The Global Year in Breach

2021:

What Happened in 2020, Why It Happened and What To Do Next

The Global Year in Breach 2021: What Happened in 2020, Why It Happened and What To Do Next

Fundamental changes in the way we lived and worked made 2020 a wild year for cybersecurity professionals. The resilience of every company was tested in the midst of a pandemic-induced, volatile economy as threats snowballed in the wake of a rapid shift to remote workforce support.

Adding to, and perhaps fueled by, those challenges, a cybercrime boom that included record-breaking phishing and ransomware threats ratcheted up the stress on IT professionals. Sectors unaccustomed to being targeted by cybercriminals suddenly found themselves under siege while unprepared companies quickly learned the cost of failing to take cybersecurity seriously.

Although 2020 was a tumultuous year, it was a year with an important tale to tell. For our Global Year in Breach 2021 report, ID Agent gathered and analyzed data from our industry-leading cybersecurity solutions, Dark Web ID and BullPhish ID, and combined it with illuminating industry statistics to give you a clear picture of how the data breach landscape evolved in 2020.

Examining the 2020 cybersecurity story through this lens provides insights into how global events can rapidly transform the cybersecurity landscape. This has enabled us to forecast continuing and emerging cybersecurity trends for 2021 and also provide helpful advice about smart risk mitigations that fit every business and every budget.

5 Key Trends That Transformed 2020 and Their Impact on 2021

Despite the chaos the COVID-19 pandemic caused across the world, ID Agent kept a keen eye on emerging cyber risk trends, how they are poised to impact businesses in 2021 and what you can do to deter them.

1. Phishing Boomed Exponentially, Creating Unprecedented Risk for Everyone

What happened: A lethal combination of unsettled workers hungry for information about a terrifying global pandemic, unprecedented lockdowns forcing a rapid shift to virtualization and a higher reliance on email as the primary form of communication created a golden opportunity for cybercriminals. Phishing attacks increased more than 660 percent, culminating in COVID-19 becoming Google's biggest phishing topic in history.

What's next: Phishing remains the No. 1 cybersecurity threat for businesses. Although 2020 was a record breaker, by the end of January Google recorded a 27 percent increase in phishing sites in 2021. Improvements in security awareness training that include phishing simulation are vital for businesses to mitigate this risk. Increasing your staff's phishing resistance can slash your company's chances of experiencing a damaging cyberattack up to 70 percent.

2. Third-Party and Supply Chain Risk Hit the Breaking Point, Leading to Disaster

What happened: The wealth of information already extant on the dark web from prior years' data breaches combined with even more information from big data breaches early in 2020 worked in bad actors' favor. It provided abundant fuel for cyberattacks that impacted businesses — over 90 percent of U.S. businesses experienced a cybersecurity incident like a data breach in 2020 because of a third-party or supply chain fault. Worldwide, over 60 percent of data breaches were the result of exposure through a third party.

What's next: Third-party and supply chain risk stole the show for parts of 2020, with two especially egregious breaches that spoke to the intertwined nature of today's businesses and today's risk. With supply chain cyberattacks expected to cause $6 trillion worth of damage in 2021, companies must take precautions against the impact of third-party data breaches by adding fail-safes measures, like secure identity and access management with multifactor authentication, to prevent unauthorized intrusions.

90% SC Fail in U.S.
60% worldwide

3. Pandemic-Triggered Remote Workforce Shift Exposed Cybersecurity Weaknesses

What happened: A sudden shift to remote work, an exceptionally stressed workforce and a tsunami of cybercrime created major challenges for businesses. Companies were forced to switch to all-remote operations without notice, exposing unprepared workers and insecure systems to risk with disastrous consequences. One study showed that remote workers caused half of all data breaches and exposed businesses to 78 percent more insider threats, while over 60 percent of remote workers interacted with phishing emails.

What's next: Remote work is here to stay. The percentage of workers whose jobs are permanently remote is expected to double in 2021. Companies have discovered the benefits of having flexible operations and a workforce that can get the job done anytime, anywhere. To address the added risk of supporting a remote workforce and to be prepared for future emergencies, organizations must focus on developing cyber resilience that ensures they are ready for anything.

4. Ransomware Lurked Around Every Corner

What happened: A massive increase in phishing brought about a correspondingly massive increase in ransomware, with an eye-popping 715 percent increase in ransomware attacks. Ransomware costs are expected to reach $20 billion in 2021, and it is estimated that a ransomware attack takes place every 11 seconds.

What's next: Organizations must make defending against ransomware one of their top IT priorities. Since the primary delivery system for ransomware is phishing, increasing the frequency and variety of phishing awareness training is vital. Studies show that a minimum of one campaign every four to six months is required for retention.

