THOMSON REUTERS
Westlaw®

COVID-related cybersquatting underscores importance of vigilant trademark policing

By David J. Steele, Esq., and Helena M. Guye, Esq., *Tucker Ellis LLP*

NOVEMBER 13, 2020

While most of the world has come to a standstill due to the COVID19 outbreak, cybercriminals have been working furiously to exploit the global turmoil. Since February 2020, the number of COVID19-related domain names registered has skyrocketed.

While some of these domain names host legitimate sites and provide useful information and resources about the pandemic, most provide misinformation, or are used in scams, phishing or malware attacks. Most of these domain names trade on the goodwill of trademarks to promote their schemes.

As global lockdowns have forced companies and consumers alike to rely on the Internet, vigilant trademark policing online has never been more urgent.

COVID-19-RELATED CYBERCRIMES

In December 2019, the novel coronavirus was first identified in China.[1] By September 2020, over 160,000 COVID-19-related domain names had been registered.[2] One study by Palo Alto Networks found that of the 116,657 COVID-19-related domain names registered between January and March, at least 2,022 were malicious and 40,261 were "high-risk."[3]

While the rate at which these domain names are registered has slowed, little has been done to effectively thwart their creation.[4] As the virus continues to develop and the world responds, trademark owners must understand both the risks these criminals pose and how to combat them.

The spread of misinformation regarding the coronavirus has been prevalent during the COVID19 pandemic.[5] A number of domain names host websites dedicated to the spread of materially false information about COVID19, from basic misunderstandings about the virus, to inaccurate medical information and full-blown conspiracy theories.[6]

Some of these sites, for example, purport to have discovered cures for COVID19, such as colloidal silver, vitamin C, garlic, or lemon and hot water (despite no evidence supporting such claims).[7] Other sites are devoted to propagating myths like "getting a flu shot increases your risk of COVID19" or, of course, "5G cell phone technology is linked to the outbreak" (again, this is not true).[8]

A number of COVID19 domain names resolve to websites dedicated to stealing visitors' personal information. Most frequently, these sites involve fake products or services. Some sites imitate government agencies and induce individuals with false offers of cash from a fictitious economic stimulus packages or the like.[9]

Often the sites seek to gain access to either personal information or financial information. Similarly, numerous domain names host malicious content that installs malware on a PC.[10]

> Some companies have defensively registered COVID-19-related domain names incorporating their existing marks.

Since the COVID-19 outbreak, phishing attempts have also been particularly rampant.[11] Phishing emails, which can be sent to personal or work email accounts, commonly imitate legitimate organizations.

For example, phishing emails may look as though they originate directly from the U.S. Centers for Disease Control or the World Health Organization, while others may impersonate a member of company's management team.[12]

By April, more than 700 domain names that are confusingly similar to popular streaming services like Netflix and Disney Plus were registered.[13] Similar trends were seen with video conferencing services like Zoom and Microsoft Teams.[14]

These infringing websites have fraudulently offered free services or subscriptions in attempts to gain access to an individual's personal or financial information.[15]

THE PROBLEM FOR TRADEMARK OWNERS

Not only are these criminals invoking hot-button COVID-19-related terms to lure Internet users, many also incorporate trademarks to boost the credibility of the domain names and lure consumers to these fraudulent sites.

Government agencies, the healthcare and medical goods industry and technology companies have been especially targeted by this

new vector of cyber threats.[16] For example, a slew of infringing domain names were recently detected by Verizon.[17]

Of particular concern were the domain names myverizonwirelessCOVID19.com and verizonwireless-COVID19.net, which resolved to sites imitating Verizon's legitimate site.[18] Verizon filed a complaint with the World Intellectual Property Organization ("WIPO"), which provides domain name dispute resolution services through its Arbitration and Mediation Center.[19]

Citing a lack of legitimate rights and the clear bad faith on the part of the registrant, WIPO ordered the transfer of the domain names to Verizon.[20] These were not the only domain names incorporating the Verizon trademark illegitimately — Verizon also recovered verizonCOVID19.com, verizonCOVID19.com and verizonCOVID19.info from registrants after requesting their identification.[21] Many other brands have fallen victim to similar schemes.[22]

Some companies have defensively registered COVID-19-related domain names incorporating their existing marks. Facebook, for example, registered over 500 domain names incorporating COVID-related terms and their Facebook and Instagram trademarks (e.g., facebook-coronavirus-info.com and instagramCOVID19.tld).[23] Apple, too, has registered the domain name AppleCoronavirus.com.[24]

EFFORTS TO COMBAT COVID-19 RELATED CYBERCRIMES

Last month, the number of consumer complaints to the U.S. Federal Trade Commission related to COVID19 surpassed 200,000, with reported fraud losses exceeding $140 million.[25]

These numbers, along with general fears about the spread of misinformation, have raised alarms among lawmakers and consumer protection groups alike. Calls to action have been made, but largely remain unanswered.

