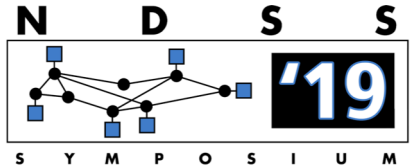
Cracking the Wall of Confinement: Understanding and Analyzing Malicious Domain Take-downs

Eihal Alowaisheq, Peng Wang, Sumayah Alrwais, Xiaojing Liao, XiaoFeng Wang, Tasneem Alowaisheq, Xianghang Mi, Siyuan Tang, Baojun Liu



Overview

- What is a domain take-down?
- Violation includes:
  - malware distribution,
  - pharmaceutical trading,
  - Copyright infringement, etc.
- Goal: mainly to disrupt the malicious traffic
  - Show warning banner
  - Notify infected hosts
  - Mimic the operation of a command and control center (C&C)
- Little information is available about the taken-down operation and their effectiveness

Research Goals

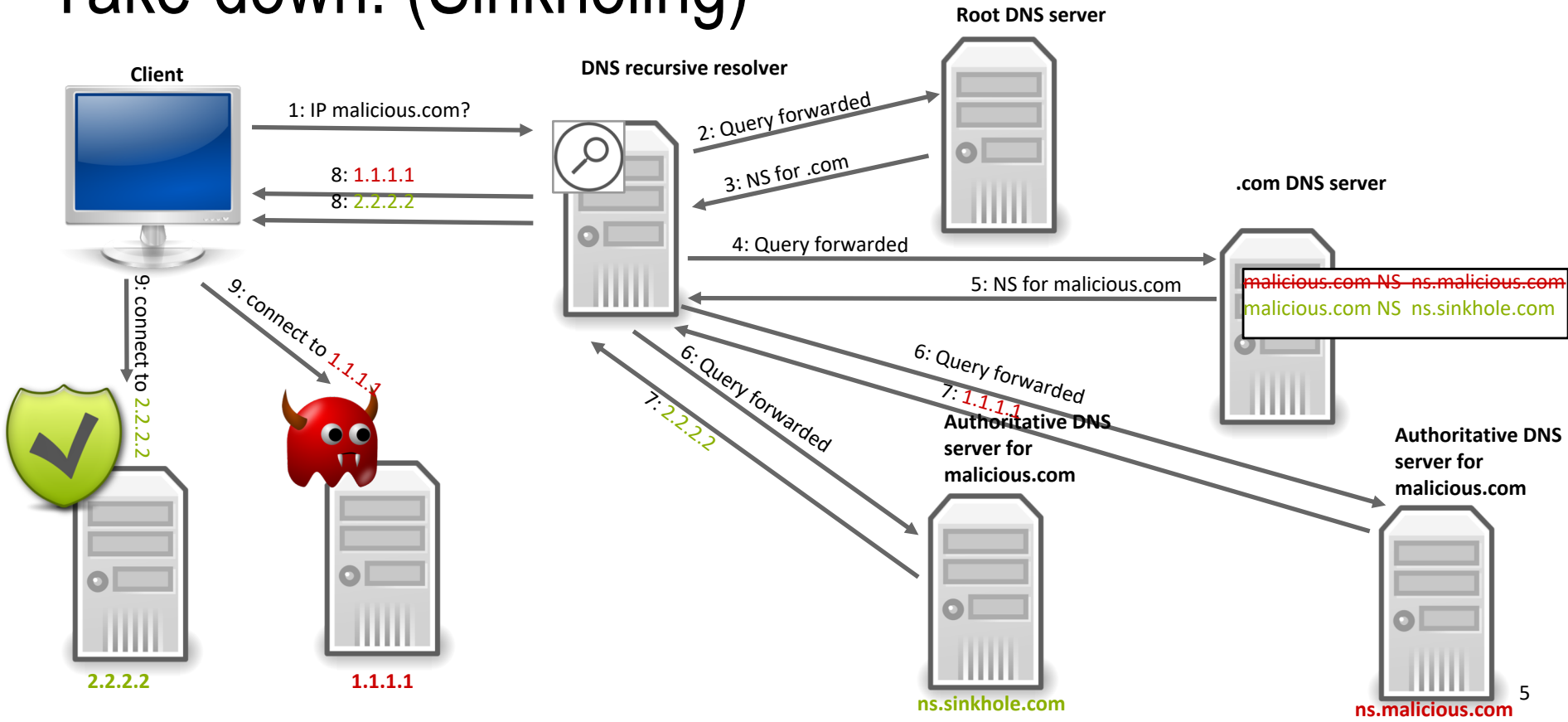
1. Understanding the take-down process
2. Assessing the **security** and **reliability** of the take-down process
3. Set some **recommendation** for a more effective take-down operation

