Cracking the Wall of Confinement: **Understanding and Analyzing Malicious Domain Take-downs.**

Baojun Liu

01/04, Beijing

Institute for Network Sciences and Cyberspace

Tsinghua University

Domain Names

Nearly everything on the Internet starts with DNS requests.

Domain Statistics

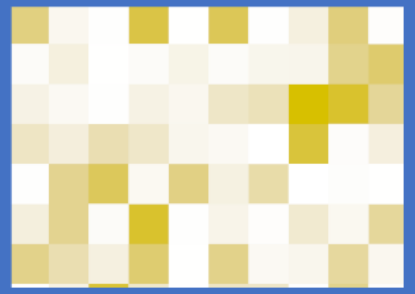
	# TLDs	# Registered
New gTLDs	1,246	50.5 M
Generic TLDs	7	185.0 M
Country TLDs	323	135.3 M
All TLDs	**1,576**	**370.9 M**

* Data source: https://domainnamestat.com/statistics/overview

Internet Malicious Activities

Malware distribution

Child Abuse



Pharmaceutical trading

Copyright infringement

Malicious Domain Take-downs

Domain Sinkhole

Change DNS configuration.

Still Resolvable

Domain Delisting

Change registration status.

Not Resolvable

Domain Delisting

An Example of Domain WHOIS Record

- Domain Name: LIUBAOJUN.ORG
- Creation Date： 2018-01-22
- Registrar: Register.com, Inc.
- Registrar IANA ID: 9
- Domain Status: https://icann.org/epp#clientTransferProhibited
- … …

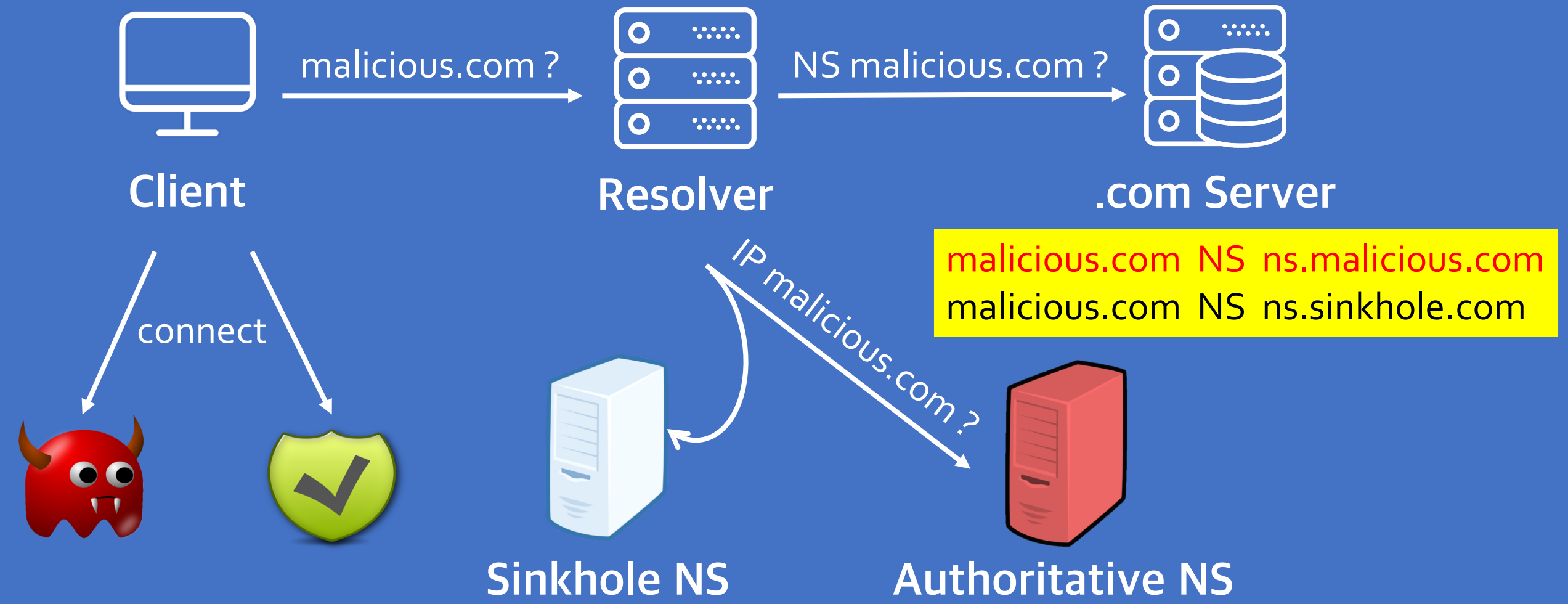
Domain Delisting

EPP Status Code: Extensible Provisioning Protocol in WHOIS record determines a domain's registration status.

