Q1 2024

FIR

FRAUD INTELLIGENCE REPORT
EMPOWERING BUSINESSES TO OUTSMART FRAUD

APRIL 2024 EDITION

FIR RISK ADVISORY LLC

FIR RISK ADVISORY LLC

FIRRISKADVISORY.COM

Q1 -2024

Introduction to the Fraud Intelligence Report (**FIR**): My last role as Senior Director, Fraud Prevention and Risk Compliance for a global technology company exposed me to the scale, rapid rise, and impact of the fraud threat landscape, especially in the world of e-commerce. My objective for this **first edition report** is to educate my peers, co-workers, and business leaders about the reality of online fraud and how this can cost your business millions in wasted fees, lost product, stolen data and lost reputation. We have sourced all the intelligence you find within this report from open-source communities, resources, and services. Our extensive review process has sifted thought all the available material and we are focused on presenting the **big picture** about the current fraud threat landscape, **risk vectors** that fraudsters commonly abuse, and **cybersecurity news** bulletins to keep you informed of recent events. We wrap with **key takeaways** as reminders to stay vigilant in protecting your business.

Our objective is to help you and your business stay aware, highlight current risk trends, and share resources to use to improve your cybersecurity posture and prevent fraud.

Empowering businesses to outsmart fraud!

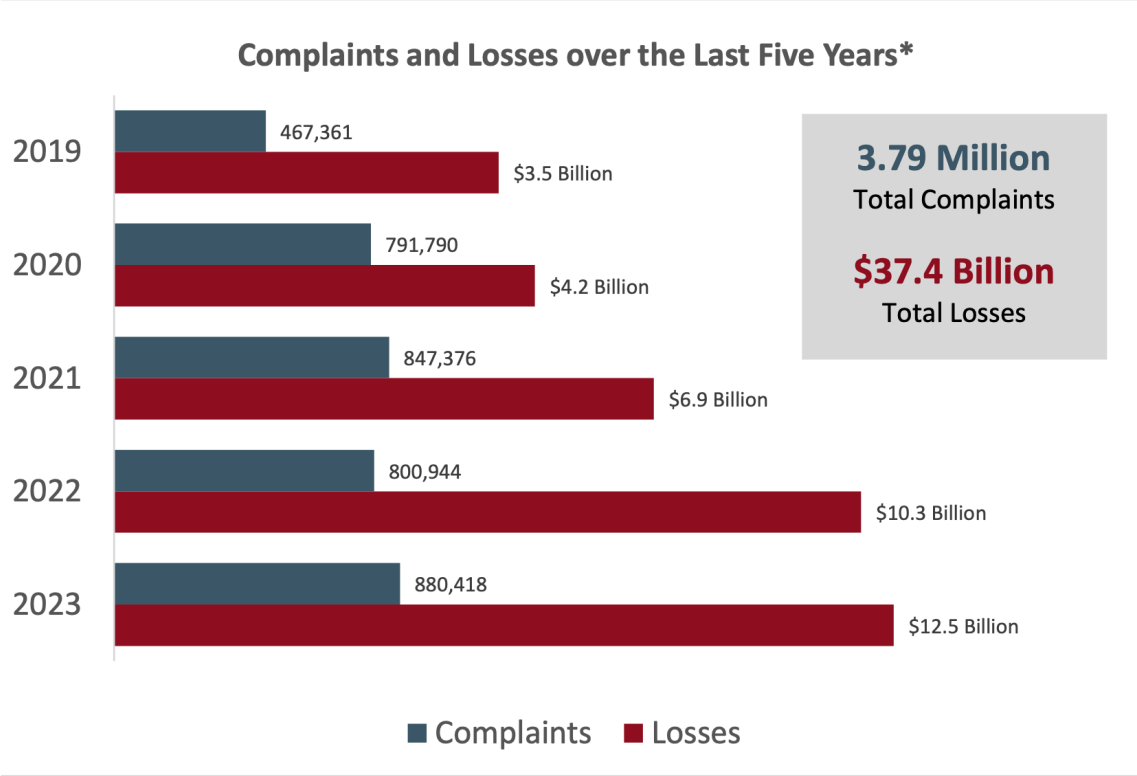
Bruce Bird, Principal, FIR Risk Advisory LLC

TABLE OF CONTENTS

BIG PICTURE

Lets start with various headlines from leading law enforcement and government sponsored sources from the past few months:

- The FBI Internet Crime Complaint Center (ic3.gov) released the 2023 IC3 Annual Report in early March 2024. In 2023, the IC3 received a record number of complaints from the American public: 880,418 complaints, with potential **losses exceeding $12.5 billion**. This is nearly a 10% increase in complaints, and represents a **22% increase** in losses, compared to 2022.