How are Domains Taken Down?

1. Administrative Aspects (Request):
    - File an *Acceptable Use Policy* (AUP) complaint
    - Obtain a court order

2. Technical Aspects (Execution):
    - **Sinkholing:** Change DNS configuration (resolvable)
    - **Delisting:** Change registration status (**un**resolvable)
    - Set the domains as “Reserved” (rare, out of scope)

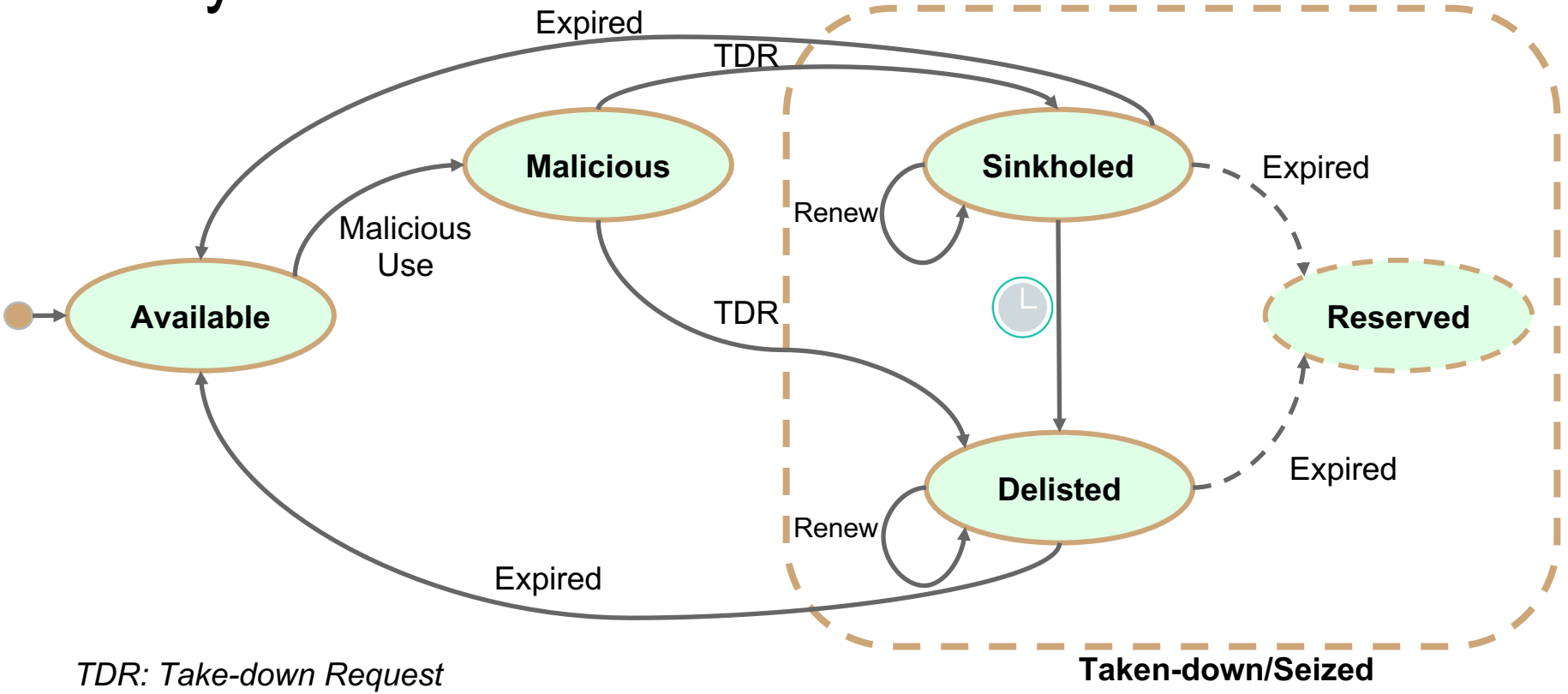
Take-down: (Sinkholing)



