DNS abuse in a time of Covid-19

Drew Bagley
drew@securedomain.org
May 2020
DNS Abuse trends

- The rapid shift to remote work has changed the dynamics of the threat environment for many organizations and individuals.
- eCrime actors are leveraging the DNS to carry out cyber attacks incorporating Covid-19 themes.
- Many campaigns focus on phishing victims to defraud them or deliver malware.
- Domain name registrations incorporating “covid-19”, “WHO,” and “CDC” have been used.
Phishing in Australia

ASD’s Australian Cyber Security Centre warned about phishing scams utilizing Covid-19 themed domain names.

Phishing in the UK

Similar campaigns have occurred in the UK utilizing Covid-19 themed domain names

Phishing emails designed to lure people into revealing passport details and other PII utilized the domain name: uk-covid-19-relieve.com

Quiz Question 1
It’s easy to tell if an email is legitimate

- A. TRUE
- B. FALSE
It’s easy to tell if an email is legitimate

- A. TRUE
- B. FALSE
Several recent campaigns have sent phishing emails that appear to be sent from legitimate WHO email addresses such as:

- eurohealthycities@who[.]int
- donate@who[.]int
- healthcaresupport@who[.]int

Tips for Staying Safe

- STOP. THINK. CONNECT. – Do not click on unknown links or open email from unknown senders, verify email headers
- Use Whois to try to determine if a domain name registration appears legitimate
- Protect your devices with an effective endpoint protection solution
- Provide cybersecurity training at your organization
- Test files and URLs before clicking on them by submitting them to free multi-scanner sites (e.g. www.hybrid-analysis.com)
Quiz Question 2
What’s an example of proactive anti-abuse?

- A. Investigating a domain name after it has been used for phishing
- B. Taking down a domain name after it has directed a user to malware
- C. Identifying a suspicious domain name before it has been used
- D. Preventing a registrant account associated with abuse from registering more domain names
- E. Both C and D
What’s an example of proactive anti-abuse?

- A. Investigating a domain name after it has been used for phishing
- B. Taking down a domain name after it has directed a user to malware
- C. Identifying a suspicious domain name before it has been used
- D. Preventing a registrant account associated with abuse from registering more domain names
- E. Both C and D
ccTLD and gTLD registrars face legal pressures to respond to abuse complaints in the form of contracts (ICANN accreditation for gTLDs), local laws, and community best practices.

There may be reputational incentives to be a clean registrar to avoid the ire of law enforcement and inclusion on blocklists.

Financial pressures from credit card chargebacks, court orders, lawsuits, loss of accreditation (gTLDs especially), and labor costs of responding to complaints.

Nonetheless, domain names impersonating the WHO, etc. are still successfully registered and used.
Quiz Question 3
Who is affected by DNS abuse?

- A. ICANN
- B. Contracted parties
- C. Only end users that click on the wrong link
- D. Consumers
- E. Everyone
Who is affected by DNS abuse?

- A. ICANN
- B. Contracted parties
- C. End users that click on the wrong link
- D. Consumers
- E. Everyone
Quiz Question 4
Who has the ability to prevent DNS abuse?

A. ICANN
B. Contracted Parties
C. End users
D. Cybersecurity experts
E. We all do
Who has the ability to do something about DNS abuse?

A. ICANN
B. Contracted Parties
C. End users
D. Cybersecurity experts
E. We all do
Internet governance matters

- The ICANN Community can raise awareness about DNS abuse
- ICANN can incentivize registrars and registries to undertake proactive anti-abuse measures
  - Scrutinize registrations that incorporate “covid-19”, “WHO”, “CDC”, etc.
  - Act quickly to mitigate DNS abuse once it’s discovered
- ICANN Org can deter contracted parties from being apathetic about DNS abuse
  - Use a data-driven approach to determining which parties are associated with high levels of abuse
  - Work with parties to mitigate abuse levels
Poll Questions
Have you been targeted by Covid-19 related phishing campaigns?

A. YES
B. NO
C. I DON’T KNOW
Have you received additional cybersecurity training from your employer since the Covid-19 pandemic began?

A. YES  
B. NO