CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

March 7, 2022

2021 Brand Intelligence Trends

Recorded Future®

Insikt Group used the Recorded Future® Platform to look at mainstream news, security vendor reporting, technical reporting around malware, vulnerabilities, security breaches, and dark web and underground forums from January 1, 2021, to December 31, 2021. The trends outlined below illustrate the current threat landscape observed via our Brand Intelligence Module of the Recorded Future® Platform.

Executive Summary

Throughout 2021, organizations faced a variety of cyber threats targeting their brands. While threats affecting brands, such as typosquats, domain abuse, and data exposure, do not garner as much attention as ransomware attacks, it is crucial that organizations actively respond to and mitigate these threats. Threats to brands affect organizations in every sector, both public and private, and can be used as staging grounds by attackers for future cyberattacks.

Data exposure continued to be a persistent threat to organizations across all industries in 2021. Data exposure can be caused by a variety of means, such as misconfigured databases and poor security protecting data held within these repositories. Several organizations felt the repercussions of poor data security in 2021 when millions of their records were exposed and in some instances illegally accessed by threat actors to be sold online to other cybercriminals. Social media services appeared to be particularly affected by data exposure in 2021: multiple platforms, including Facebook, SocialArk, LinkedIn, and Gettr, had large amounts of user data published on dark web and underground forums.

Reputational damage from cyberattacks can be severe. Throughout 2021, ransomware operators have continued using extortion tactics to name and shame their victims, a tactic that gained popularity in 2020. Although it is difficult to assign an exact cost to the reputational damage that results from lost or exposed data, ransomware operators continue to charge high ransoms, from tens of thousands to millions of dollars, and many organizations are willing to pay those ransoms. This willingness to pay suggests that companies believe the alternative of lost reputation or reduced competitive advantage has a cost greater than that of the ransom.

Key Judgments

- We identified more than 1.3 million references to typosquats affecting 10 major organizations in the Fortune 500 in 2021.
- Data exposure continued to be a persistent threat to organizations across all industries in 2021. The average total cost of a data breach in the United States, the country with the highest average cost for 11 years in a row, increased to $9.05 million from $8.64 million, and the average total cost globally was $4.24 million USD in 2021.
- In 2021, we observed over 2 million references appearing on ransomware extortion sites tracked within the Recorded Future Platform, and more than 29 million references using our Dark Web Ransomware Extortion Sites source.

Domain Abuse

Fraudulent domains that mimic the appearance of the genuine domain of an organization are used to target customers and employees and can result in credential theft, reputational damage, and potentially millions of dollars of damages. Throughout 2021, Recorded Future observed typosquats affecting organizations across all private sector industries as well as governments worldwide.

Using the Recorded Future Platform, we analyzed typosquats affecting a sample of 10 major companies from the 2021 Fortune 500 list. These companies represent organizations operating in a variety of business functions. While not indicative of the sum of all typosquats in 2021, the results show how domain abuse affects several large sectors, including technology, retail, healthcare and pharmaceuticals, financial services, and energy. Altogether, we observed more than 1.3 million references to typosquats of these 10 companies. An organization operating in the technology sector had the highest number of references with 562,734, while an organization in the healthcare and pharmaceutical sector saw the least with 4,799 references.