Take-down: (Delisting)

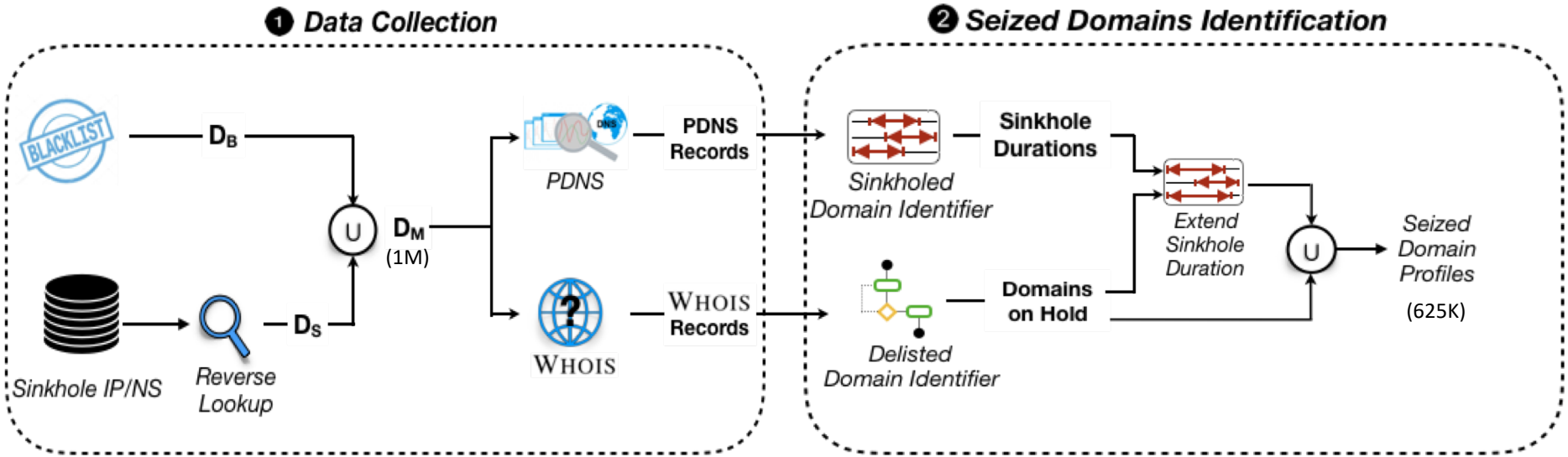
- Domain is **not resolvable**: `NXDOMAIN`
- Extensible Provisioning Protocol (EPP) status code in `Whois` record determines a domain's **registration status**
- Status codes: **`serverHold`**, and **`clientHold`** remove the domain from the DNS
- Note: These status codes are **NOT** exclusively used in take-down operations