The difficulty quelling these domain name registrations stems in part from a lack of compliance efforts by The Internet Corporation for Assigned Names and Numbers ("ICANN"), the administrative body that coordinates and manages the domain name space. Thus far, ICANN has only appealed to domain name registrars to police fraud in a letter, asking them to systematically identify and review possible abuses.[26]

The response from domain name registrars, who profit from domain name registrations, has been woefully lacking. While some registrars like GoDaddy will investigate and remove abusive sites in response to a credible report,[27] many registrars entirely ignore reports of fraud and abuse.[28]

For example, after receiving no reply its notice, the U.S. Department of Justice, took the extraordinary step of filing suit in federal court and seeking a temporary restraining order to shut down the domain name coronavirusmedicalkit.com, a site offering bogus "free vaccine kits."[29] The court ordered the domain registrar, NameCheap, to disable the domain name and to serve a copy of the order on its customer.[30]

In April 2020, U.S. Senators Maggie Hassan (D-N.H.), Mazie Hirono (D-Hawaii) and Cory Booker (D-N.J.) sent joint letters to the executives of various domain name registrars in hopes of pushing them to act.[31]

> Companies should respond both offensively and defensively to properly protect their marks.

Despite this effort, government actors are facing an uphill battle in preventing the further proliferation of these cybercrimes.

PROTECTING YOUR COMPANY AND CUSTOMERS

It is imperative that trademark owners take action to prevent online cybercriminals from utilizing the company's trademarks in furtherance of their fraud.

Companies should respond both offensively and defensively to properly protect their marks, taking steps to prevent the registration of infringing, malicious domains and responding to their registration.

Companies should look to brand protection technologies and experts to provide additional support. For example, trademark owners should utilize a domain name monitoring service to monitor and detect new registrations containing a trademark (or variants).[32]

Similarly, service providers can also monitor social media sites and websites for improper use of trademarks (and even the names of key executives).[33] Additionally, service providers can monitor for phishing and malware targeting trademarks.[34]

These services provide early notice of potential problems and inform appropriate enforcement action. Lastly, companies should also consider registering multiple domain names that are confusingly similar to their brand purely for defensive purposes.

In the event an infringing domain name is registered, trademark owners have a number of legal and non-legal remedies available, with varying degrees of cost and efficiency.

In the most extreme matters, or where immediate action is needed, trademark holders can file a lawsuit seeking injunctive and/or monetary relief under the Anticybersquatting Consumer Protection Act ("ACPA"), 15 U.S.C.A. § 1125(d).[35]

If online content does not involve cybersquatting (i.e., use only on a website or social media platform), a conventional trademark infringement and/or false designation of origin lawsuit would be equally viable.

An alternative to cybersquatting litigation is the ICANN Uniform Domain Name Dispute Resolution Policy ("UDRP"). The UDRP is a material term to nearly all domain name registration agreements, and provides an efficient tool to recovering infringing domain names. Proceedings are typically resolved in 5-7 weeks and, assuming the complainant prevails, the domain name is transferred 10 days later. However, no injunctive relief or damages are available, only the transfer of the domain names.

Another sometimes-overlooked option is the federal Digital Millennium Copyright Act ("DMCA"), which provides effective content takedown procedures that are followed by many Internet hosting companies. 17 U.S.C.A. § 512(c).

Because many scams involve using copies of the trademark owner's website, infringers commonly copy one or more of the company's copyright protected photographs or graphics. Sending a DMCA takedown notice to the hosting company may result in the entire website being taken down by the hosting company.

If successful, this technique can get an offending website taken down while a UDRP proceeding is being pursued.

Several other tools exist and can be used in combination, including with the tools discussed above. For example, filing a complaint with the domain name registry, registrar, or website hosting company, or one or more "black hole" websites when a domain name is used for phishing attacks or mail spamming, have also proven effective.

Filing a complaint with all of them will simply increase the odds that the website is taken down. Additionally, following up by email, letter and telephone has also proven to be more effective than not following up.