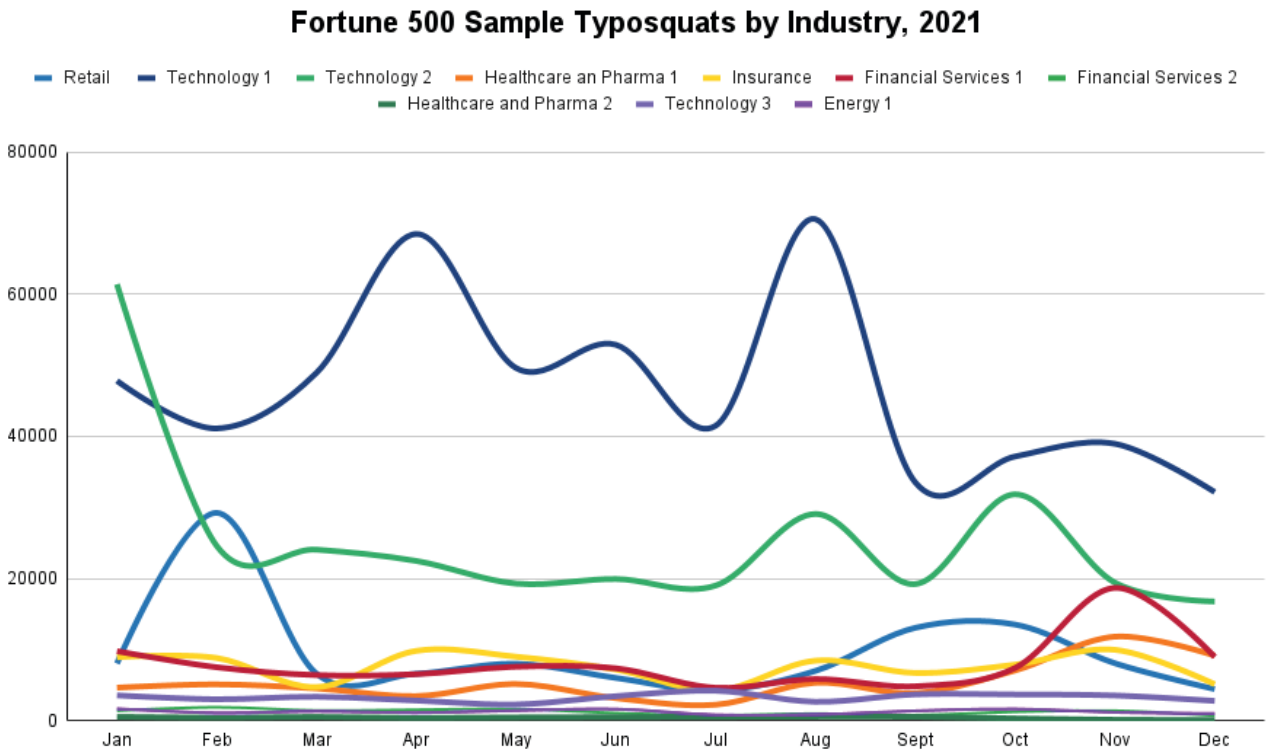

Figure 1: Typosquat references to 10 major Fortune 500 organizations from January 1 to December 31, 2021 (Source: Recorded Future)

We observed over 5,000 references to the typosquat attack vector, peaking in August and September 2021. This activity is reflected in 6 of the Fortune 10 organizations experiencing an uptick in observed typosquats during this period. Consistent typosquat volume targeting the Fortune 10 demonstrates the prevalence of typosquatting across major industry verticals.

To defend against domain abuse, organizations should monitor for new domain registrations and URLs containing strings with similar nomenclature potentially targeting their brand, which can be used in phishing attacks, along with new certificates registered for those domains as certificate registration can be evidence of threat actors setting up phishing infrastructure, with this step meant to lend legitimacy to domains. Brand Intelligence from Recorded Future automatically detects typosquats and other forms of domain abuse in real time.

In addition, we recommend organizations ensure that Domain-based Message Authentication, Reporting, and Conformance (DMARC) is set up to prevent threat actors from spoofing legitimate domains to send phishing emails. Google provides a comprehensive list of recommendations on how to set up DMARC, which includes preparation to setting up DMARC, defining your DMARC policy, adding your DMARC record, and implementing DMARC rollout.