2023 IC3 Report

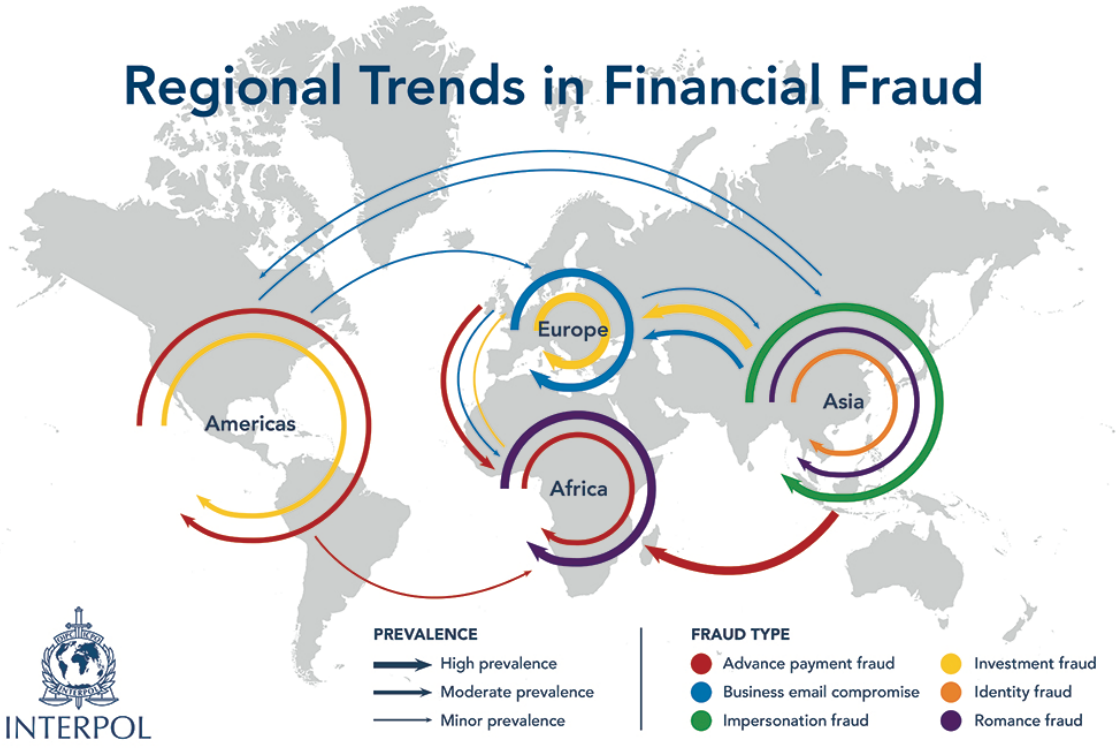
- A new INTERPOL assessment (https://www.interpol.int/) released on March 11, 2024 on global financial fraud highlights how the increased use of technology is enabling organized crime groups to better target victims around the world. The use of Artificial Intelligence (AI), large language models and cryptocurrencies combined with

phishing- and ransomware-as-a-service business models have resulted in more sophisticated and professional fraud campaigns without the need for advanced technical skills, and at relatively little cost.

- INTERPOL Secretary General Jürgen Stock said:

  "We are facing an **epidemic in the growth of financial fraud**, leading to individuals, often vulnerable people, and companies being defrauded on a massive and global scale.

  "Changes in technology and the rapid increase in the scale and volume of organized crime has driven the creation of a range of new ways to defraud innocent people, business and even governments. With the development of AI and Cryptocurrencies, the **situation is only going to get worse** without urgent action."



https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology

- Europol's (https://www.europol.europa.eu/) new report, published April 5, 2024, entitled "Decoding the EU's most threatening criminal networks", delves into the characteristics of 821 criminal networks that pose the highest threat.

