LexisNexis® Intellectual Property

Defending Brands - New Realities, New Partnerships

How IT Security and Brand Protection Teams Can Collaborate to Reduce Brand Abuse Across Customer-Facing Digital Channels — and Enhance Brand Resiliency

Introduction

The first decade of the 21st century saw a new phenomenon: the rise of the digital world. E-commerce, social media, mobile computing, smartphones, and remote work ushered in new ways of conducting business, learning, entertaining ourselves and connecting with others.

A parallel, yet unsurprising, phenomenon — the rise of brand weaponization online — emerged during this time, as the on-demand economy became the norm. Unscrupulous, profit-seeking actors instantly recognized the vast opportunity to use the power of well-known brands, and fast-growing digital channels for consumer-brand interaction, to lure unsuspecting users to sites containing scams, malware, and counterfeit goods.

Now, 20 years into the new century, we see the digital world expanding not only further, but also, more rapidly. Consider the following figures and trends:

- From 2016 to 2019, mobile app downloads worldwide increased from nearly 141 billion to 204 billion.[1]
- In 2018, an estimated 1.8 billion people worldwide purchased goods online; that figure is projected to rise to over 2.4 billion people by 2021.[2]
- There are more than 3.8 billion social media users worldwide[3]. And they spend an average of two hours and 24 minutes per day multi-networking across an average of eight social networks and messaging apps.

In short, people can interact even more immediately, frequently, and intimately with their favorite brands through public, customer-facing digital channels, using any device. True to form, malicious actors have responded by using these channels to their advantage. They are abusing brands — and users' trust in brands — to make mischief and profit. That is hurting businesses worldwide: Consider that the sale of counterfeit and pirated goods alone could displace up to $1.2 trillion dollars of legitimate companies' global sales by 2022.[5]

A New Perspective: Legal and IT Security Teams as Brand Defenders

The most organized, well-funded, and economically motivated actors engaged in brand abuse are creating sophisticated, multichannel campaigns that are difficult to investigate and remediate. That reality is creating more demands on brand protection and legal teams charged with securing intellectual property in their organizations and opens an opportunity to collaborate with IT security teams — including those responsible for cybersecurity, threat intelligence, fraud prevention, and security operations centers (SOC).

Working together on the front lines as "brand defenders," security and legal teams can combine their resources and methods to identify, investigate, and abate incidents of online brand abuse and related crimes. Currently, despite their shared mission and adversaries, these teams typically work independently from each other, operating in functional silos and using disparate systems, tools, and processes. Often, they may be unaware of each other's similar efforts, until their paths must cross in the wake of a serious incident of brand abuse that must be investigated and remediated as quickly as possible.

This approach to team collaboration is reactive, not proactive — and thus, ineffective for keeping pace with the diverse array of brand threats emerging in, and often straddling across, customer-facing digital channels. A better plan is for these teams to work in tandem on monitoring brand abuse, and to exchange relevant data about key threats, as needed, with speed and ease. By combining traditional security data with brand abuse data, these teams can uncover higher-risk bad actors, new patterns of abuse, and new tactics. Together, they can help the business gain a more holistic view of threats — and find more success in thwarting brand abuse across multiple digital channels.

By committing to active collaboration and employing the right technology to detect and stunt threats, legal and brand protection teams and IT security staff can mount an even more robust defense of intellectual property and brands in the digital world. They can also create a strong offense that helps to reduce the the 'time to live' or, in security parlance, the meantime to remediate (MTTR) for these pervasive and costly threats, which range from fake domains to apps impersonating brands in third-party app stores to abuse of review and ratings processes on brand platforms.

> **By working together, brand defenders will gain greater insight, prioritize responses — and strengthen brand resiliency.**

General Counsel (GC), head of intellectual property, and other leaders in the legal function will want to consider working with chief information security officers (CISOs) and other security leaders to make this collaboration a reality. Doing so can help ease the work burden on both teams and make them more effective in their roles overall. And, this collaboration can help to increase brand resiliency by ensuring the brand can stay strong — and retain customers' trust — even when it inevitably faces threats in the digital landscape that are designed to undermine, or take advantage of, the brand's good reputation and value.

