Th

venza®
Better Visibility. Better Defense.

Case Study

Look-alike Domains

Contents

Executive Summary 3

Look-alike Domains 3

Threat Vector 3

Consequences 3

Defense Limitations 4

Case Study 4

Challenge 4

Solution 4

Results 5

Key Takeaways 5

Response 5

Tools 6

Legal 6

Considerations 6

Prevention 7

How VENZA Can Help 7

Executive Summary

From ransomware to hacking, hoteliers face relentless cyber threats daily that challenge the resilience of their security infrastructure.

Yet, a possibly greater threat looms—one that bypasses even the strongest security measures and targets a hotel's most valuable assets: its brand and reputation.

Look-alike Domains

Look-alike domains are fraudulent websites designed to mimic legitimate ones, deceiving users into believing they are interacting with a business.

These sites exploit a brand's trusted reputation to steal money, harvest credentials, access sensitive accounts, collect personal information, or spread malicious content.

They are often used in broad phishing attacks targeting consumers via email, advertising, and social media.

Threat Vector

Every day, thousands of new domains are registered to mimic legitimate services, with businesses facing an average of 40 attacks each month. While often targeting major companies like Google and Microsoft, look-alike domains threaten organisations of all sizes and industries.

These attacks are cost-effective and scalable for hackers, due in part to low domain registration fees and readily available dark web toolkits priced as low as $300 USD. Because of this, shutting down a single fraudulent site is often insufficient, as hackers can easily create two more to take its place.

Consequences

This threat causes both quantitative and non-quantitative damage. Quantitative losses are measurable, such as the revenue lost from potential customers. Non-quantitative damages, however, include the potentially irreparable harm to a brand's value and trustworthiness.

Defrauded victims often blame the legitimate business, sharing frustrations publicly and deterring potential customers. The resulting regulatory scrutiny and reputational harm weaken the brand's market position, making customer attraction and retention difficult.

Defense Limitations

Despite improved detection methods, businesses often struggle to combat the volume and sophistication of look-alike domains.

Because these domains closely resemble those of their victims with only subtle variations, they are frequently hard to detect and, once found, difficult to remove due to legal and jurisdictional hurdles.

Additionally, hackers often exploit vulnerabilities in the Domain Name System (DNS), a critical layer of internet security to make their sites appear more legitimate. Compromising the DNS layer can grant attackers access to entire networks.

Case Study

In 2023, a prestigious global hotel brand in the Mexican Caribbean fell victim to a sophisticated cyberattack targeting its online ecosystem with look-alike domains. By January 2024, they sought VENZA's hospitality expertise for assistance.

Challenge

Fraudsters created 65 highly convincing counterfeit URLs mimicking the hotel brand's legitimate website to steal from unsuspecting guests by convincing them to book and pay for false reservations.

To bolster the legitimacy of these sites, criminals funneled traffic to them using over 500+ fraudulent social media accounts across multiple platforms.

The company suffered direct financial losses exceeding $30,000 USD, as well as incalculable damage to the brand's globally trusted reputation.

Instead of beginning their dream vacation, defrauded guests arrived at the resort's front desk only to discover they had been deceived, losing both their money and personal information to cybercriminals.

The situation was a ticking time bomb with far-reaching consequences.

Solution

Recognizing that limited action could embolden cybercriminals, VENZA took decisive measures to address current and future threats.

In collaboration with legal counsel, takedown demands were issued for each of the fraudulent websites and social media accounts. Legal notices were also filed with regulatory and enforcement agencies, including the Anti-Phishing Working Group, the U.S. Federal Trade Commission (FTC), and the U.S. Federal Bureau of Investigation (FBI).

Results

The assault was successfully neutralized, with all fraudulent domains and social media accounts removed.

To mitigate future legal risks, VENZA conducted thorough due diligence and reported the activity to enforcement agencies. This not only classified the activity as criminal but also underscored the company's commitment to consumer protection in the event of an investigation.