    - This first-of-its-kind EU-wide assessment decodes the ABCD of the most threatening criminal networks – they are **Agile**, **Borderless**, **Controlling** and **Destructive**.

    - **9 most threatening criminal networks focus on cyber-attacks**, main nationalities are Russian, Ukrainian and operate in France, Germany, Switzerland and the United States.

    - **Cybercrime As A Service**: Genesis Market, one of the biggest criminal facilitators **selling stolen account credentials** to hackers worldwide, is taken down. This marketplace offers for sale so called 'bots' that infect victims' devices **through malware or account takeover attacks**. Such a bot provides criminals access to all the data stored on the devices, such as logins and passwords. The price per bot ranges from USD 0.70 to several hundreds of dollars depending on the amount and nature of the stolen data. The most expensive ones contain financial information that give access to online banking accounts.

- The United Kingdom National Cyber Security Centre (NCSC) released a report January 24, 2024 on the near-term **impact of AI on the cyber threat** (https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat), a few key judgments from the report:

    - Artificial intelligence (AI) will **almost certainly increase the volume and heighten the impact of cyber attacks** over the next two years. However, the impact on the cyber threat will be uneven.

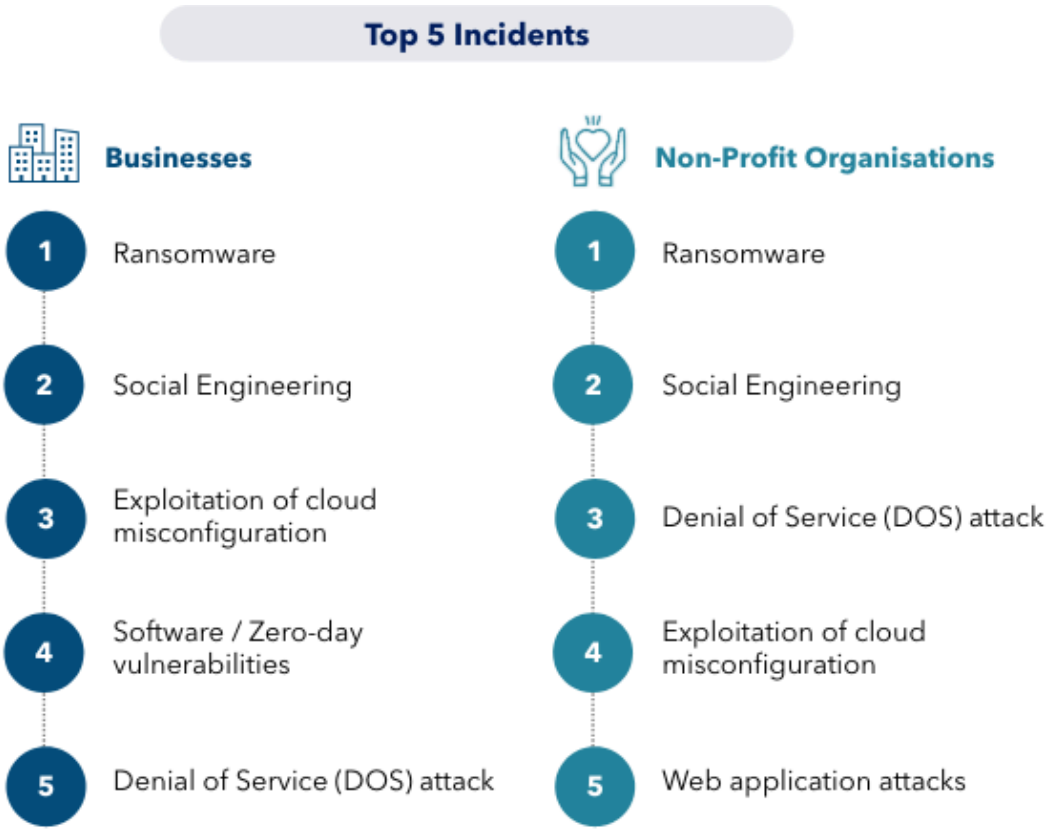
    - AI will almost certainly make cyber attacks more impactful because **threat actors will be able to analyze exfiltrated data faster and more effectively, and use it to train AI models**.