This white paper explores both the challenge and opportunity that legal and IT security teams face as united brand defenders in the digital world. It examines some of the ways that malicious actors are weaponizing brands across customer-facing digital channels, and it outlines the economic impacts of brand abuse conducted in these channels. Also presented are some best practices and strategies that legal and IT security teams can use to respond to brand attacks more swiftly and effectively — together.

How Bad Actors Weaponize Brands Across Multiple Digital Channels

Let's begin with an example of how bad actors take advantage of brands and weaponize them: A consumer packaged goods, (CPG) company's digital marketing team builds and launches a mobile app intended to drive customer loyalty, and enthusiasm for a well-known sports drink brand. The highly interactive app lets fans form their own virtual sports team, design a logo and uniforms, create a stadium and team bus, and more.

Malicious actors hijack this customer loyalty campaign by creating their own version of the app — thereby infringing on the CPG brand's intellectual property. Then, they make their cleverly designed, brand-infringing app available in various third-party app stores. But they don't stop there. Next, they run ads in paid search and social media to promote their app. They even go so far as to adapt the app and related promotional strategies to cater to local dialects and customs of specific target audiences in various countries.

The fraudulent app is dangerous to users in that it demands that the users agree to excessive permissions in order to access certain features of the app. Trusting the brand name associated with it and assuming that the app is legitimate, hundreds of users freely accept the terms. The app then proliferates across the users' contact lists — ultimately allowing the digital criminals behind the campaign to harvest the personally identifiable information (PII) of those contacts and target them in additional scams.

Weaponized Brand: Red Flag

Attacks that feature hijacked brands can deliver a wide range of threats to unsuspecting users, ranging from confusion and inauthentic experiences to dangerous malware. Apps with over-reaching permissions, as described in the example in this paper, are a way for adversaries to extend the reach of their campaigns even further by tapping into users' contact lists.

Brand Abuse Can Arise Anywhere in a Consumer's Online Journey

The scenario of the CPG firm is just one example of an attack that exploits a brand. Of course, adversaries don't need to go to such lengths to abuse brands and take advantage of users. There are many places online where consumers interact with brands and where digital criminals can introduce threats.

For example, a consumer's online journey to learn more about a specific brand could easily include any, or all, of the following activities, experiences, and digital touchpoints:

- Viewing social media posts
- Conducting searches on the web and in major and third-party app stores
- Viewing online ads served up in search results or through retargeting
- Receiving an email with an offer
- Visiting a website or an e-commerce marketplace listing

Malicious actors can prey upon consumers at any of these touchpoints by using brands as tempting lures, exploiting users' trust in those brands, as well as in the digital channels they are using to interact with those brands. Through social engineering and technology-driven exploits, adversaries can divert consumers from their intended path, and then monetize their activities by selling fake products in marketplaces or stealing their identities with malware — to name a few tactics.

And why wouldn't digital criminals try to cut into the consumer's buying journey, given how much time and money people spend online? For instance, nearly one-third of adults in the United States (28%) report that they are online "almost constantly," according to a recent Pew Research Center survey.6 And e-commerce spending by U.S. consumers alone is projected to reach nearly $970 billion by 2023 — up from about $567 billion in 2019.[7]

Granted that e-commerce spending projection was made prior to the COVID-19 pandemic. However, it stands to reason that even with this black swan event disrupting the global economy, e-commerce spending will only continue to grow over time. And so, too, will online purchasing scams. In 2019, these scams represented nearly one in four complaints to the Better Business Bureau (BBB), with more than 81% of consumers reporting that they had suffered a financial loss.[8] Often, these impersonation schemes exploit the brand names associated with some of the world's top-trafficked websites.

Weaponized Brand: Red Flag

As part of the groundwork for launching an attack, adversaries will often register domain names that include the name of the brand they want to exploit in their malicious campaign (e.g., getanalysisofyour-BANKNAMEstatment.com). They will also register multiple variants of domain names, along with different top-level domains.

The Economic Impact of Online Brand Abuse for Enterprises and Consumers

Unfortunately, abusing brands and launching attacks across customer-facing digital channels has never been easier for unscrupulous actors. And the impact of these campaigns can be severe — for both enterprises and consumers.

The impacts of attacks using hijacked brands include damaged customer relationships and eroded brand reputation. Consumers lose trust, and word of their poor brand experiences can easily spread like wildfire through digital channels, causing other loyal consumers to lose trust. The risk of unflattering media exposure may follow such an attack as well. Depending on the severity of the issue, the business may find it needs to invest more in customer service to manage customers' complaints, and in media and customer relations for damage control.

