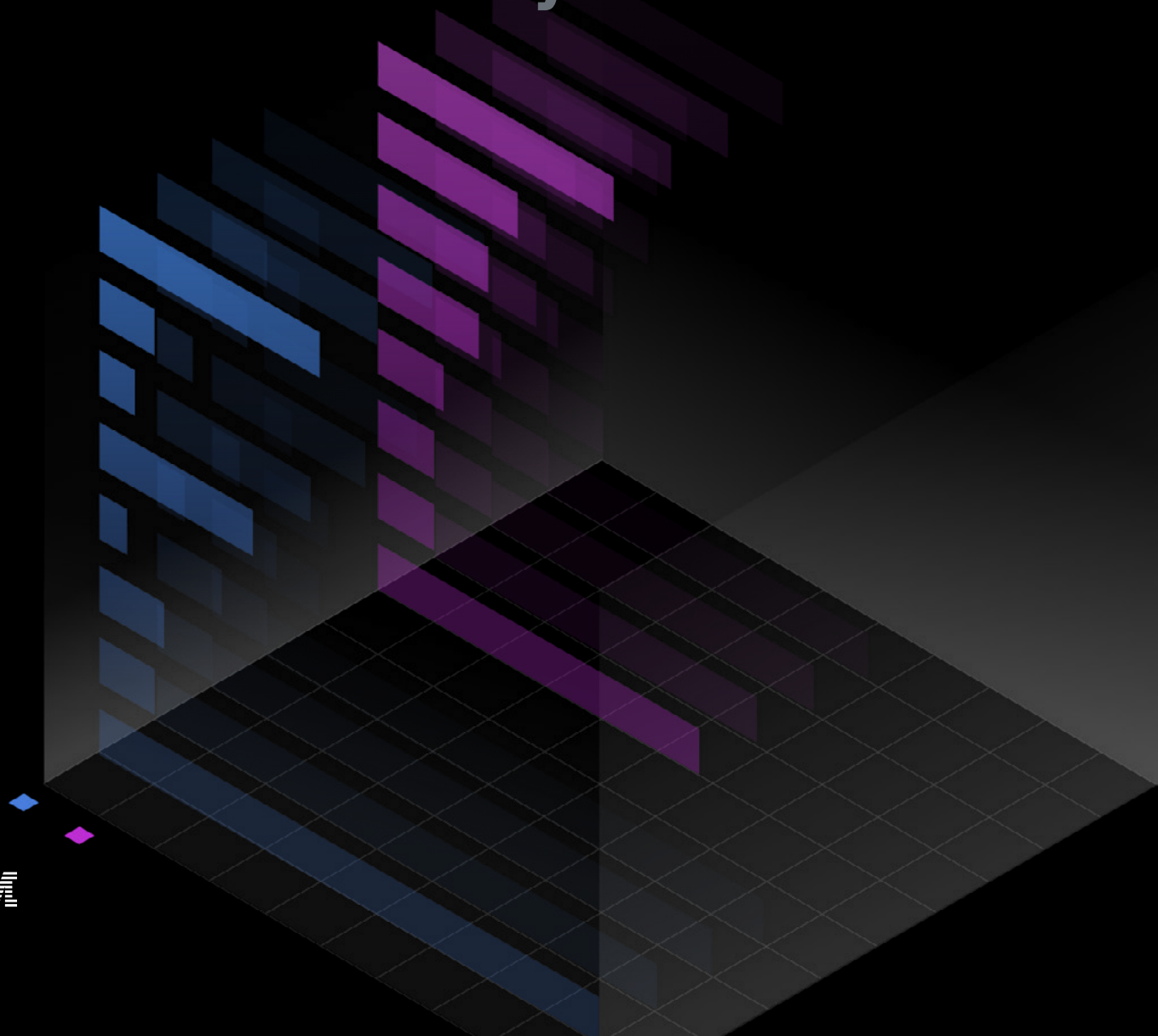
IBM Security

# X-Force Threat Intelligence Index 2021

## Executive Summary



IBM

# Introduction

The year 2020 was without a doubt one of the most consequential and transformational in recent memory: A global pandemic, economic turmoil impacting millions of people's lives, and social and political unrest. The reverberations from these events affected businesses in profound ways, with many making a major shift to distributed workforces.

In the cyber realm, the extraordinary circumstances in 2020 handed cyber adversaries opportunities to exploit the necessities of communication networks and provided rich targets in supply chains and critical infrastructure. The year ended as it began, with the discovery of a globally consequential threat that required rapid response and remediation. An attack that has largely been attributed to a nation state actor, which leveraged a backdoor in network monitoring software to attack government and private sector organizations, demonstrated how third-party risk should be anticipated, but can't be predicted.