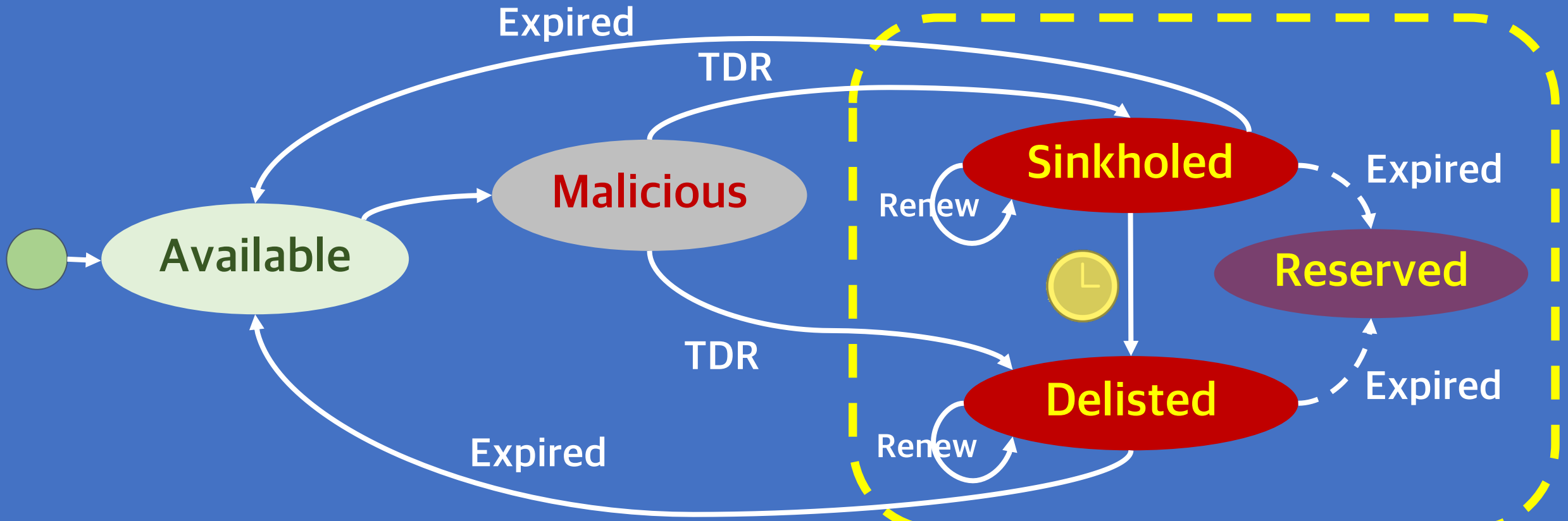
Status codes: serverHold, clientHold remove the domain from the DNS.

Domain is not resolvable: NXDOMAIN.