There is also the potential for significant loss of revenues. The latter losses can be especially staggering when they involve the sale of counterfeit goods that goes unabated for an extended period. According to a recent report by the EU Intellectual Property Officer (EUIPO), global sales of counterfeit products exceeds $522 billion annually and represents 3.3% of world trade.[9]

Another financial impact for enterprises due to weaponized brands is increased advertising and marketing costs, as brands find they must bid against malicious actors for their own branded keywords — and their rightful share of attention in customer-facing digital channels.

As for consumers, brand abuse can lead to a poor experience and inconvenience, as well as actual harm. There is the financial impact of identity theft as an example. And there is the potential risk to the physical health or well-being of a consumer, if that individual purchases, and then uses or consumes, substandard or dangerous products.

The Tainted Code Risk

Even seemingly benign brand-infringing activity on websites or in apps can represent a risk to enterprises. For example, an homage from a fan can become a malevolent threat when its creator unknowingly uses tainted code from a software development platform like GitHub.

This can, in turn, lead to user compromise and exposure to scams that could ultimately threaten the continuity of a company's digital business and its digital brands.

How Brand Protection and Security Teams Can Detect and Respond to Online Brand Abuse — Together

There are many commonalities in the work that IT security and legal teams do independently to undermine the efforts of malicious actors. These teams also have a shared purpose and vision: They both want to protect the business, its brand and reputation, and its users and customers — and take down bad actors.

The reality is that these teams also need to work together. If they want to be effective in achieving their purpose and realizing their vision, they can't go it alone in the digital world. There is simply too much ground to cover, and the threats are myriad. However, when these teams combine their efforts and resources, including their data, they not only can detect threats faster but also reduce the time to live or MTTR of these threats. This is critical, because in the digital world, not moving fast enough to ensure the integrity of consumer-brand interactions in every digital touchpoint means increased risk for customers and brand holders.

That said, getting these two functions to collaborate is not as simple as flipping a switch. These teams may not be used to sharing information and typically have very different approaches to their work. With that in mind, here are five steps that GCs and CISOs can take to align their teams to create a more unified group of brand defenders:

1 Create shared workflows.

Brand protection and IT security teams need to optimize workflows so that they can expedite top priority remediations. And by optimizing these workflows, the business can then track and monitor the status of its brand protection program from the initial identification of a threat through to enforcement. That's why it's critical to determine this framework upfront, and not when a threat emerges.

2 Formalize data sharing and risk mitigation protocols.

Deciding how to formalize data sharing and which risk mitigation protocols to use are issues that should be considered from the outset as well — ideally when establishing the framework for creating shared workflows. Some questions to consider include:

- How will our functions share and correlate information in a timely fashion? What tools will they use to share data? How will we capture and preserve evidence in case we determine that civil or criminal litigation is warranted in the future?
- What sorts of activities (e.g., tabletop exercises) should we use to plan our response to frequently seen patterns of brand abuse?
- When a threat is discovered, what steps will we take to work together to stop it and reduce its impact and MTTR? What protocols should we follow in terms of escalating incidents, and are there associated actions to take such as blocking traffic from a suspicious domain?
- In the event of a major crisis involving brand abuse, what is the action plan for a response?

3 Choose metrics for measuring progress — and success.

Once the "how" of working together is outlined, CISOs and GCs will want to decide on the metrics their teams will use to gauge their success (or need for improvement) in fighting brand abuse. One measurement could be tracking MTTR, for example, and how that figure is being reduced over time.

Also, as lessons are learned about what works well and what doesn't in terms of identifying and remediating brand threats, that information should be integrated into the teams' shared workflows to help inform future work.

4 Sweep and monitor digital channels.

The brand protection team and the IT security team — along with other business groups such as marketing — should work together to sweep and monitor digital channels both before and after the launch of a new product or promotion. Combining brand and security data feeds can help to uncover more instances of emerging brand abuse sooner and identify correlation points for further investigation. This process needs to start well before the launch date of the product or promotion and continue for as long as deemed necessary.

