SECUREDOMAIN FOUNDATION

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

SECUREDOMAIN
FOUNDATION

Phishing in Australia

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

Source: https://www.staysmartonline.gov.au/alert-service/covid-19-scam-messages-targeting-australians

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

```
Domain Name: uk-covid-19-relieve.com
Registry Domain ID: 2505659685_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2020-03-21T00:28:25Z
Creation Date: 2020-03-21T00:28:25Z
Registrar Registration Expiration Date: 2022-03-21T00:28:25Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: London
Registrant Country: UK
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=uk-covid-19-relieve.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=uk-covid-19-relieve.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=uk-covid-19-relieve.com
Name Server: NS19.DOMAINCONTROL.COM
Name Server: NS20.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-05-01T14:00:00Z <<<
```

Source: CrowdStrike, https://www.crowdstrike.com/blog/covid-19-cyber-threats/

Quiz Question 1

It's easy to tell if an email is legitimate

- A. TRUE
- B. FALSE

SECUREDOMAIN
FOUNDATION

It's easy to tell if an email is legitimate

- A. TRUE
- **B. FALSE**

SECUREDOMAIN
FOUNDATION

WHO focused phishing campaign

WHO domain
name spoofing

From: WORLD HEALTH ORGANIZATION (WHO) [mailto:healthcaresupport@who.int]
Sent: Thursday, March 26, 2020 3:05 PM
Subject: [W.H.O] COVID-19 VACCINE NOW AVAILABLE

World Health Organization

part(1):
AVALABLE COVID-19 VACCINE .doc 35 KB
Download All Attachment for Vaccine update(in .iso file) Download All Attachment for Vaccine Update (in .iso file)
1 unnamed 0.32 KB
Show this HTML in a new window?

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

SECURE DOMAIN FOUNDATION

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**

SECUREDOMAIN
FOUNDATION

LEGAL, REPUTATION, AND FINANCIAL VARIABLES:

- 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

SECURE DOMAIN FOUNDATION

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

SECURE DOMAIN FOUNDATION

Who is affected by DNS abuse?

- A. ICANN
- B. Contracted parties
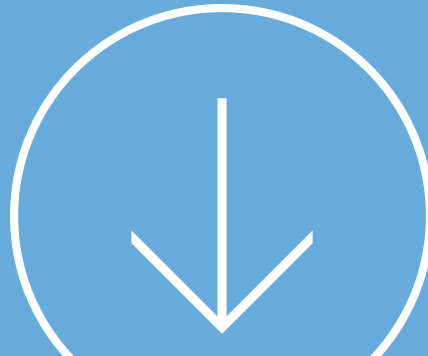- C. End users that click on the wrong link
- D. Consumers
- **E. Everyone**

SECURE DOMAIN FOUNDATION

Quiz Question 4

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

SECURE DOMAIN
FOUNDATION

Poll Questions

SECUREDOMAIN
FOUNDATION

www.securedomain.org

Drew Bagley
drew@securedomain.org