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)

Client

1: IP malicious.com?

DNS recursive resolver

2: Query forwarded

3: NS for .com

4: Query forwarded

5: NS for malicious.com

6: Query forwarded

7: 1.1.1.1

Authoritative DNS server for malicious.com

8: connect to 1.1.1.1

9: connect to 2.2.2.2

9: connect to 1.1.1.1

2.2.2.2

1.1.1.1

1.1.1.1

2.2.2.2

malicious.com NS ns.malicious.com

malicious.com NS ns.sinkhole.com

Root DNS server

.com DNS server

Authoritative DNS server for malicious.com

ns.sinkhole.com

ns.malicious.com

Client
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

Available → Malicious
Malicious Use → Malicious
TDR → Sinkholed
Sinkholed → Delisted
Expire → Renew
Delisted → Expire
Sinkholed → Reserved
Reserved

TDR: Take-down Request
Approach
Analysis of Take-down Operations (Distribution)

Sinkholed (609K)
Blacklisted (466K)
Delisted (22K)

A (35K)
B (4K)
C (17K)
D (200)
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

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

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**

<table>
<thead>
<tr>
<th>Subdomain</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>zzyiwabmkz.info.</td>
<td>NS</td>
<td>ns.cwgsh.com.</td>
</tr>
<tr>
<td>zzyiwabmkz.info.</td>
<td>NS</td>
<td>ns.cwgsh.net.</td>
</tr>
<tr>
<td>zzyiwabmkz.info.</td>
<td>NS</td>
<td>ns.cwgsh.org.</td>
</tr>
<tr>
<td><a href="http://www.zzyiwabmkz.info">www.zzyiwabmkz.info</a>.</td>
<td>A</td>
<td>190.2.131.62</td>
</tr>
<tr>
<td>ww9.zzyiwabmkz.info.</td>
<td>A</td>
<td>166.78.101.108</td>
</tr>
</tbody>
</table>

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?