Domain Sinkhole



Lifecycle of Taken-down Domains



TDR: Take-down Request

Taken-down / Seized

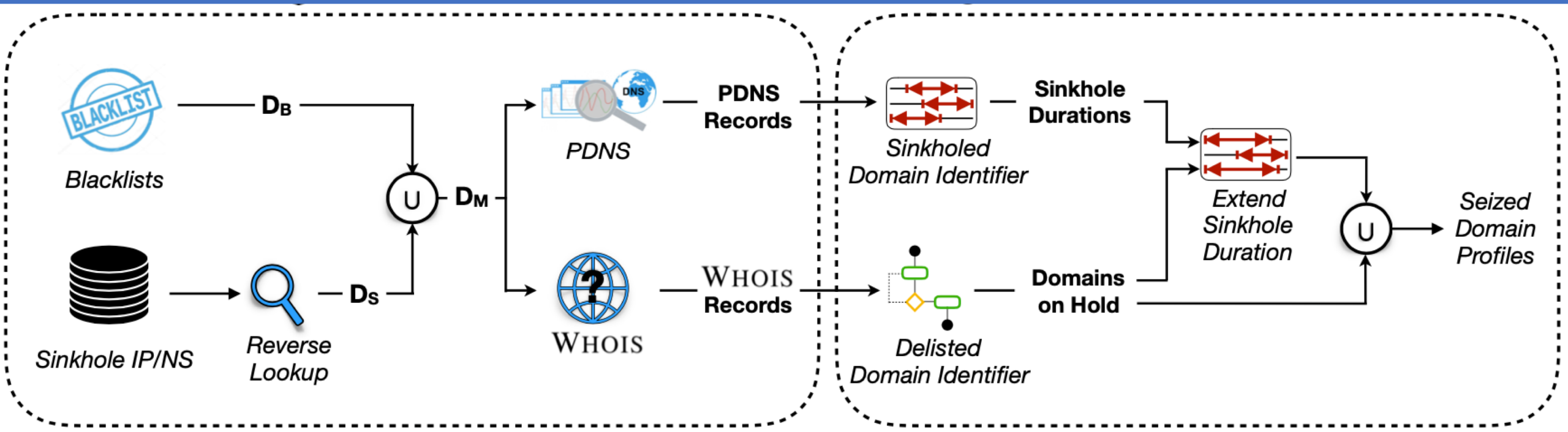
Research Goals

G1: Understanding the take-down process.

G2: Assessing the security and reliability of take-down process.

G3: Set some recommendation for a more effective take-down operation.