Lifecycle of Taken-down Domains

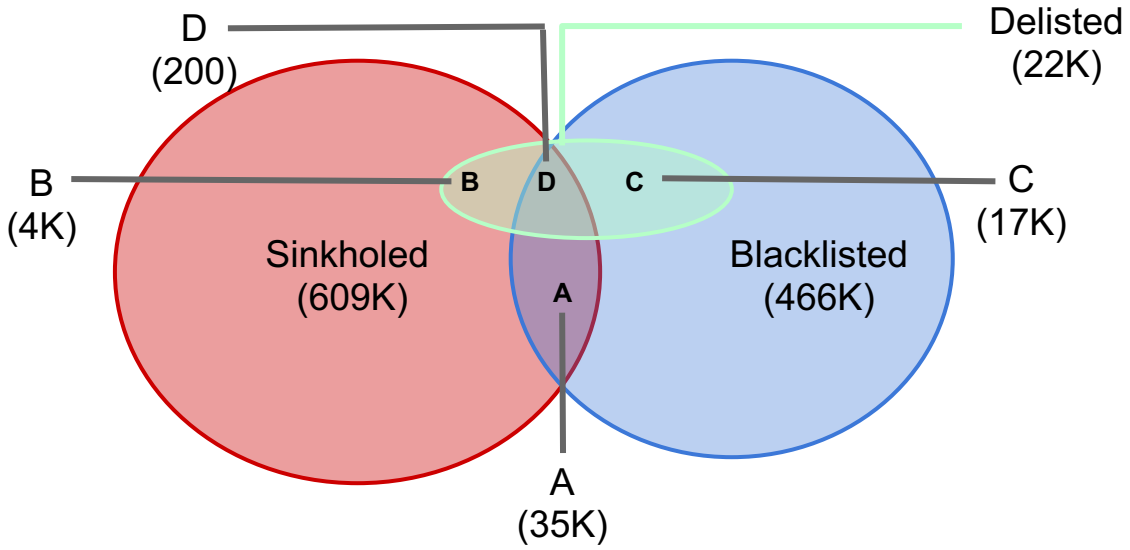


TDR: Take-down Request

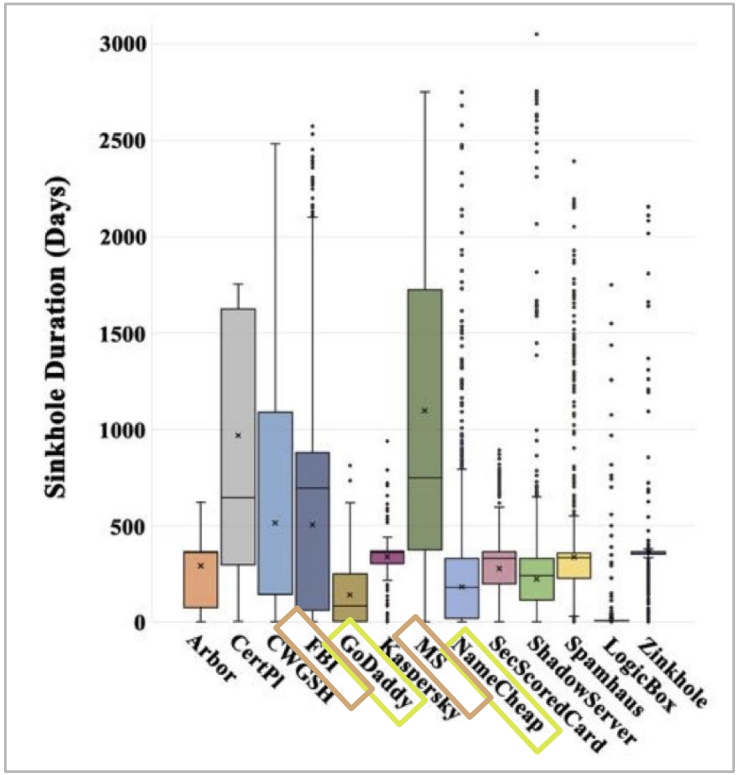
Approach


1 Data Collection
2 Seized Domains Identification
BLACKLIST
D_B
D_S
U
D_M
(1M)
Sinkhole IP/NS
Reverse Lookup
PDNS
PDNS Records
WHOIS
WHOIS Records
Sinkholed Domain Identifier
Sinkhole Durations
Extend Sinkhole Duration
Delisted Domain Identifier
Domains on Hold
Seized Domain Profiles
(625K)

