DOMAIN INDUSTRY IS PROFITING OFF ILLEGAL ONLINE DRUGS & COVID-19 SCAMS

ONLINE CRIMINALS ARE EXPLOITING THE PUBLIC HEALTH EMERGENCY FOR PROFIT

The pandemic has led to an explosion of cybercrime, preying upon a population desperate for safety and reassurance. These criminal activities require domain names, which are being used to run phishing, spam, and malware campaigns, and scam sites.[1]

- During March 2020, at least **100,000 new domain names** were registered containing terms like "covid," "corona," and "virus"[2], plus more domains registered to sell items such as medical masks.[3] Beyond this, other domains were used to spam out advertisements for COVID-themed scams.
- As of March 2020, the number of confirmed *malicious* COVID-related domains is in the thousands.
- Nearly 6,500 of those domains have the ability to send and receive email -- which is a strong indication that they could be used in phishing, fraud or business email compromise attacks.
- 122 of the names also contain the string "vaccine" and over 400 contain the string "test" with well over 20% of both those sets of names also ready to send and receive email.

BUT THERE IS A SOLUTION: DOMAIN INDUSTRY ACCOUNTABILITY

Domain name registries and registrars (R/R) must act to stop online COVID-19 scams, and sales of illicit opioids and of counterfeit or unapproved prescription drugs.

- R/Rs have the power to stop massive amounts of public health harms and fraud online.
- R/Rs should immediately, upon notice from a credible party, lock and suspend any domain name that is used to facilitate the COVID-19 scams and the illegal online sales of medicines and illicit drugs.
- Some U.S.-based R/R will shut down *(i.e. lock and suspend)* rogue websites based on information from trusted third-party notifiers like LegitScript, U.S. FDA and others. But many others do not and often serve as safe-havens for illicit activity.
- Especially during a Public Health Emergency, we need *all* actors – including R/Rs – to do whatever they can to stop online COVID-19 frauds and the illegal sale of healthcare products online.

WHAT ARE DOMAIN NAME REGISTRIES & REGISTRARS?

- **A domain name registry company creates, operates, and enforces requirements for domain extensions such as .com, .edu, .org, and tech.** Examples of registries include Verisign, Radix, Neustar, etc.
- **A domain name registrar is an accredited company that sells domain names to the public.** Examples of registrars include GoDaddy, Epik, Tucows, Domain, Hover, etc.

HISTORY OF ALLOWING PUBLIC HEALTH HARMS ONLINE

[1] "The Internet is drowning in COVID-19-related malware and phishing scams." Ars Technica, 16 March 2020, at: https://arstechnica.com/information-technology/2020/03/the-internet-is-drowning-in-covid-19-related-malware-and-phishing-scams/and "Coronavirus Used in Malicious Campaigns." Trend Micro, 20 March 2020, at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

[2] Don't Panic: COVID-19 Cyber Threats." Palo Alto Networks Unit 42 blog, 24 March 2020, at: https://unit42.paloaltonetworks.com/covid19-cyber-threats/

[3] "Domain Name Registration Data at the Crossroads: The State of Data Protection, Compliance, and Contactability at ICANN." Interisle Consulting Group, LLC, 31 March 2020, page 18, at: http://bit.ly/DataCrossroads

According to the U.S. Food and Drug Administration (FDA)[4], registries and registrars often will not act to prevent public health harm online without a specific court order. This has been true even when:

- The domain names themselves explicitly imply illegal activity (e.g. www.covidcures.com)
- The R/R has been notified by a trusted third-party that certain domain names on their platform are being used in violation of the R/R's own contracts (terms of use agreements)
- The R/R has knowledge that a domain name is unequivocally being used to sell opioids, offer COVID-19 "cures," or otherwise endanger public health and safety

THE RESULT: R/Rs are profiting from licensing domains names that create and/or exacerbate existing public health harms. This puts lives at risk, especially in a Public Health Emergency when millions of Americans are sheltering-in- place and rely on the internet for access to healthcare information, products, and services.

WHY THE ONLINE SCAMS ARE ESPECIALLY HARD TO COMBAT

Historically, public and private cyber investigators and first-responders could "triage" attacks by obtaining information about thousands of domain names using a service called WHOIS in near real-time.

- These parties are responsible for the majority of the more than two billion WHOIS queries every day, most of those in automated fashion, to track and measure the proper functioning of domain names, and to judge the risks they pose.
- But over the last two years, access to WHOIS data has been drastically curtailed as a result of ICANN policies, the EU data privacy laws, and to the elective practices of registrars and registries.

COVID-themed attacks are easier to conduct and harder to mitigate because domain industry policies and business interests interfere with the acquisition of information that's essential to investigation, identification, mitigation, and apprehension of the criminal actors.

- In a correspondence to registrars GoDaddy, NameCheap, Register.com and others, the NYC Office of the Attorney General states that, "the current environment demands the highest vigilance" and has asked the registrars for proactive steps to prevent, find, and suspend these malicious domains.
- The U.S. Department of Justice notified registrar NameCheap that "Communications facilitated by your entity and made by your direct customers or business partners have been linked to [such] criminal activity", referring to fraudulent schemes targeting U.S. citizens exploiting the current COVID-19 pandemic.

POLICYMAKERS CAN FORCE THE U.S.-BASED DOMAIN INDUSTRY TO ACT

Immediate action is required to protect American citizens from ongoing harm and to maintain the trust and integrity of the Internet during a time where it is relied upon most:

- Registrars must lock and suspend when COVID-themed domain names are suspicious or when first responders provide evidence that they are harmful.
- To maintain internet security and transparency, legislation is needed to require registries and registrars to provide open access to WHOIS records that are accurate, non-anonymous and accessible at scale.

[4] FDA Presentation at ASOP Global Foundation Research Symposium, November 2018: https://asopfoundation.pharmacy/wp-content/uploads/2018/11/DAshley-ASOP-Global-Foundation-Research-Symposium-Presentation-11.14.2018.pdf*; See also* FDA Registry and Registrar Abuse Complaints, https://www.fda.gov/consumers/health-fraud-scams/registrar-and-registry-abuse- complaints.