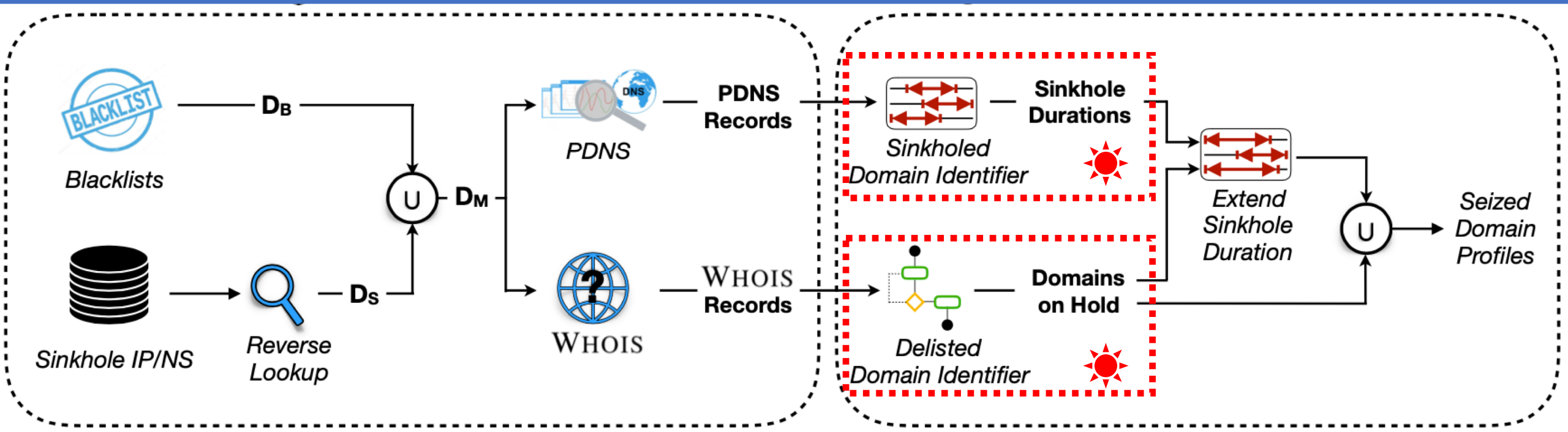
Methodology



Data Collection

Seized Domains Identification

Challenges

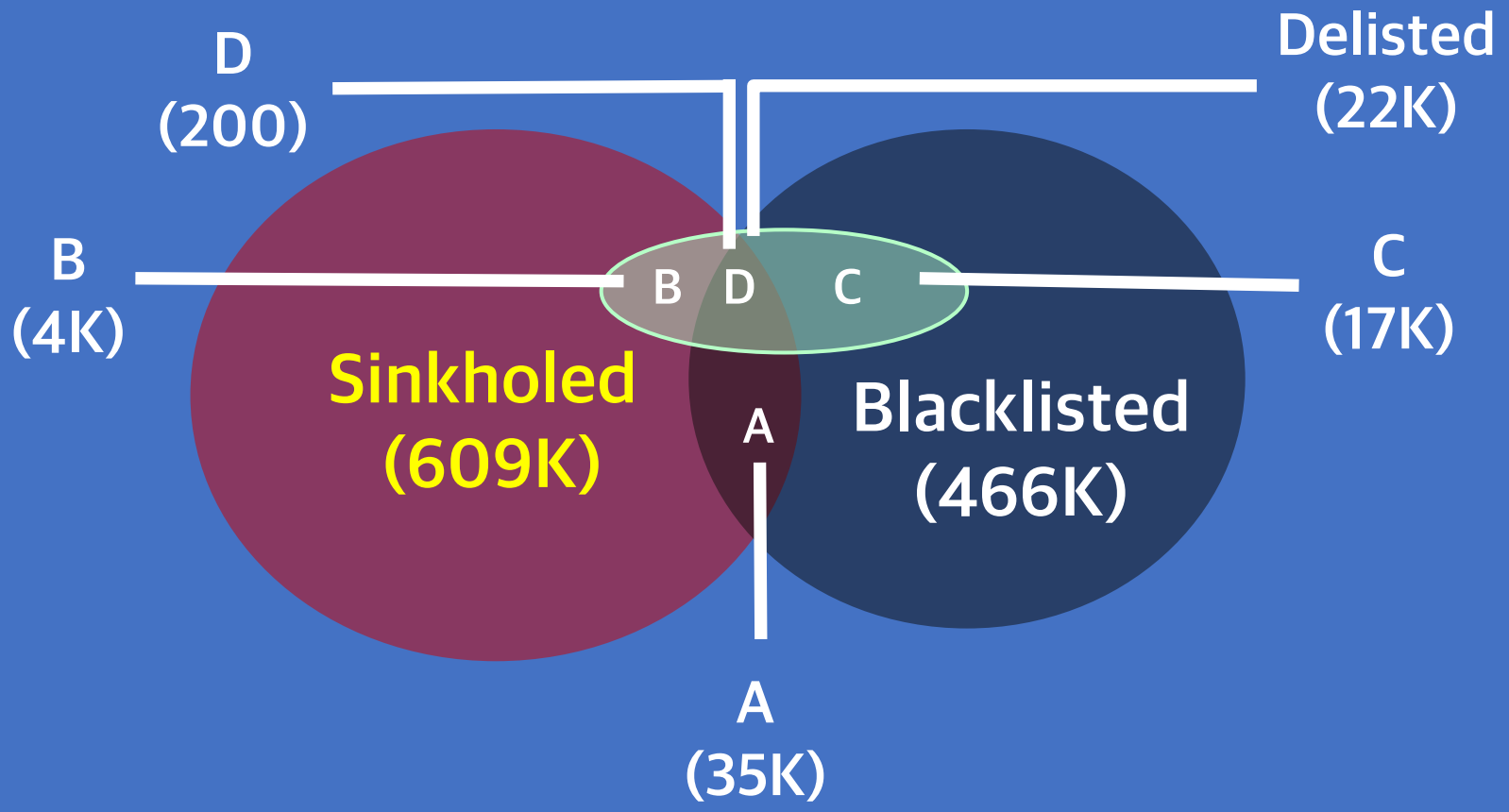


Data Collection

Seized Domains Identification

