Industry Brief

Domain protection during COVID-19: More important than ever

The way we do business has dramatically changed with COVID-19. Millions of people are being asked to work from home and many organizations are using virtual platforms for their meetings, conferences, and events. Unfortunately, the surge in video conferencing has also led to a surge in bad actors looking to capitalize on this trend.

Zoom.us, an online video conferencing platform, has seen exponential growth in popularity since the health crisis. In March, the **number of daily Zoom meeting participants reached over 200 million**. Opportunistic cyber-criminals, looking to cash in on Zoom's popularity, have been quick to act, targeting users of this popular platform.

In a **recent webinar hosted by the Cyber Tech Accord**, Greg Aaron from Illumintel stated there were 1,054 attacks against Zoom in April of 2020. The majority of these attacks were phishing attacks disguised as fake meeting notifications. Others were links offering victims malware disguised as software downloads.

In situations like this, bad actors are relying on brand confusion to perpetrate their crimes. While the domain Zoom.us leads directly to the legitimate site, bad actors are snapping up variations of this domain name, including variations in both the domain name and top-level domain extension (TLDs).

Bad actors are also targeting terms directly related to the health crisis in domain name registrations. During the earliest days of the pandemic, our analysts discovered more than 22,000 domains containing the strings COVID, COVID-19, or Coronavirus registered between January and March of 2020.

Brands must remain vigilant and proactive in monitoring new domain name registrations for use of their trademarked names and IP to prevent abuse, a formidable task. According to Verisign's most recent **Domain Name Industry Brief**, domain name registrations have grown by 13.5 million, or 3.9 percent, year over year, as of the end of 2019.

In addition, the implementation of the General Data Protection Regulation (GDPR) and the Internet Corporation for Assigned Names and Number's (ICANN) conservative temporary policy which favors privacy and limits registrar liability, have made it exponentially more difficult, expensive and slow to enforce against cybersquatters, cybercriminals, and infringement. Partnering with a brand protection agency can help alleviate this burden.

Brands and their customers both suffer the effects of fraud and the betrayal of trust when bad actors are allowed to operate with impunity online. When an infringing domain is discovered, swift and decisive action is necessary. To help combat abuses and make digital channels safer for everyone, we've created a **guide to domain name enforcement**, including sample templates for reporting infringement, for brandholders and their legal teams to use.

Subscribe to Our Blog for More Industry Briefs.