To help meet the challenges of these times, IBM Security X-Force assesses the cyber threat landscape and assists organizations in understanding the evolving threats, their associated risk, and how to prioritize cybersecurity efforts. In addition to the premium threat intelligence we provide to customers, we analyze the wealth of data we gather to produce the X-Force Threat Intelligence Index, an annual check-in on the threat landscape and how it's changing.

Among the trends that we tracked, ransomware continued its surge to become the number one threat type, representing 23% of security events X-Force responded to in 2020. Ransomware attackers increased the pressure to extort payment by combining data encryption with threats to leak the data on public sites. The success of these schemes helped just one ransomware gang reap profits of over $123 million in 2020[1], according to X-Force estimates.

Manufacturing organizations weathered an onslaught of ransomware and other attacks in 2020. The manufacturing industry overall was the second-most targeted, after finance and insurance, having been the eighth-most targeted industry in 2019. X-Force discovered sophisticated attackers using targeted spear phishing campaigns in attacks against manufacturing businesses and NGOs involved in the COVID-19 vaccine supply chain.

1. All currency in this report is in United States dollars.

Threat actors were also innovating their malware, particularly malware that targeted Linux, the open source code that supports business-critical cloud infrastructure and data storage. Analysis by Intezer discovered 56 new families of Linux malware in 2020, far more than the level of innovation found in other threat types.

There is reason to hope that 2021 will shape up to be a better year. Trends are notoriously hard to predict, but the one constant thing we can rely on is change. Resilience in the face of rising and falling challenges in cybersecurity requires actionable intelligence and a strategic vision for the future of a more open, connected security.

In the spirit of strength through community, IBM Security is pleased to offer the 2021 X-Force Threat Intelligence Index. The findings in this report can help security teams, risk professionals, decision-makers, researchers, the media and others, understand where threats have been in the past year and help prepare for whatever comes next.

# Executive summary

IBM Security X-Force drew on billions of data points collected from our customers and public sources between January and December 2020 to analyze attack types, infection vectors, and global and industry comparisons. The following are some of the top findings presented in the X-Force Threat Intelligence Index.

## 23%

**Ransomware share of attacks**

Ransomware was the most popular attack method in 2020, making up 23% of all incidents IBM Security X-Force responded to and helped remediate.

## $123 million+

**Estimated profits from top ransomware**

X-Force conservatively estimates that Sodinokibi (also known as REvil) ransomware actors alone made at least $123 million in profits in 2020 and stole around 21.6 terabytes of data.

## 25%

**Top vulnerability share of attacks in Q1 2020**

Threat actors capitalized on a path traversal Citrix flaw, exploiting this vulnerability in 25% of all attacks in the first three months of the year and 8% of total attacks in all of 2020.

## 35%

**Scan-and-exploit share of top infection vectors**

Scanning and exploiting vulnerabilities jumped up to the top infection vector in 2020, surpassing phishing which was the top vector in 2019.

## #2

**Manufacturing rank in top attacked industries**

Manufacturing was the second-most attacked industry in 2020, up from eighth place in 2019, and second only to financial services.

# 5 hours

**Length of attack-training videos on a threat group server**

Operational errors by Iranian nation-state attackers allowed X-Force researchers to discover around 5 hours of video on a misconfigured server, yielding insight into their techniques.

# 100+

**Executives targeted in precision phishing campaign**

In mid-2020, X-Force uncovered a global phishing campaign that reached more than 100 high ranking executives in management and procurement roles for a task force acquiring personal protective equipment (PPE) in the battle against COVID-19.

# 49%

**ICS-related vulnerability growth rate, 2019-2020**

Industrial control systems (ICS)-related vulnerabilities discovered in 2020 were 49% higher year-over-year from 2019.

# 56

**Number of new Linux malware families**

The number of new Linux-related malware families discovered in 2020 was 56, its highest level ever. This represented a 40% year-over-year increase from 2019-2020.

# 31%

**European share of attacks**

Europe was the most-attacked geography in 2020, experiencing 31% of attacks observed by X-Force, followed by North America (27%) and Asia (25%).

# Looking ahead

In 2021, a mix of old and new threats will require security teams to consider a lot of risks simultaneously. Based on X-Force analysis, these are some of the key takeaways for priorities in the next year.

— **The risk surface will continue to grow in 2021.** With thousands of new vulnerabilities likely to be reported in both old and new applications and devices.

— **Double extortion for ransomware will likely persist through 2021.** Attackers publicly leaking data on name and shame sites increases threat actors' leverage to command high prices for ransomware infections.

