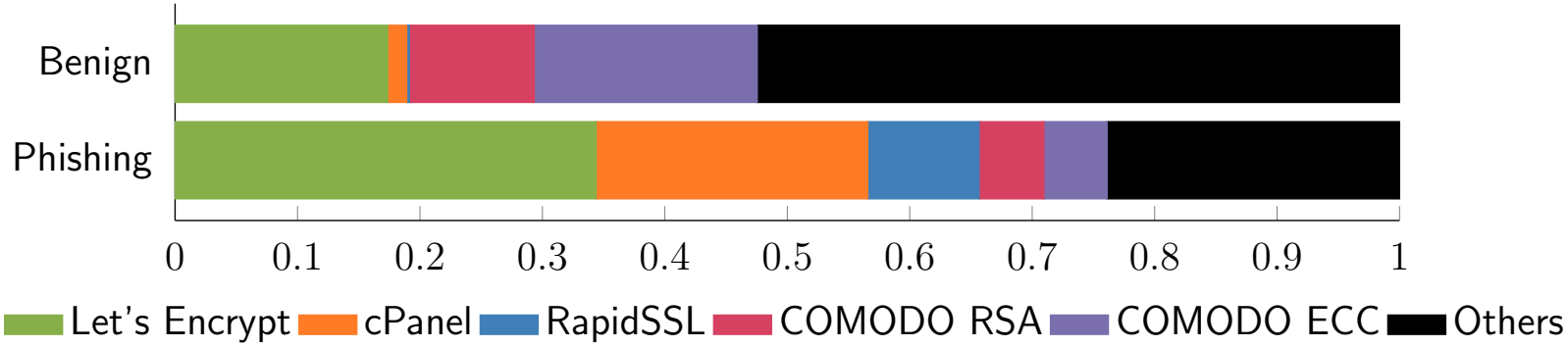
General Differences

Distribution of (5 most common phishing) Issuers:



General Differences

Distribution of (5 most common phishing) Issuers:



⇒ Not generally possible to determine if phishing or benign from certificate alone

Specific Target

Rank	Target	Certificates		
1	PayPal	1169		

Specific Target

Rank	Target	Certificates	Organization	
1	PayPal	1169	0	

Specific Target

Rank	Target	Certificates	Organization	URL DN
1	PayPal	1169	0	84

Specific Target

Rank	Target	Certificates	Organization	URL DN
1	PayPal	1169	0	84
3	Microsoft	297	47*	10
12	Dropbox	37	1*	2
14	Google	33	1*	1

*: Hosted on the target's own infrastructure.

Specific Target

Rank	Target	Certificates	Organization	URL DN
1	PayPal	1169	0	84
3	Microsoft	297	47*	10
12	Dropbox	37	1*	2
14	Google	33	1*	1

*: Hosted on the target's own infrastructure.

⇒ No evidence of active replication of certificate information,
but abuse of target infrastructure possible

Suitability of Certificates for Phishing Detection

- Discriminative power
  - Benign websites without EV/OV certificate



Suitability of Certificates for Phishing Detection

- Discriminative power
  - Benign websites without EV/OV certificate
- Robustness
  - Trust in CAs?



Suitability of Certificates for Phishing Detection

- Discriminative power
  - Benign websites without EV/OV certificate
- Robustness
  - Trust in CAs?
  - Certificate Transparency



Suitability of Certificates for Phishing Detection

- Discriminative power
  - Benign websites without EV/OV certificate
- Robustness
  - Trust in CAs?
  - Certificate Transparency
- Other potential problems
  - TLS interception



Conclusion

- In general **hard to differentiate** certificates of benign and phishing websites
- Currently **no evidence that attackers actively replicate** the content of target certificates
  - But: hosting on target infrastructure sometimes possible
- Certificates as possible resource for future research:
  - Automated detection?
  - User Education?

Conclusion

- In general **hard to differentiate** certificates of benign and phishing websites
- Currently **no evidence that attackers actively replicate** the content of target certificates
  - But: hosting on target infrastructure sometimes possible
- Certificates as possible resource for future research:
  - Automated detection?
  - User Education?

Thank you for your attention!