5. Dark Web Danger Increased as Cybercrime Surged

What happened: A perfect storm of factors led to a perfect window of opportunity for cybercriminals, and they pounced on it. Dark web activity increased by 44 percent, with a corresponding 80 percent jump in overall cybercrime. Two in five SMBs were hit by bad actors.

What's next: Cybercrime risks will continue, and damage is expected to reach $6 trillion in 2021. Over 60 percent of the information that was already on the dark web by January 2020 could be used to damage businesses. Even more data made its way to the dark web in 2020 with an estimated 22 million new records added to the mix. This data will be used to facilitate new cyberattacks including hacking, phishing, business email compromise and credential stuffing. Companies must keep an eye on dark web danger to mitigate risks and spare themselves from unpleasant surprises.

Cybercrime risks will continue, and damage is expected to reach

reach $6 trillion in 2021.

The Week in Breach: Weekly Breach Records

Every Wednesday in "The Week in Breach," we list Dark Web ID's Top Threats of the Week. While there was a clear winner for the industry hit hardest by cyberattacks in 2020, everyone got a piece of the pie, reiterating the fact that no business is safe from cybercrime.

Dark Web ID's Top Weekly At-Risk Industries of 2020

Top Compromise Type: Domain
Top Source of Hits: ID Theft Forums

Weeks at the Top of the Chart

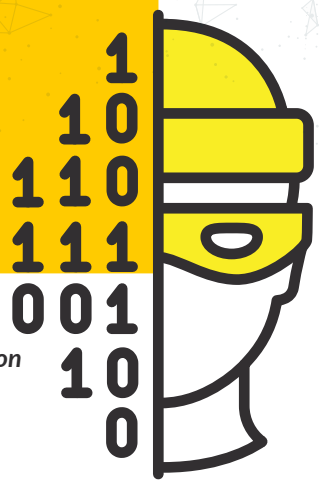
Education and Research	**24**
Media & Entertainment	**7**
Finance & Insurance	**6**
High Tech & IT	5
Medical & Healthcare	3
Manufacturing	2
Hospitality	2
Aerospace & Defense	1
Service Provider	1
Sales & Retail	1

Phishing Was the King of Risks in 2020 and Will Continue to Rule in 2021

Phishing was the lead actor in nearly every cybercrime disaster of 2020, demonstrating the necessity for dynamic, user friendly security awareness training that includes phishing resistance. Companies in every sector rely on BullPhish ID as their phishing resistance training solution, giving us unbeatable insight into the types of phishing messages that employees found most tempting in 2020.

What Phishing Lures Are Employees Most Likely to Fall For?

The data on this one is very clear – **employees are most likely to interact with and provide information in response to seemingly routine permissions messages.** Faux messaging that combined COVID-19 with administrative messaging ran a distant second but still captured a substantial amount of credentials.



Top ID Agent Phishing Simulation Campaigns That Successfully Drew Employee Interaction

Fraud Warning: Suspicious Login Detected – 11,027 clicked

An Unusual Google Chrome Sign-In Detected – 7,557 clicked

Email Quarantine Request for Suspicious Activity – 5,978 clicked

Top ID Agent Phishing Simulation Campaigns That Captured Credentials and Data

Fraud Warning: Suspicious Login Detected – 1,827 captures

An Unusual Google Chrome Sign-In Detected – 1,594 captures

COVID-19 Mandatory Seminar – 846 captures

What Training Courses Are Organizations Using the Most?

Industry observers raised the alarm as the COVID-19 pandemic spawned a suddenly remote workforce, warning of precipitate increases in phishing threats – and cybersecurity professionals listened, choosing phishing resistance courses as their top priority in 2020.

3

Top 3 Security Awareness Training Courses of 2020

How to Avoid Phishing Scams – **6,410**

Phishing: Introduction to Phishing – **4,413**

Good Password Practices – **4,107**

Cybercriminals Broke New Ground on the Dark Web and so Did Dark Web ID

An enormous increase in cybercrime, combined with a plethora of new information hitting dark web data markets and dumps, meant expansion for everyone on the dark web in 2020. And where bad actors go to do their business, so too does Dark Web ID to guard against credential compromise.

What are we monitoring?

Our unique blend of human and machine intelligence analyzes the dark web 24/7/365 to alert clients if their protected credentials pop up in a dark web market or data dump, including the 20,773 domains, 17,259 personal email addresses and 8,832 IP addresses that we added to our watch lists in 2020.

Who are we protecting?

A growing number of organizations that enjoy peace of mind from dark web threats include nearly 4,000 partners (that are now protecting more than 40,000 small businesses) and more than 150 mid-market enterprises.

How many compromised credentials did we uncover?