Collected Dataset

Distribution Analysis

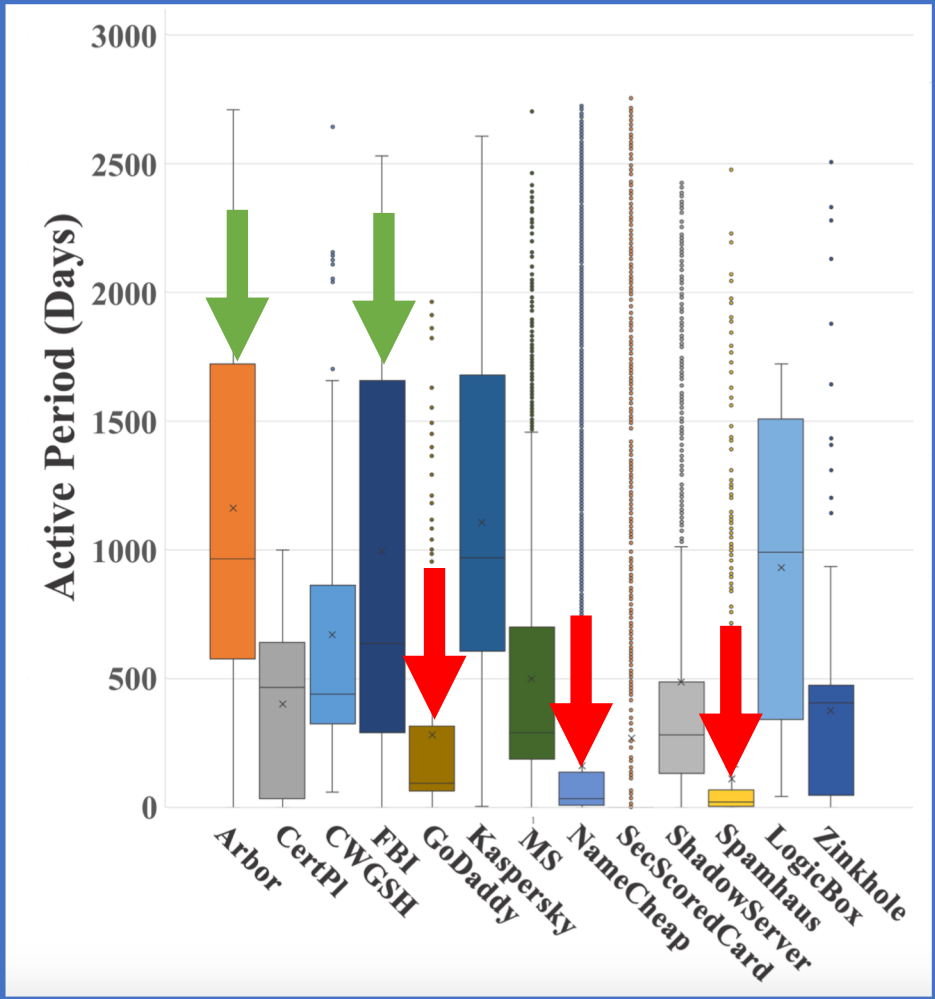


Sinkholes Operators

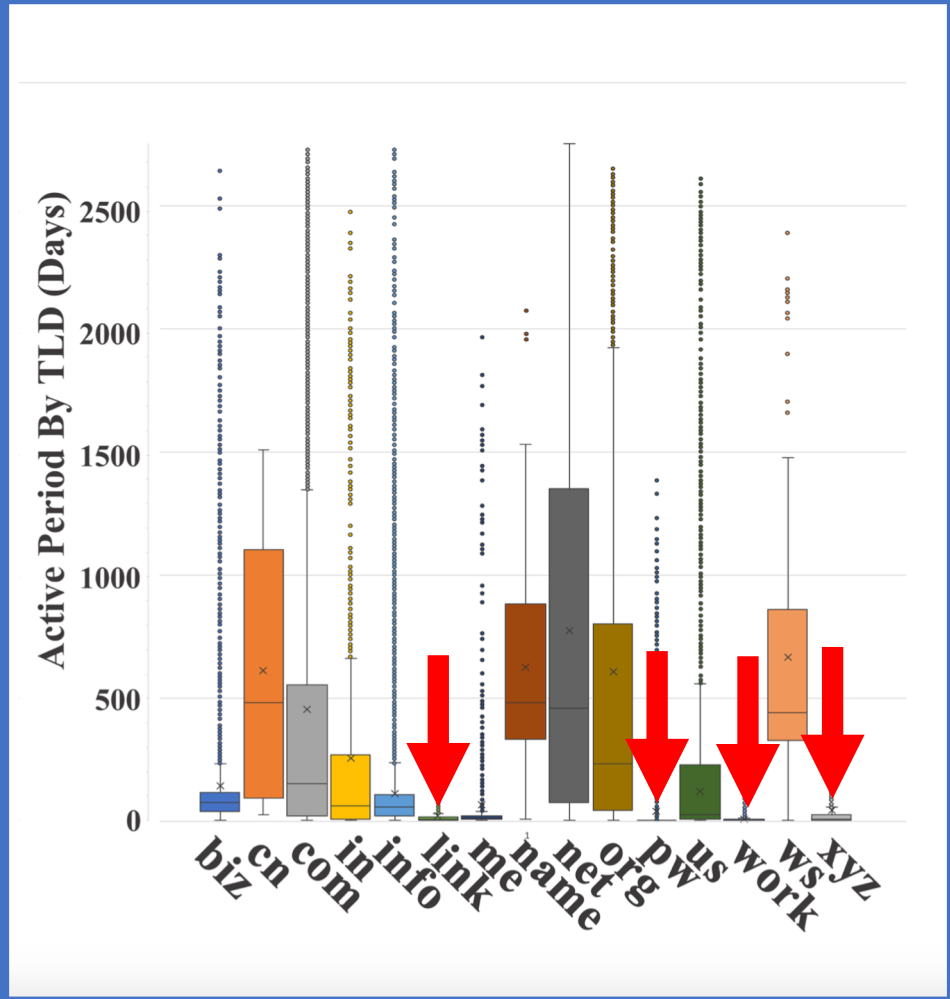
Example: 5 (out of 19) identified sinkhole operators.