Data Exposure

Data exposure continued to be a persistent and costly threat to organizations across all industries in 2021. IBM/Ponemon Institute's annual "Cost of A Data Breach" report, published in July 2021, identified the global average cost of a data breach to be $4.24 million, an increase from the average of $3.86 million reported in 2020. In addition, the average total cost of a data breach in the United States, the country with the highest average cost for 11 years in a row, increased to $9.05 million from $8.64 million. The average total cost globally is $4.24 million USD.

Organizations affected by significant data exposures in 2021 include the following:

- SocialArks Data Breach: On January 11, 2021, SocialArks, a Chinese social media management company, suffered a data breach that resulted in the exposure of over 400 GB of data, according to a report from SafetyDetectives. This affected the personally identifiable information (PII) of over 200 million social media users worldwide and included accounts from Facebook, Instagram, and LinkedIn.
- Bykea Misconfigured Server: On January 28, 2021, security researchers disclosed a data security incident involving Bykea, a Pakistan-based transportation, logistics, and cash on delivery payments company. The company's complete production server containing 200 GB of data with over 400 million records was exposed without any password or encryption and was discovered by the research team on November 14, 2020. API logs of the company's web and mobile sites and PII were stored in the Elasticsearch server. Information contained in the unsecured database included customers' data such as full names, phone numbers, and email addresses, partners' (drivers') information like full names, phone numbers, addresses, CNICI (Computerized National Identity Card), driver's license information, body temperature, and other details, including internal API logs, collection and delivery location information, user token ID with cookie details and session logs, specific GPS coordinates, vehicle information, user device information, and encrypted IMEI numbers.
- Facebook Data Leak: On April 3, 2021, an unknown threat actor shared a data breach that exposed over 500 million users' data on Raid Forums according to a report from Bleeping Computer. The stolen data included users' full names, phone numbers, locations, email addresses, Facebook IDs, and biographical information. Of this data, Recorded Future indexed all users whose profile information contained an email address, which in total is 119,781,651.
- Cognate Data Leak: On June 14, 2021, news reports emerged about a data security incident involving the cybersecurity analytics firm Cognyte. Security researchers at Comparitech disclosed that a database was left unsecured by Cognyte, exposing over 5 billion records. The database contained a collection of previous data breaches as part of the company's cyber intelligence service. Information contained in the exposed database includes names, passwords, email addresses, and the original source of the leak. Bob Diachenko, who led the research team, stated that they discovered the database on May 29, 2021. Cognyte secured the database 3 days after it was notified about the data leak. Comparitech could not determine if third parties were able to obtain a copy of the database during its exposure or how long it was exposed on the web before search engines indexed the database.
- Data of Millions of T-Mobile Customers Advertised on Dark Web: On August 16, 2021, telecommunications giant T-Mobile USA confirmed that hackers breached some of their internal servers after millions of records of customer data were put up for sale on a dark web forum. The company did not go into details and stated they were in the process of analyzing what data was "illegally accessed" and if "any personal customer data" was stolen. This came after the personal information of millions of T-Mobile customers was already advertised on the dark web on August 14, 2021. The advertisement referenced information for 30 million T-Mobile customers, and the seller claimed the data was part of a larger package containing details for 100 million T-Mobile customers. According to the seller, they were able to obtain the information from multiple T-Mobile servers because the company left a Gateway GPRS Support Node (GGSN) exposed to the internet. The information, which appears to be authentic after security researchers analyzed the sample data, includes Social Security numbers, names, addresses, unique IMEI numbers, and the driver's license numbers of more than 100 million customers. Based on the August 14 2021 post, the seller advertised that interested buyers could get a subset of 30 million Social Security numbers and driver's licenses for 6 bitcoins (at the time, about $277,895). The rest of the data was sold privately by the seller. The seller later stated that they lost access to the servers, suggesting that T-Mobile discovered the data breach and secured the servers.

As the examples above show, the information found in these breaches often consists of customer or employee data including PII. Attackers can use this information to conduct phishing and spearphishing attacks and brute-force password cracking attacks. Recorded Future has developed a system to detect and alert organizations when their credentials appear in breaches such as the examples outlined above and to automatically detect phishing attempts made using credentials in the Recorded Future platform.