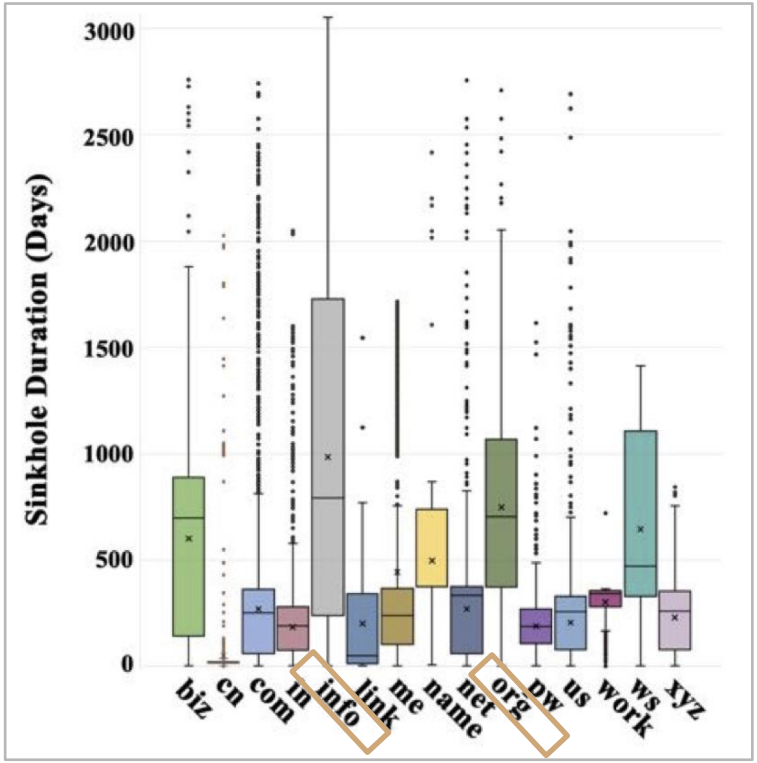
Analysis of Take-down Operations (Distribution)



Analysis of Take-down Operations (Sinkhole Duration)



By Sinkhole Operator



By TLD Registry

Findings

- Domain availability after release:
  - 56.46%,
  - 14% in less than 10 months
- Some malicious domains have been **maliciously re-registered** again after being released
- We were able to **hijack a taken-down domain** due to a DNS misconfiguration
- **Expired nameservers** purchased by new owners cause the traffic of around 30K domains to be redirected to new owners

Findings: (Hijacking a taken-down domain)

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

```
first seen in zone: 2012-06-27
last seen in zone:  2018-07-22
rrtype:     NS
rdata:      ns-9.awsdns-01.com.
            ns-922.awsdns-51.net.
            ns-1168.awsdns-18.org.
            ns-1876.awsdns-42.co.uk.
first seen: 2012-06-26
last seen:  2013-01-05
rrtype:     A
rdata:      204.236.228.238
```

The PDNS records for carders.org (NS and A). The NS record was still set at .org TLD “dangling NS”

```
carders.org.        NS   ns-1601.awsdns-08.co.uk.
                    NS   ns-1168.awsdns-18.org.
                    NS   ns-762.awsdns-31.net.
                    NS   ns-226.awsdns-28.com.

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

Our takeover of carders.org exploiting the dangling NS record and setting a new A record. The set IP address points to our webserver

Findings: (Expired Nameservers)

- Sinkholes operated by Conficker Working Group: `ns.cwgsh.{com,net,org}`
- Domains `cwgsh.{com,net,org}` expired on Feb. 2011

zzyiwabmkz.info.	**NS**	ns.cwgsh.com.
zzyiwabmkz.info.	**NS**	ns.cwgsh.net.
zzyiwabmkz.info.	**NS**	ns.cwgsh.org.
www.zzyiwabmkz.info.	**A**	190.2.131.62
ww9.zzyiwabmkz.info.	**A**	166.78.101.108

A record sets for new subdomains of zzyiwabmkz.info observed in July 2018. After expiration of cwgsh.{com,net,org}

Conclusion

We recommend setting specific policies **regulating take-down** procedures

- Checking DNS configurations
- Take-down **duration** and **release process**:
  a. Malware distribution: must remain taken down until no more traffic is received
  b. Other illicit activity:
     i. Domain's popularity
     ii. Domain's current traffic
     iii. Type of illicit activity

Thank you

Questions?