Operator	# Sinkholed Domains	Type of Operator	Nameservers
NameCheap	194,772	Registrar	blockedduetophishing.**pleasecontactsupport.com**
FBI	131,875	Law Enforcement	ns[*].**fbi-cyber.net**
Microsoft	103,853	Tech Company	ns[*].**microsoftinternetsafety.net**
Shadowserver	87,974	Non Profit	sinkhole.**shadowserver.org**
Security Scorecard	39,034	Security Vendor	ns[*].**honeybot.us**

Active Duration

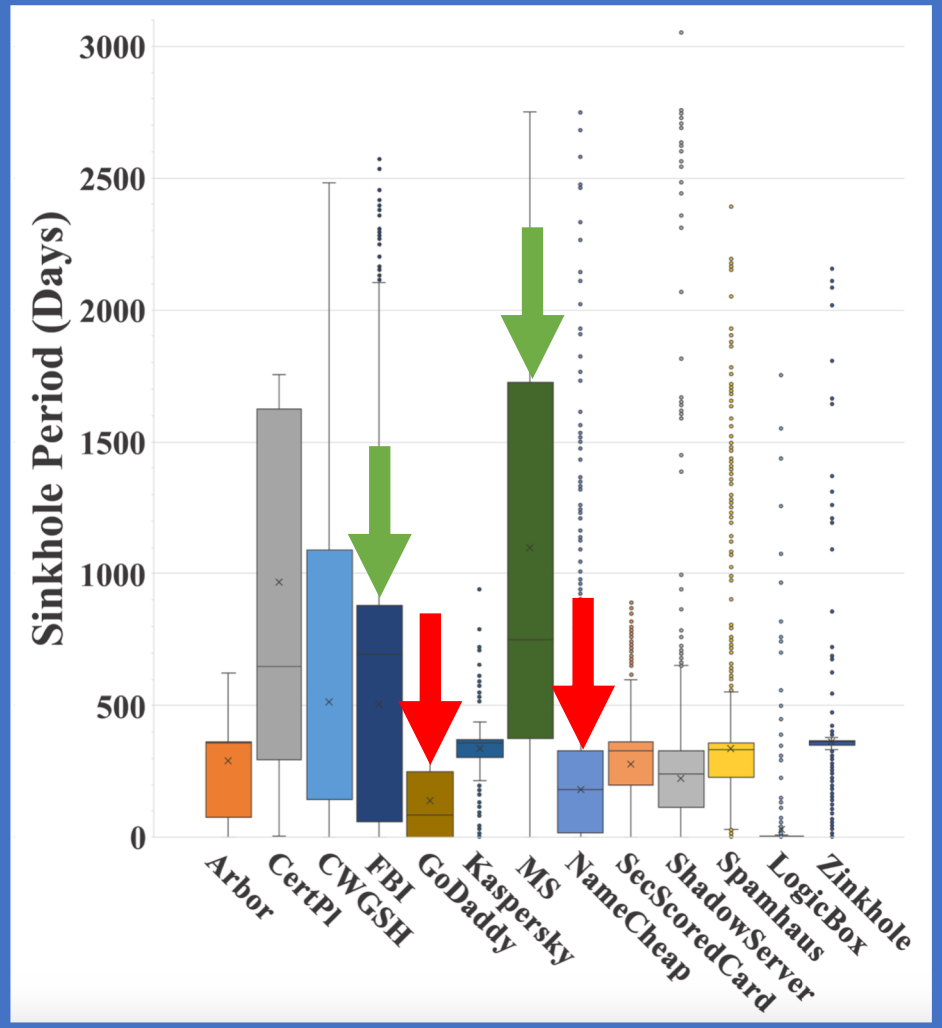


By Sinkhole Operator

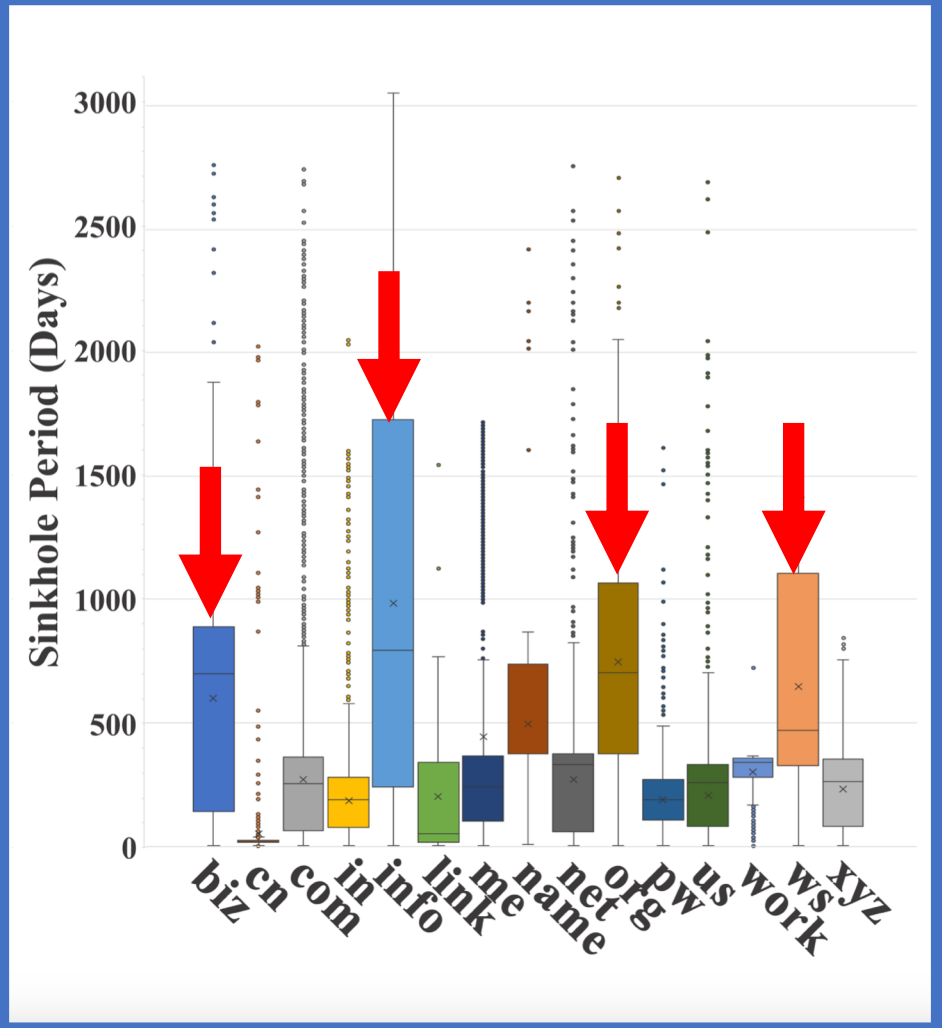


By Top TLDs

Sinkhole Duration



By Sinkhole Operator



By Top TLDs

Domain Availability

I'll be back !!!

350K (56.46%) of all the taken-down domains in the past six years have been released.

7,148 (14.14%) of the domain taken down in the past ten months have been released.

Domain Take-downs Misconfiguration

Exploiting the dangling NS record.

- `carders.org` was initially taken-down by the FBI
- FBI utilized Amazon Route 53

```
carders.org.            NS    ns-9.awsdns-01.com.
carders.org.            NS    ns-922.awsdns-51.net.
carders.org.            NS    ns-1168.awsdns-18.org.
carders.org.            NS    ns-1876.awsdns-42.co.uk.

first seen: 2012-06-27
last seen: 2018-07-22
```

Domain Take-downs Misconfiguration

Exploiting the dangling NS record.

- `carders.org` was initially taken-down by the FBI
- FBI utilized Amazon Route 53

```
carders.org.          NS    ns-9.awsdns-01.com.
carders.org.          NS    ns-922.awsdns-51.net.
carders.org.          NS    ns-1168.awsdns-18.org.
carders.org.          NS    ns-1876.awsdns-42.co.uk.

www.carders.org.      A     8.188.96.3.
carders.org.          A     ALIAS www.carders.org.
```

Liu, Daiping, and etc. "All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records." CCS 2016.

For Recommendations: In the real world

Recommendations

Regulating take-down procedures

- Checking DNS configuration
- Take-down duration and release process

  Malware dirtribution

  Type of illicit activity; Domain's popularity; Domain's Traffic

DNS technical terms translation

- Domain take-down, Sinkhole, and etc.
- DNS Root Server Instance (ICANN)