5 Continue applying function-specific expertise and tools.

The legal and IT security functions have their own tools, systems, and data for investigating and mitigating threats. They should continue to use these resources to uncover and abate all aspects of a brand attack and monitor malicious activity. What will be different moving forward, though, once these two functions commit to more formal collaboration, is how they exchange data throughout an investigation.

Ideally, the teams will use collaboration hubs to facilitate data exchange, help manage workflows and provide access to remediation capabilities, advanced analytics, reporting, and evidence preservation. The system they select also should be capable of continuous monitoring since no human team can track incidents of new and unknown brand abuse across all digital channels around the globe, and around the clock. And the technology they use should provide them with the insight and tools to help them not only find, but also thwart, sophisticated criminal networks that are abusing the organization's intellectual property, trademarks and brands.

Conclusion: A Positive Cycle That Can Strengthen Brand Resiliency

Weaponized brands used in online attacks threaten the continuity of digital business. Within a matter of clicks, even the most well-known brands can go from valuable to vulnerable. But by combining their focus and resources, and sharing information, legal and IT security teams can create a positive cycle that enhances investigations, augments attribution efforts, accelerates resolution, and helps to reduce the impact of attacks using brands as weapons.

An Opportunity: Strengthen Brand Resiliency

Seasoned brand protection professionals know the lure of valuable intellectual property and the challenges of securing it in the digital world. Collaborating with IT security teams can reduce the impact of attacks using their brands, streamline mitigation, and increase efficiency.

By working together and using the right technology and tools, these brand defenders will gain greater insight into threats, prioritize responses to the most serious instances — and strengthen brand resiliency.

So, what does this positive cycle look like in practice? Imagine this scenario: A malicious actor uses several branded and unbranded websites to mount an attack. The brand protection group uses their tools and workflows, which are built around intellectual property constructs, to uncover more than 100 brand-abusing sites, social accounts, ad accounts, and e-commerce marketplace listings, as well as other data.

Through this process, the brand protection team also discovers evidence of another cyber threat that's creating risk for the business. They pass that information to the IT security team for further investigation and remediation.

About LexisNexis® Intellectual Property

LexisNexis Intellectual Property brings clarity to innovation for businesses worldwide. We enable innovators to accomplish more by helping them make informed decisions, be more productive, comply with regulations and ultimately achieve a competitive advantage for their business. Our suite of workflow and analytics solutions (LexisNexis® IP Data Direct, LexisNexis PatentAdvisor®, LexisNexis PatentOptimizer®, LexisNexis® PatentSight® and LexisNexis TotalPatent One®) enables companies to be more efficient and effective at bringing meaningful innovations to our world. We are proud to directly support and serve these innovators in their endeavors to better humankind.

www.LexisNexisIP.com/BrandProtection

1. "Mobile App Usage, Statistics & Facts," Statista, August 1, 2019: https://www.statista.com/topics/1002/mobile-app-usage/.
2. "Number of Digital Buyers Worldwide From 2014 to 2021," Statista, July 3, 2019: https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/.
3. Digital 2020: Global Digital Overview, We Are Social and HootSuite report, by Simon Kemp, January 30, 2020: https://datareportal.com/reports/digital-2020-global-digital-overview.
4. Social: GlobalWebIndex's flagship report on the latest trends in social media, 2020, available for download at: https://www.globalwebindex.com/reports/social.
5. The Economic Impacts of Counterfeiting and Privacy, report prepared for BASCAP and INTA, Frontier Economics LLC, 2016: https://iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf.
6. "About three-in-ten U.S. adults say they are 'almost constantly' online," by Andrew Perrin and Madhu Kumar, Pew Research Center Fact Tank, July 25, 2019:
7. "U.S. E-commerce 2019: Mobile and Social Commerce Fuel Ongoing Ecommerce Channel Shift," by Andrew Lipsman, June 27, 2019: https://www.emarketer.com/content/us-ecommerce-2019.
8. New Risks and Emerging Technologies: 2019 BBB Scam Tracker Risk Report, 2020, available for download at: https://www.bbb.org/globalassets/local-bbbs/council-113/media/bbb-institute/riskreport2019/2019-scamtracker-riskreport-digital.pdf.
9. "Counterfeit and pirated goods represent 3.3% of global trade: report," Agence France-Presse (AFP), France24.com, March 18, 2019: https://www.france24.com/en/20190318-counterfeit-pirated-goods-represent-33-global-trade-report.