— **Threat actors continue to shift their sights to different attack vectors.** Targeting of Linux systems, operational technology (OT), IoT devices, and cloud environments will continue. As targeting of these systems and devices becomes more advanced, threat actors may rapidly shift efforts, especially following any high-profile incident.

— **Every industry has its share of risks.** The year-over-year shift in industry-specific targeting highlights the risk to all industry sectors and a need for meaningful advancements and maturity in cybersecurity programs across the board.

# Recommendations for resilience

Based on IBM Security X-Force findings in this report, keeping up with threat intelligence and building strong response capabilities are impactful ways to help mitigate threats in the evolving landscape, regardless of which industry or country one operates in.

X-Force recommends the following steps that organizations can take to better prepare for cyber threats in 2021:

**Get in front of the threat rather than react to it.** Leverage threat intelligence to better understand threat actor motivations and tactics to prioritize security resources.

**Preparation is key for a response to ransomware.** Planning for a ransomware attack—including a plan that addresses blended ransomware and data theft extortion techniques—and regularly drilling this plan can make all the difference in how your organization responds in the critical moment.

**Double check your organization's patch management structure.** With scanning and exploiting being the most common infection vector last year, harden your infrastructure and reinvigorate internal detections to find and stop automated exploitation attempts quickly and effectively.

**Protect against insider threats.** Use data loss prevention (DLP) solutions, training, and monitoring to prevent inadvertent or malicious insiders from breaching your organization.

**Build and train an incident response team within your organization.** If that's not a possibility, engage an effective incident response capability for prompt response to high-impact incidents.

**Stress test your organization's incident response plan to develop muscle memory.** Tabletop exercises or cyber range experiences can provide your team with critical experience to improve reaction time, reduce downtime, and ultimately save money in the case of a breach.

**Implement multifactor authentication (MFA).** Adding layers of protection to accounts continues to be one of the most efficient security priorities for organizations.

**Have backups, test backups, and store backups offline.** Not only ensuring the presence of backups but also their effectiveness through real-world testing makes a critical difference in the organization's security, especially with 2020 data showing a resurgence in ransomware activity.

# About IBM Security X-Force

## IBM Security X-Force delivers insights, detection, and response capabilities to help clients improve their security posture.

IBM Security X-Force Threat Intelligence combines IBM security operations telemetry, research, incident response investigations, commercial data, and open sources to aid clients in understanding emerging threats and quickly making informed security decisions.

Additionally, the highly-trained X-Force Incident Response team provides strategic remediation that helps organizations achieve better control over security incidents and breaches.

X-Force combined with the IBM Security Command Center cyber range experiences train clients to be ready for the realities of today's threats.

Throughout the year, IBM X-Force researchers also provide ongoing research and analysis in the form of blogs, white papers, webinars and podcasts, highlighting our insight into advanced threat actors, new malware, and new attack methods. In addition, we provide a large body of current, cutting-edge analysis to subscription clients on our Premier Threat Intelligence platform.

### Take the next step

Learn about orchestrating your incident response with IBM Security >

## About IBM Security

IBM Security works with you to help protect your business with an advanced and integrated portfolio of enterprise security products and services, infused with AI, and a modern approach to your security strategy using a zero trust principles, helping you thrive in the face of uncertainty. By aligning your security strategy to your business; integrating solutions designed to protect your digital users, assets, and data; and deploying technology to manage your defenses against growing threats, we help you to manage and govern risk that supports today's hybrid cloud environments.

Our new modern, open approach, the IBM Cloud Pak for Security platform, is built on RedHat Open Shift and supports today's hybrid multi cloud environments with an extensive partner ecosystem. Cloud Pak for Security is an enterprise-ready containerized software solution that enables you to manage the security of your data and applications –by quickly integrating your existing security tools to generate deeper insights into threats across hybrid cloud environments– leaving your data where it is, allowing easy orchestration and automation of your security response.

For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

## Contributors

**Lead author:**
Camille Singleton

**Contributors:**
Allison Wikoff
Ari Eitan (Intezer)
Charles DeBeck
Charlotte Hammond
Chenta Lee
Chris Sperry
Christopher Kiefer
Claire Zaboeva
David McMillen
David Moulton
Dirk Hartz
Georgia Prassinos
Ian Gallagher (Intezer)
John Zorabedian
Joshua Chung
Kelly Kane
Lauren Jensen
Limor Kessem
Mark Usher
Martin Steigemann
Matthew DeFir
Megan Radogna
Melissa Frydrych
Michelle Alvarez
Mitch Mayne
Nick Rossman
Patty Cahill-Ingraham
Randall Rossi
Richard Emerson
Salina Wuttke
Scott Craig
Scott Moore



IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2021



IBM **Security**