Lastly, for more egregious matters, consider reporting the incident to the Internet Crime Complaint Center[36] or local law enforcement.

CONCLUSION

Cybercriminals will continue to exploit the COVID19 pandemic to engage in various types of cybercrime, especially attacks that utilize trademarks in domain names.

Trademark owners must be vigilant and increase their policing efforts to protect the company and its customers. Effectively using existing commercially available monitoring tools, and taking appropriate enforcement actions to combat these attacks, will mitigate any likely harm.

Notes

[1] Hudson Institute, Coronavirus Timeline, Hudson.org, https://bit.ly/32blkth (last updated Oct. 16, 2020).

[2] Hold Integrity, Domain Registration Data, holdintegrity.com, https://bit.ly/383Lulz (last updated Sep. 9, 2020). Hold Integrity, a Wisconsin-based domain name monitoring service provider, publishes a running list of COVID-19 related domain names.

[3] Janos Szurdi, Zhanhao Chen, Oleksii Starov, Adrian McCabe and Ruian Duan, "Studying How Cybercriminals Prey on the COVID-19 Pandemic," Palo Alto Networks (Apr. 22, 2020, 6:00 AM), https://bit.ly/3elhvXg.

[4] "Sipping from the Coronavirus Domain Firehose," Krebsonsecurity.com (Apr. 16, 2020), https://bit.ly/35YcQGZ.

[5] Amir Bagherpour, "COVID Misinformation is Killing People," Scientific American (Oct. 11, 2020), https://bit.ly/3jVQuuN.

[6] See Tonya Riley, "The Cybersecurity 202: Internet domain names are ripe for scam during coronavirus crisis," The Washington Post (Sep. 8, 2020), https://wapo.st/3enR4Ag.

[7] U.S. FDA, Fraudulent Coronavirus Disease 2019 (COVID-19) Products, fda.gov, https://bit.ly/2GmSO02 (last visited Oct. 27, 2020). The Food and Drug Administration publishes a list of warning letters it has issued to firms selling fraudulent products that claim to prevent or treat coronavirus.

[8] See NewsGuard, Coronavirus Misinformation Tracking Center, newsguardtech.com, (last visited Oct. 27, 2020) https://bit.ly/3el4AEO.

[9] Lee Clifford, "Scammers have registered 150,000 fake stimulus check websites. Here's how to protect yourself," Fortune (Apr. 28, 2020, 5:00 PM), https://bit.ly/34TkuTJ.

[10] For example, see *Commissioners for HM Revenue and Customs v. Khasanov*, No. D2020-1074, 2020 WL 3639828 (WIPO Arb. Jun. 26, 2020) (use of hmrc-refund-covid-19.com to distribute malware).

[11] Tom Kelly, "How hackers are using COVID-19 to find new phishing victims," Security Magazine (Jun. 23, 2020), https://bit.ly/327c2OW.

[12] See Steven Merrill, "Protect Your Wallet — and Your Health — from Pandemic Scammers," fbi.gov, https://bit.ly/3enJBBt. *See also Princess Cruises Lines Ltd. v. Yamshikov*, No. FA 2005001898334, 2020 WL 4595999 (Nat. Arb. Forum July 3, 2020) (Impersonating company president and seeking personal information from complainant's employees in connection with phishing).

[13] Phil Muncaster, "Hackers Target Netflix and Disney+ with #COVID19 Phishing," Infosecurity Magazine (Apr. 22, 2020), https://bit.ly/329nHNi.

[14] Jay Peters, "Hackers are impersonating Zoom, Microsoft Teams, and Google Meet for phishing scams," The Verge (May 12, 2020, 6:00 AM), https://bit.ly/3jSPPKw.

[15] *Id*.

[16] *See, e.g., Gilead Sciences Inc. v. Main Contact*, No. D2020-0776, 2020 WL 2320037 (WIPO Arb. May. 5, 2020) (passively holding coronagileadsciences.com domain names); *Gilead Sciences Inc. v. JH Kang*, No. DCO2020-0019 (WIPO Arb. May. 28, 2020) (use of gileadcopay.co in connection with a parked website that displays links or pay-per-click advertisements); *Sanofi v. Liu*, No. D2020-0617, 2020 WL 2619858 (WIPO Arb. May. 15, 2020) (use of sanofivaccine.com in connection with parking pages); *Reckitt & Colman (Overseas) Health Limited Reckitt Benckiser (India) Private Limited v. Madhumita Mohan*, No. D2020-0990, 2020 WL 4448573 (WIPO Arb. Jul. 20, 2020) (use of dettoldisinfectantspray.com, dettolhandsanitizer.com and dettolhandwash.com in connection with landing pages containing links to third parties providing competitive goods).