    - All types of cyber threat actor – state and non-state, skilled and less skilled – **are already using AI,** to varying degrees.

- AI provides **capability uplift in reconnaissance and social engineering**, almost certainly making both more effective, efficient, and harder to detect.

- AI lowers the barrier for novice cyber criminals, hackers-for-hire and hacktivists to carry out effective access and information gathering operations. This **enhanced access will likely contribute to the global ransomware threat** over the next two years.

- Singapore's Cyber Security Agency (https://www.csa.gov.sg/) released their Cybersecurity Health Report on March 28, 2024 with key findings of cybersecurity incidents that organizations are vulnerable to, business impact of those incidents, and how organizations manage their cybersecurity. Highlights include:
  - **Over 8 in 10 organizations have encountered a cybersecurity incident in a year**



Singapore Cybersecurity Health Report 2023

- **Only 1 in 3 organizations** have implemented **3 OR MORE** categories of measures in Cyber Essentials, challenges in adopting cybersecurity:

Singapore Cybersecurity Health Report 2023

Turning to a couple vendors who published free-to-download reports recently, that caught our attention:

- CrowdStrike (https://www.crowdstrike.com/) "2024 Global Threat Report" highlights eCrime, a highly attractive and lucrative business venture for many criminals. The report claims that **eCrime** persisted **as the most pervasive threat across the 2023 threat landscape** as adversaries leverages techniques to maximize stealth, speed and impact.