To safeguard against future threats, VENZA provided the brand with customized legal templates for takedowns and reporting, along with training on their use. This proactive strategy ensured the brand was prepared to respond decisively if a similar issue arose.

Key Takeaways

Given the multifaceted and coordinated nature of the attack, the hotel brand did not have the luxury of a partial response.

A comprehensive countermeasure was necessary—not only to address the threat's scope but also to deliver a clear message to the criminals: every attack would be met with decisive force, deterring future attempts and pushing their ventures elsewhere.

Hoteliers seeking to mitigate a large-scale attack—or currently facing one—should consider several key factors.

Response

Two effective strategies exist for addressing and taking down look-alike domains.

1. **Tools**: Software to identify malicious domains and issue automated takedowns quickly.
2. **Legal**: Counsel to issue formal notices and filings, providing an official and structured method to mitigate this threat.

Both approaches have advantages and limitations; their effectiveness is chiefly dependent on the scale and scope of the attack.

Tools

Many security software tools and systems can automate the process of detecting, analyzing, alerting, and taking down look-alike domains.

The advantage of these solutions is clear: they quickly detect malicious domains and issue automated takedowns, sometimes in less than a day.

However, automated takedowns often fail to address the root cause—the hackers themselves. This approach does not prevent future attacks and may even embolden the attackers to become more aggressive in their efforts.

Legal

Legal takedowns offer a formal and recognized approach to removing malicious content, providing legitimacy and setting a precedent that has been shown to deter further attacks.

Legal filings also provide an added layer of due diligence, creating official records that demonstrate proactive action towards mitigation. This is particularly critical for large-scale incidents that may draw the attention of regulatory bodies, such as the FTC, if consumer complaints escalate.

By maintaining formal documentation, a company can clearly establish that the issue stemmed from a targeted attack on the brand, not an internal breach or system compromise.

However, this method is often time-consuming. It also requires thorough validation and evidence, making it resource-intensive and potentially slower to implement. Depending on the scale of the threat, it can also become expensive.

Considerations

When deciding on the most effective approach, the scale and nature of the attack must be carefully considered.

Take, for example, the renowned hotel brand that sought VENZA's expertise. Detection was not their issue—their internal teams had already identified the fraudulent sites and accounts. However, they found themselves trapped in a game of "whack-a-mole,"

repeatedly addressing individual threats without a lasting solution. For them, a comprehensive and resolute legal response was essential to put an end to the cycle.

On the other hand, tools and software can serve as effective measures to detect and mitigate such issues early, preventing them from escalating. These solutions act as a means of control and containment, while legal action serves as the decisive step to eliminate a specific attacker.

Prevention

Hoteliers can take steps to reduce the risk of look-alike domains and prevent their spread.

1. **Use automated detection and takedown solutions.**
    - These solutions can quickly identify and remove malicious domains before the situation escalates.
2. **Register domain variations.**
    - Preemptively register common typos, misspellings, and multiple top-level domains (e.g., .com, .net) to block attackers from exploiting them.
3. **Optimize SEO.**
    - Enhance the website's visibility on search engines, increasing the likelihood that guests will find the official site.
4. **Be active on social media.**
    - Regularly update official accounts across social media platforms, making legitimate content easier to identify.
5. **Encourage direct bookings.**
    - Promote direct reservations and advise guests to bookmark official websites.

How VENZA Can Help

As hospitality's trusted leader in cybersecurity and data protection, VENZA delivers cutting-edge solutions to combat and prevent look-alike domain threats.

Ready to protect your brand? Contact the experts at VENZA today. Visit www.venzagroup.com or email bettervisibility@venzagroup.com to get started.

About VENZA

VENZA is a leading provider of security awareness data protection solutions that empower the hospitality industry to mitigate vulnerabilities and ensure compliance. VENZA supports over 2000 hotels globally, keeping guests and their data safe from breaches with 360-degree visibility for proactive management of risks. This allows property managers to focus on guest service and building trust in their brand.

Visit www.VENZAGroup.com for additional details.

Contact Us

Sales: sales@venzagroup.com

Customer Success: success@venzagroup.com