Reputational Damage to Brands

Reputational damage from cyberattacks can be severe. Throughout 2021, ransomware operators have continued using extortion tactics to name and shame their victims, a tactic that gained popularity in 2020. Organizations worldwide remain at a heightened risk of reputational damage, along with the financial costs of remediation, as threat actors continue using ransomware attacks to exfiltrate and publicly post victims' data on extortion websites. Brands that suffer from reputational damage can lose market share or competitive advantage. Stolen data could include partnership agreements and contracts, sales strategies, corporate financial statements, and so on. It is difficult to assign a broad market value to this data as it varies from organization to organization, but given ransomware operators' continued use of extortion techniques in the last 2 years, it is very likely that this value is high enough to have prompted many organizations to pay a ransom rather than expose data. And based on the large ransoms that operators have demanded (and received) in the recent past, it is also very likely that companies have interpreted this type of data exposure as costing them reputation or competitive advantage at a value of millions of dollars.

Ransomware continues to dominate the threat landscape and mainstream media reporting. In 2021, multiple ransomware attacks were observed targeting high-profile Fortune 500 companies such as Colonial Pipeline, which was targeted by Darkside ransomware, Accenture, which was targeted by the Lockbit2.0 ransomware, and Kaseya, which was targeted by the Ragnarok ransomware.

Insikt Group recommends that all organizations maintain offline backups and implement proactive security measures such as the patching of disclosed vulnerabilities as quickly as possible, multi-factor authentication (MFA), and network segmentation to reduce the risk of ransomware infection. It also remains vital to educate users on new and emerging TTPs used by threat actors, especially phishing lures, as they are often the initial entry point for ransomware operators.

Ransomware Extortion Sites

In 2021, we observed over 2 million references appearing on ransomware extortion sites tracked within the Recorded Future platform. Recorded Future currently tracks 46 ransomware extortion sites. We also observed more than 29 million references using our Dark Web Ransomware Extortion Sites source. This is a stark increase from 2020, when Recorded Future observed 734,000 references in our Dark Web Ransomware Extortion Sites source.

Cost of a Ransomware Attack

According to Forbes, the average cost globally of a ransomware attack for an organization has more than doubled since 2019. In 2019, the average cost of a ransomware attack was $761,000 USD. The cost increased to $1.85 million USD in 2020. Of note, the average cost to remediate a ransomware attack for a US-based organization was $2.09 million USD. The increase in cost can likely be tied to ransomware operators employing more advanced tactics, techniques, and procedures (TTPs) in their attacks. These more advanced TTPs make it more difficult for organizations to remediate and recover affected infrastructure.

Case Study: Incidents and Brand in 2021

We looked at Facebook Inc., now Meta Platforms Inc, for this case study regarding brand for several reasons. First, Meta had heterogeneous incidents. We believe this will allow other organizations to analyze varied situational outcomes. Second, there were multiple data points for each incident. Third, with an understanding that an organization's brand can be affected by events in positive, neutral or negative ways, we believe it would be useful to identify which association went with each incident. Overall, each event detailed in this case study has data connected to organizational growth or loss and, when applicable, included if the event was positive, neutral, or negative. Several prominent events from 2021 affected Meta: data breaches, a multi-hour outage, a US Congressional testimony, rebranding, and an anti-phishing lawsuit.

During 2021, the monthly active users for Facebook grew, but also slowed quarter by quarter, dropping from 2% in Q1 to 0.5% in Q4, its lowest growth rate between 2018 and 2021. Negative associations with a brand can lead to slowed growth according to research published by IEEE; data from the Recorded Future Platform showed an increase in negative sentiment toward Facebook in Q4.