- **75%** increase in cloud intrusions
- **75%** of attacks were malware-free

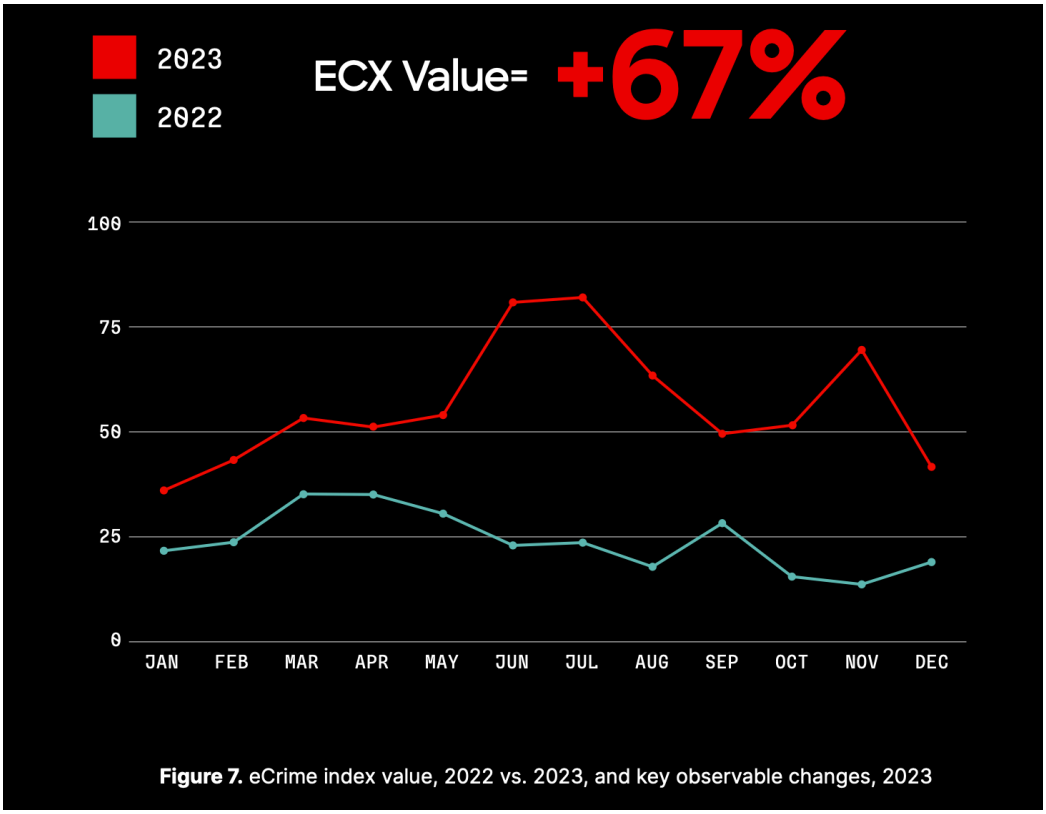


Figure 7. eCrime index value, 2022 vs. 2023, and key observable changes, 2023

https://go.crowdstrike.com/global-threat-report-2024.html

- Zscaler (https://www.zscaler.com) "2023 ThreatLabz State of Encrypted Attacks Report" reveals **threats over HTTPS grew by 24.3% year-over-year** (as observed in the Zscaler cloud) with United States and India as top targets of encrypted attacks and a significant **85.9% of total threats are now delivered over encrypted channels**!
- The top most affected industries are:

Industry	Hits (2023)	Hits (2022)	% increase or decrease
Manufacturing	9,403,706,582	7,494,604,812	25.5
Technology and communication	6,956,157,168	7,323,180,837	-5.0
Services	3,978,413,560	2,187,364,878	81.9
Healthcare	2,359,043,105	1,827,667,810	29.1
Education	1,998,373,381	530,937,876	276.4
Finance and insurance	1,804,458,367	2,419,792,119	-25.4
Government	1,567,591,565	549,974,161	185.0
Others	942,462,021	1,092,807,995	-13.8
Retail and wholesale	709,096,364	811,342,584	-12.6

Zscaler ThreatLabz 2023 State of Encrypted Attacks Report

The above are just a few resources that are online and available to us for information sharing. Each quarter, we will be searching for the most relevant and up-to-date sources to bring to you. The trend of fraudulent activity by external threat actors has been escalating quickly since 2018 and accounts for well **over 80%** of all cyber attacks. The largest motive is financial ("Verizon 2023 Data Breach Investigations Report" reported **94.6% of the data breaches they investigated were driven by financial motives**) and Corporations are at risk of being victimized by the sophistication, agility, and resourcefulness of these threat actors.

Our objective is to shine the light on fraudster activity and how that activity impacts the risk for Organizations of all sizes. This report (FIR) is intended to keep you up to date on the many resources, fraud news, and global/regional trends as concisely as possible.

INSIGHT #1: CYBER CRIME IS BIG BUSINESS AND CONTINUES TO RISE; ALL ORGANIZATIONS ARE AT RISK.

INSIGHT #2: AI IS A GAME CHANGER AND YOU MUST PREPARE NOW!

TOP RISK VECTORS/ ATTACKS TREND

Global financial fraud trends making the news:

1. Business Email Compromise (BEC) and Social Engineering Attacks:

Verizon 2023 Data Breach Investigations Report Summary of findings "Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 5, and now represent more than **50% of incidents within the Social Engineering pattern**."