Conclusions

Understanding Domain Take-downs

Sinkholes Operators

Active duration & Sinkhole duration

Security & Reliability

Domain release process

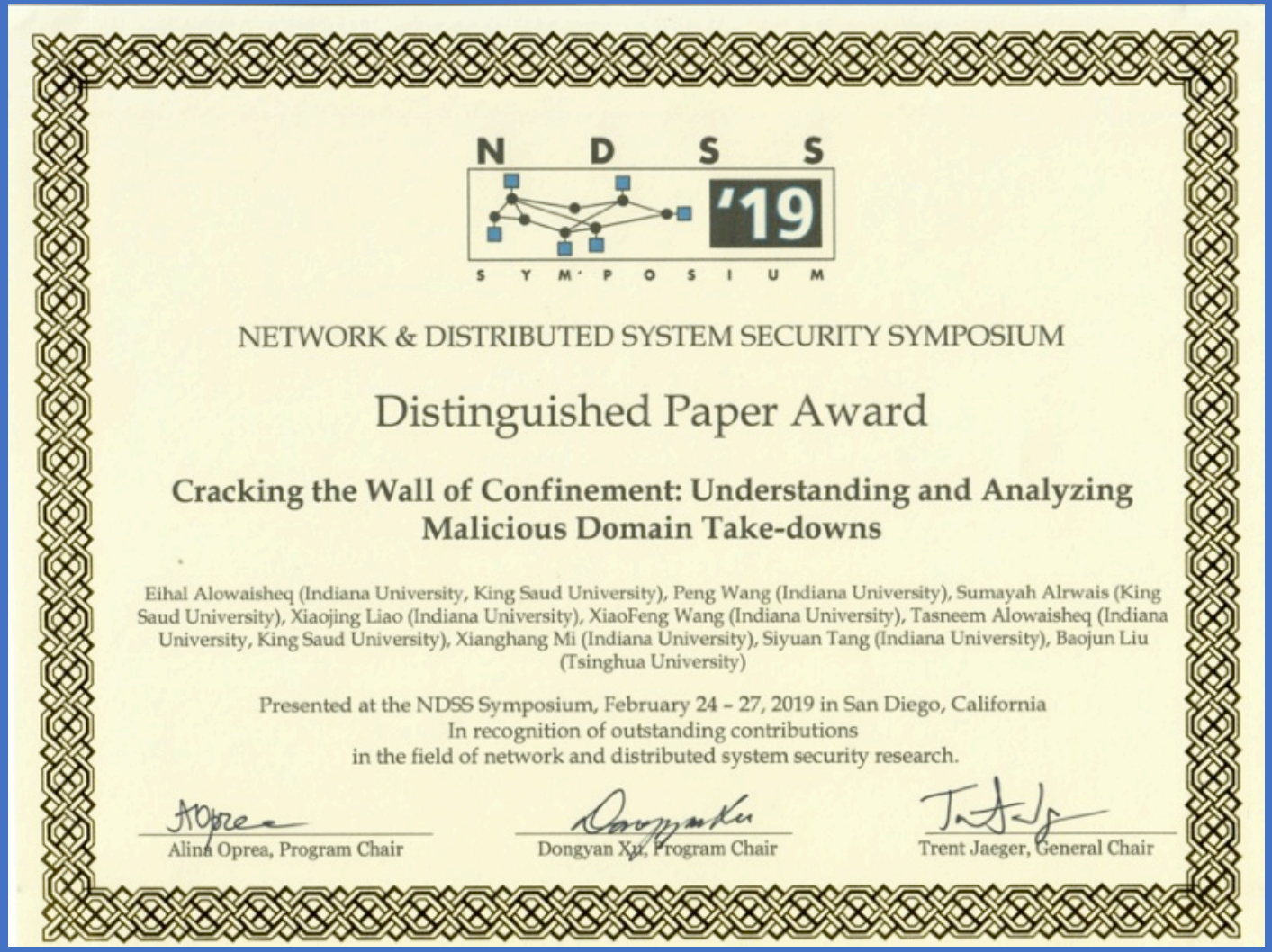
Domain take-downs misconfigurations

Recommendations / Best practices

Regulating take-down procedures

Take-down duration and release process

NDSS Distinguished Paper Award, 2019



N D S S '19

S Y M P O S I U M

NETWORK & DISTRIBUTED SYSTEM SECURITY SYMPOSIUM

Distinguished Paper Award

Cracking the Wall of Confinement: Understanding and Analyzing Malicious Domain Take-downs

Eihal Alowaisheq (Indiana University, King Saud University), Peng Wang (Indiana University), Sumayah Alrwais (King Saud University), Xiaojing Liao (Indiana University), XiaoFeng Wang (Indiana University), Tasneem Alowaisheq (Indiana University, King Saud University), Xianghang Mi (Indiana University), Siyuan Tang (Indiana University), Baojun Liu (Tsinghua University)

Presented at the NDSS Symposium, February 24 – 27, 2019 in San Diego, California
In recognition of outstanding contributions
in the field of network and distributed system security research.

Alina Oprea, Program Chair

Dongyan Xu, Program Chair

Trent Jaeger, General Chair

Cracking the Wall of Confinement: **Understanding and Analyzing Malicious Domain Take-downs.**

Baojun Liu

https://www.liubaojun.org

Open for any question !