Domain Reputation Lists

A tool against domain abuse

Raymond Dijkxhoorn (raymond@surbl.org) / Joe Wein (joewein@surbl.org)
What are Domain Reputation Lists?

- The **earliest DNS Blocklists** were lists of **sender IPs** (e.g. Vixie/Rands’s MAPS / Spamhaus SBL)
- URI Blocklists are different because...

  - **URI Blocklists** are a type of Domain Reputation List for **abusive domains advertised in Email links**
  - SURBL was created in 2004 primarily to filter email, for example:
    - SURBL Multi

Other well known domain reputation lists are SpamHaus DBL and URIBL, each with their own data quality and reach.

Different categories:

    Phishing – Malware – Spam - Cracked websites - Bitcoin – Fake brand sites
What are Domain Reputation Lists?

- Both Sender IP Blocklists and URI Blocklists can be used for traffic filtering
- Sender IP Blocklists work well as a first check, but:
  - blocking all mail from Gmail, Yahoo, ISP outbound mail servers, etc. is not practical
  - spammers use legitimate mail servers with stolen credentials or hacked accounts
- URI Blocklists have more overhead but are more selective
  - most spam and most phishing mails include links
  - can block by sites in the email payload, regardless of sender
  - can also be used to block based on HELO data (email)
- Sender IP Blocklists and URI Blocklists work best in combination:
  - sender IP checks catch 80-90% of abuse
  - URI reputation lists checks will catch most of the rest
How to use a URI Blocklist

Example:

<a href="http://paypalukverify.com/click/here.html">Verify your PayPal account now!</a>

Steps:

- Extract the host name or domain name
  - paypalukverify.com
- Prepend domain to URI Blocklist zone
  - paypalukverify.com, multi.surbl.org
- Perform A record DNS query
How to use a URI Blocklist (continued)

- If **NXDOMAIN** is returned: The host is **not listed**
- Otherwise check the returned A record(s)
  - paypalukverify.com.multi.surbl.org. 180 IN A 127.0.0.8
  - lowest octet indicates type of listing (e.g. 0x08 = PH = phishing)
  - Additional information may be returned via TXT record
  - "Blocked, paypalukverify.com on lists [ph], See: [http://www.surbl.org/lists.html](http://www.surbl.org/lists.html)"

Do not check sender IP addresses against a domain blocklist!

We have full URI data available also for selected sources (including lookup APIs for automating these)!
Where does the data come from?

- Spam trap hits
  - URIs are extracted from emails sent to addresses that did not opt-in to receive bulk mail
  - Geographically diverse traps with real-time feeds to central processing
  - Not all spam trap URIs will be listed (innocent bystanders)
  - Spam traps are mined to derive rules for other listing methods
- Zone File Analysis
  - Daily downloads or near real-time zone transfers
  - Use domain age to determine domain reputation
- DNS query mining
- Whois data – Find related abusive registrations (reverse whois)
  - Impacted by GDPR
- Trusted data partners – Governmental / Takedown operators / Registries / Registrars
- Other proprietary research

We work with many registries to see where we can help the global community
Common use of reputation data

Use by Mail providers / ESPs:

- Used for mail filtering by some of the largest e-mail providers
- Outbound mail filtering protects IP reputation of sender IPs

Use by hosting providers

- Can be alerted to abusive domains or cracked websites on their networks
- Protects their reputation

Security Vendors

- Used for DNS Firewall (RPZ) by corporates and security vendors
- Even domains that aren’t listed yet when mail arrives can be blocked by the time a link is clicked
- Attempted accesses to malicious domains can be redirected inside the network

SURBL was the first data provider that supplied a RPZ feed
Use by Registries and Registrars

- Registries and registrars use it for abuse monitoring
- Used in ICANN Domain Abuse Activity Reporting (DAAR)
- Spamhaus and SURBL publish “most abused TLDs” lists – ‘TLD health’
- Can be used to suspend or notify abusive clients
- Our goal: Listings will be expired when domains are deactivated
- Provides incentive for shutting down bad domains
- Saves resources and minimizes damage

But how do we find out about domain shutdowns?
Can we help SURBL make the world a better place?

- Zone file downloads help
- Zone file transfers (i.e. near real time) are even better
- Non-rate limited WHOIS will allow reputation providers to verify deactivations
- Get in touch with us for custom projects
- Work collectively to get your TLD space cleaned up!

And last but not least!

- Tell us about sink-holed domain sets!
Summary

- Domain Reputation Lists have been around for 15+ years
- Used by some of the largest IT companies in the world
- They provide real-time intelligence on abusive domains
- Can be used for email filtering, DNS firewalls and abuse monitoring
- Mutual benefits through data exchange
- Useful toolset for law enforcement
Open discussion

We are here this week to talk! – Please reach out to us!