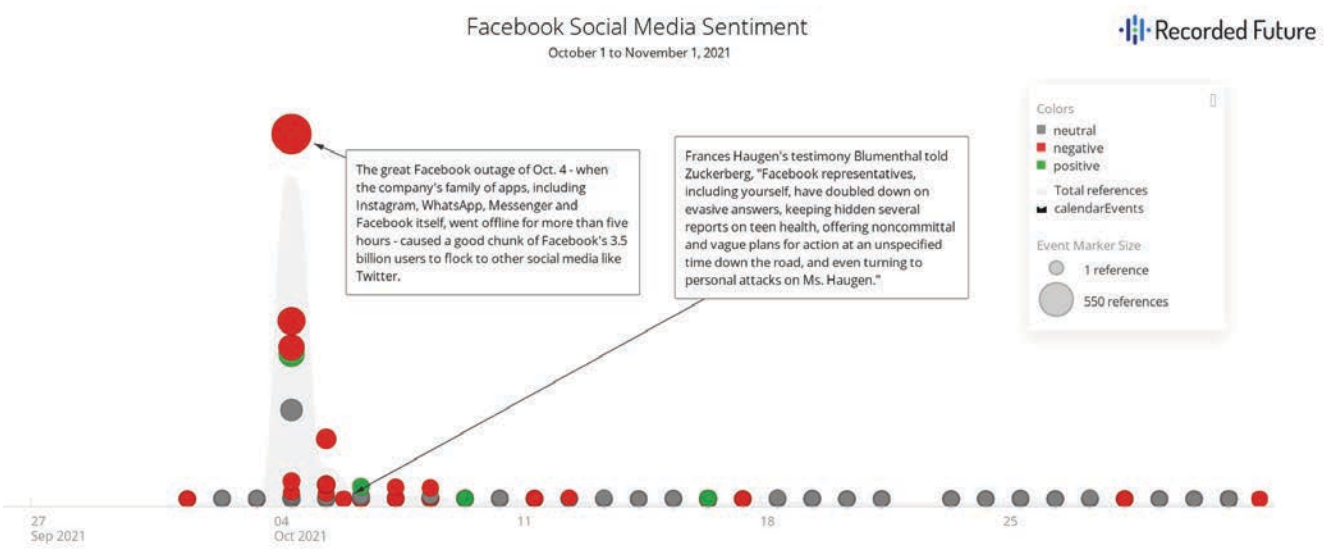

Figure 2: Sentiment and Facebook from October 1 to October 31, 2021 (Source: Recorded Future)

On October 4, 2021, users reported that they could not connect to Facebook and platforms associated with the company for approximately 7 hours. During the outage, Facebook, Inc shares fell by around 5%.

In 2018, Glassdoor listed Facebook, Inc as number 1 for best places to work, but by 2021 it decreased to 11 and at the time of this writing was at 47. Reporting from CNBC identified that it may be more difficult for organizations to attract top talent due to their employer brand.

On October 5, 2021, a Facebook former employee, Frances Haugen, testified in front of US Congress and shared [1, 2] internal studies completed by Facebook, Inc about society and social media as well as social media and perceptions for teens and pre-teens. According to internal company studies, 13.5% of teen girls said that Instagram made their thoughts about suicide worse, and 17% of teen girls stated it made their eating disorders worse.

On October 28, 2021, the parent company Facebook, Inc announced that they were rebranding their parent company to Meta Platforms, Inc. or Meta. AppleInsider identified that the rebrand could cost up to $20 million USD.

On December 20, 2021, Meta filed an anti-phishing lawsuit to place an injunction on 39,000 domains and their operators, targeting phishing schemes that impersonated Facebook, Facebook Messenger, Instagram, and WhatsApp (all products owned by Meta). In an email to The Record, Crane Hassold, the director of threat intelligence at Abnormal Security, stated, “Based on the content of the lawsuit, however, I don’t see anything that would trigger a noticeable impact to the actual frequency of phishing attacks abusing Facebook’s brands.”

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.