[17] *See Verizon Trademark Services LLC v. Walker*, No. D2020-0960, 2020 WL 2836417 (WIPO Arb. May. 26, 2020) (Respondent used myverizonwirelesscovid19.com and verizonwireless-covid-19.net to impersonate the complainant and perpetrate a phishing scheme).

[18] *Id*.

[19] *Id*.

[20] *Id*.

[21] "Verizon recovers infringing covid-19 domain names"; "Michael Jordan ends long-running dispute"; "Syria fee changes — news digest," (Apr. 14, 2020), World Trademark Review, https://bit.ly/2TRtEdi.

[22] *See, e.g.*, *Facebook Inc. v. Super Privacy Service LTD c/o Dynadot / Xiamen Tianmu zhuangshi sheji youxian gongsi*, No. D2020-0885, 2020 WL 2619886 (WIPO Arb. May. 18, 2020) (use of facebookcovid19.com in connection with a parking page displaying PPC links to various third-party products); *Google LLC v. Ghosh*, No. FA2003001888606, 2020 WL 2488805 (Nat. Arb. Forum Apr. 3, 2020) (use of googlecoronavirus.com); *Citizens Financial Group Inc. v. Rodrigues / Fundacion Comercio Electronico*, No. FA2004001894431, 2020 WL 3077004 (Nat. Arb. Forum May. 30, 2020) (use of citizensbankppp.com to resolve to a website with links to competitor).

[23] Andrew Allemann, "Facebook registers over 500 Covid-19 related domain names," Domain Name Wire (Apr. 2, 2020), https://bit.ly/2GnpNBp.

[24] *See* World Trademark Review, *supra* note 21.

[25] *See* Chris Melka, "COVID-19 domains: what's going on?," Clarivate (Apr. 9, 2020), https://bit.ly/3jWYU50.

[26] Letter from ICANN President & CEO to gTLD Registries and Registrars, ICANN, https://go.icann.org/389hyoe (last visited Oct. 30, 2020).

[27] James Bladel, "GoDaddy combats coronavirus-related fraud and abuse," GoDaddy.com (Mar. 26, 2020), https://bit.ly/2TNE7WS.

[28] *See* Krebsonsecurity.com, *supra* note 4.

[29] *United States v. Doe*, No. 20-cv-306, 2020 WL 1426796 (W.D. Tex. Mar. 22, 2020).

[30] *Id*.

[31] "Hirono, Booker, Hassan Call on Domain Name Gatekeepers to Combat Coronavirus-Related Scams and Misinformation," (Apr. 14, 2020) Hirono.Senate.Gov, https://bit.ly/32zJWMt (last visited Oct. 30, 2020).

[32] An internet search using Google.com for "domain name monitoring services" provided a list of multiple companies providing domain name monitoring services.

[33] An internet search using Google.com for "social media monitoring tools" provided a list of multiple companies providing social media monitoring services.

[34] An internet search using Google.com for "phishing monitoring services" provided a list of multiple companies providing phishing and malware monitoring services.

[35] For example, *see 3M Co. v. Performance Supply LLC*, 458 F. Supp. 3d 181 (S.D.N.Y. 2020) (granting preliminary injunction against unauthorized resellers of PPE utilizing 3M's trademarks).

[36] www.ic3.gov.

This article was published on Westlaw Today on November 13, 2020.

ABOUT THE AUTHORS

David J. Steele (L) is a partner at **Tucker Ellis LLP** in Los Angeles who practices trademark and internet law. He focuses much of his time protecting well-known trademarks from infringement of all types, and has successfully handled hundreds of cybersquatting matters, including numerous federal cases. He is an adjunct professor at Loyola Law School in Los Angeles, where he has taught trademark law and internet law since 2001. He can be reached at david.steele@tuckerellis.com. **Helena M. Guye** (R) is an associate attorney at the firm's St. Louis office, focusing her practice on intellectual property litigation. She handles a variety of matters, including trademarks, copyrights, patents and trade secrets, and can be reached at helena.guye@tuckerellis.com. This article reflects the situation at the time it was written based on the rapidly changing nature of the COVID-19 pandemic.