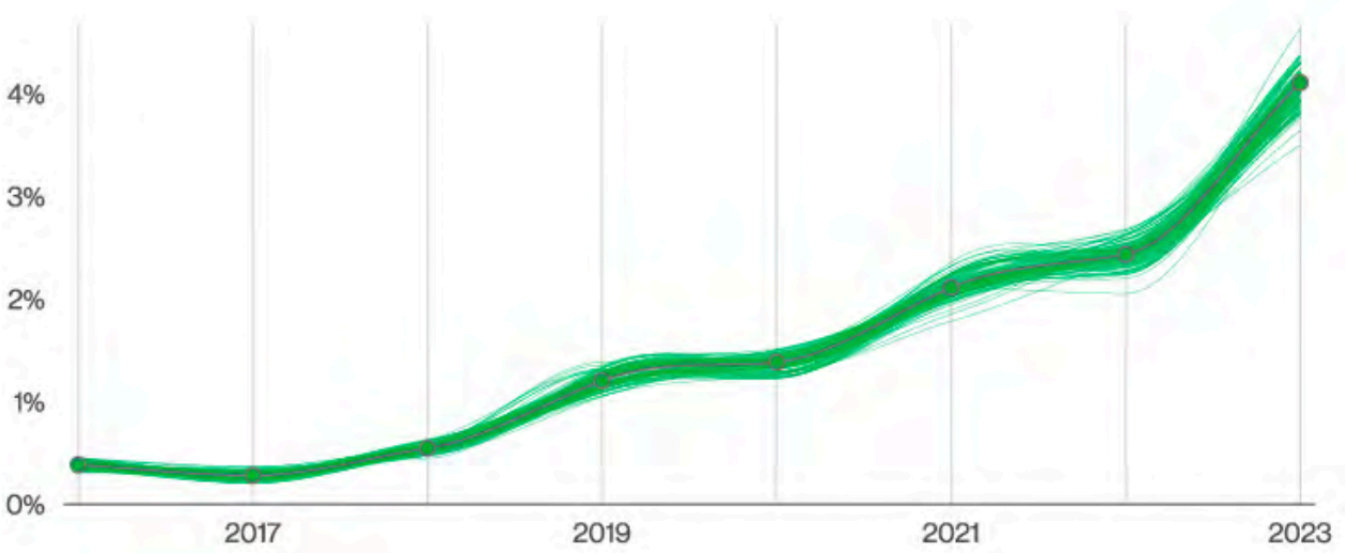


Figure 5. Pretexting incidents over time

Verizon 2023 Data Breach Investigations Report

Phishing with a Personal Touch: Attackers are becoming more sophisticated in crafting personalized spear phishing emails that target specific individuals within a company. These emails may leverage information gleaned from social media or data breaches to appear legitimate.

Supply Chain Compromise: Criminals are increasingly targeting third-party vendors and partners within a corporation's supply chain. By compromising a supplier's email system, attackers can impersonate legitimate vendors and initiate fraudulent payments.

INSIGHT #3: EMAIL COMPROMISE LEADS TO BIG FRAUD SUCCESS; PATCH EMAIL SERVERS TIMELY AND PROTECT AGAINST SOCIAL ENGINEERING ATTACKS.

2. Deepfakes and Synthetic Identity Fraud:

Evolving Technology, Growing Threat: The use of deepfakes (realistic AI-generated videos) to impersonate executives for fraudulent purposes is a growing concern.

Synthetic Identities for Financial Gain: Criminals are creating synthetic identities, combining real and fabricated data, to bypass fraud detection systems and open fraudulent accounts or obtain loans.

INSIGHT #4: BORN-BAD AKA FAKE ACCOUNTS ARE A FOOTHOLD FOR FRAUDSTERS INTO YOUR BUSINESS.

3. Ransomware and Extortion:

Double Extortion Schemes: Ransomware attackers are now not only encrypting data but also stealing it before encryption, threatening to leak it if the ransom isn't paid. This "double extortion" tactic puts even more pressure on victims to pay.

RaaS (Ransomware as a Service) Model: The rise of RaaS lowers the barrier to entry for cybercriminals, making ransomware attacks more widespread.

Verizon DBIR reported that “Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically

steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries."