Way too many. And the possibilities for compromise that all businesses face grow every day. In 2020, we pulled 10,924,662 compromises for the domains we monitor, and 24,254 compromises for monitored email accounts.

Increased Cybercrime Is the Forecast for 2021 and Beyond

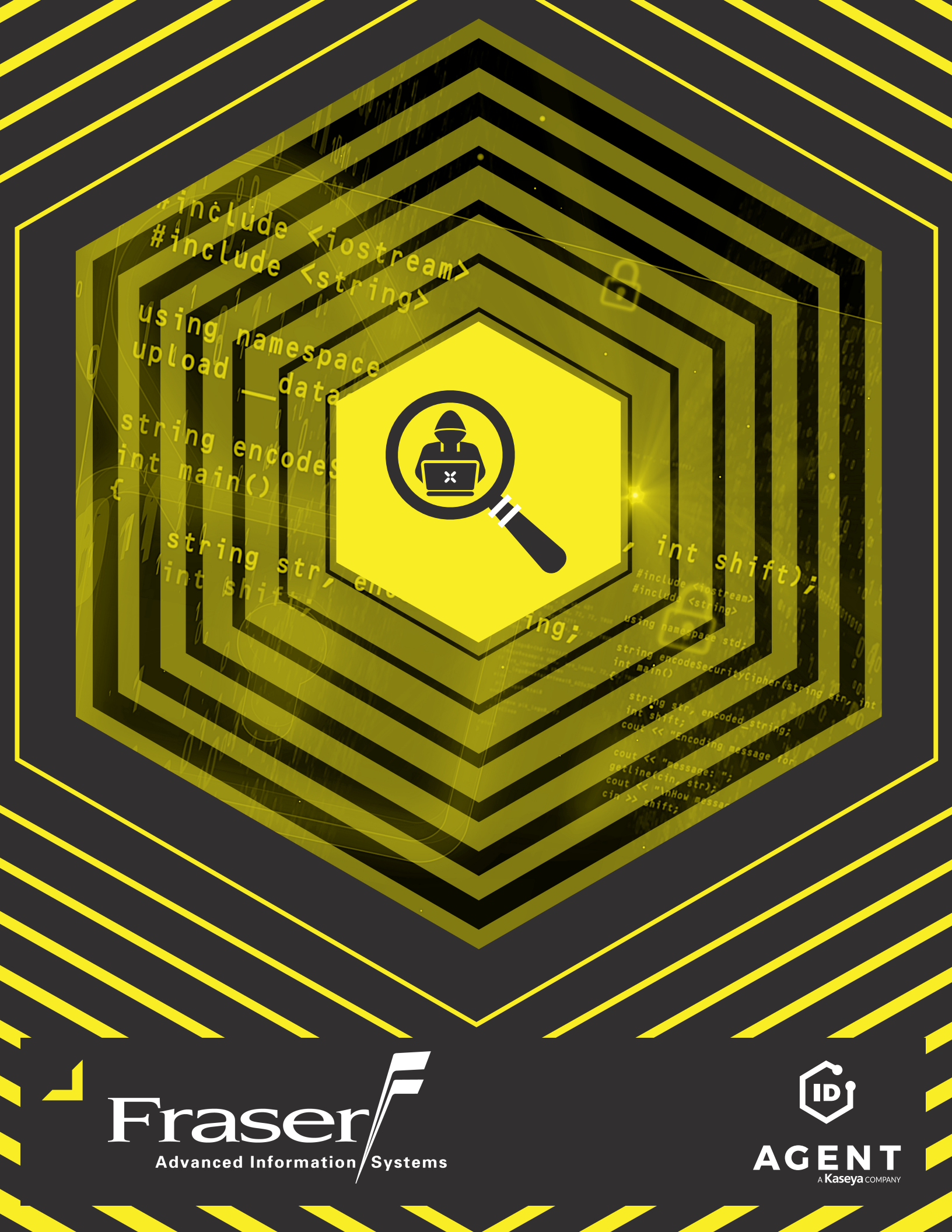
Cybercrime isn't going anywhere but up. Businesses face greater risks than ever before from an abundance of dark web data-related cyberattacks, a constant onslaught of phishing and the continuing tumult from the global pandemic. In a challenging economy, even cybercriminals have to work a little bit harder. Unfortunately, they seem to be rising to the challenge.

Is your defense ready?

Get Your Business Protected From Ransomware and Phishing

Fraser Advanced Information Systems

Fraser Advanced Information Systems | Tel: 610.378.0101 | Visit us online at www.fraser-ais.com


#include <iostream>
#include <string>
using namespace
upload
string encodes
int main()
string str,
int shift);
Fraser
Advanced Information Systems
ID
AGENT
A Kaseya COMPANY