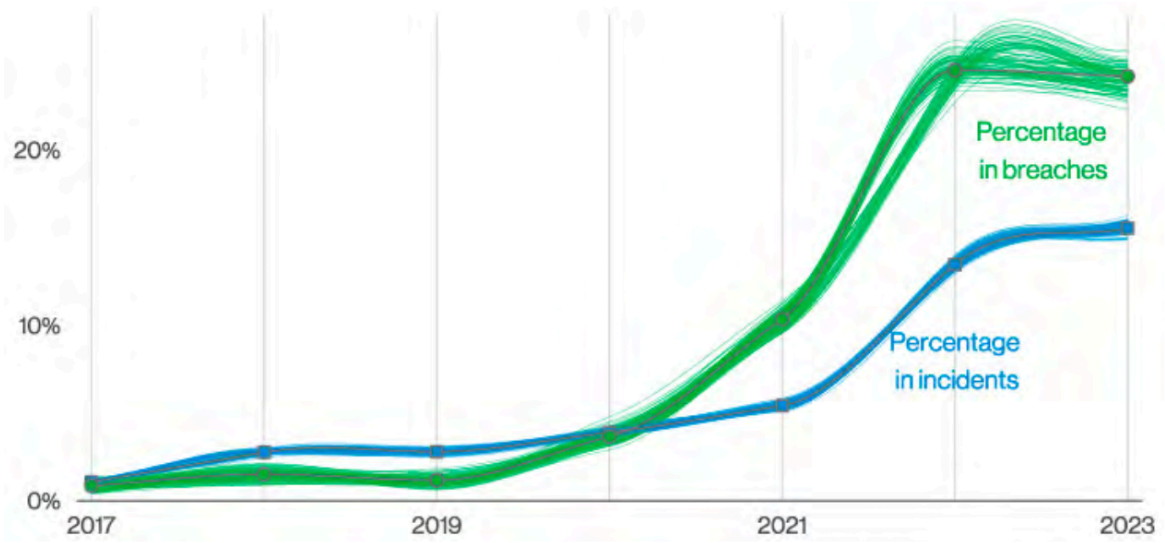


Figure 8. Ransomware action variety over time

Verizon 2023 Data Breach Investigations Report

4. Cloud-Based Fraud:

Exploiting Cloud Vulnerabilities: As more corporate data and applications migrate to the cloud, attackers are increasingly targeting vulnerabilities in cloud platforms and misconfigured cloud security settings.

Account Takeover (ATO) in the Cloud: Cloud-based accounts are valuable targets for attackers. Adversaries can authenticate to a system and/or user account using stolen credentials. Session cookies and tokens can be stolen to masquerade as the legitimate user and authenticate to an application. One-time-passwords (OTPs) theft allows the adversary to bypass multi-factor authentication (MFA) by email compromise, socially engineering the victim, or other advanced attack methods. Once compromised, these

accounts can be used to steal data and/or assets, commit payment fraud; test credit cards on your payment platform; and deploy malware, or launch further attacks.

INSIGHT #5: ACCOUNT TAKEOVERS ARE IDEAL FOR FRAUDSTERS TO MASK/HIDE THEIR ACTIVITY WITHIN YOUR REAL CUSTOMERS AND USER ACCOUNTS.

Emerging Fraud Methods: Fraudsters are constantly innovating and developing new methods to exploit vulnerabilities. **Cryptocurrency** is a big target and fraudsters are focused on getting their share. Three emerging trends in 2024 are: 1. **Phishing Attacks:** Criminals send emails or messages impersonating legitimate cryptocurrency exchanges or wallets, tricking users into revealing their login credentials or sending crypto to fraudulent addresses. 2. **Rug Pulls:** Developers create a seemingly legitimate cryptocurrency, build a community, then abandon the project and steal all invested funds. 3. **Social Engineering:** Attackers leverage social media and messaging platforms to manipulate users into sending cryptocurrency to them!

Staying informed about the latest threats is crucial for corporations to maintain a strong security posture.

By prioritizing cybersecurity and staying informed about the latest fraud tactics, organizations of all sizes can significantly reduce their risk of falling victim to these increasingly sophisticated attacks.

INSIGHT #6: PAYMENT FRAUD IS ONE OF THE EASIEST FRAUDS TO CONDUCT AND RESULT IN CHARGEBACKS AS STOLEN CARD DATA IS USED.

INSIGHT #7: CARD TESTING IS A "FREE SERVICE" TO FRAUDSTERS IF YOUR PAYMENT PLATFORM DOESN'T BLOCK FAKE CARD VERIFICATIONS AND AUTHORIZATIONS.

INSIGHT #8: CRYPTOCURRENCY IS A FOCUS OF THREAT ACTORS.

ATTACKS AND ATTACKERS MAKING NEWS

- Cybersecurity & Infrastructure Security Agency (https://www.cisa.gov/news-events/cybersecurity-advisories) released a cybersecurity advisory on February 26, 2024 detailing recent tactics, techniques, and procedures (TTPs) of the group commonly know as **APT29**, also known as Midnight Blizzard, the Dukes, or Cozy Bear.

- The UK National Cyber Security Centre (NCSC) and international partners assess that APT29 is a cyber espionage group, **almost certainly part of the SVR**, an element of the **Russian intelligence services**. The US National Security Agency (NSA), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Cyber National Mission Force (CNMF), the Federal Bureau of Investigation (FBI), Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (CCCS), and New Zealand Government Communications Security Bureau (GCSB) agree with this attribution and the details provided in this advisory. To download the PDF version of this report: https://www.ncsc.gov.uk/files/Advisory-SVR-cyber-actors-adapt-tactics-for-initial-cloud-access.pdf.

- Attack details of the advisory include:

    - Previous SVR campaigns reveal the actors have successfully **used brute forcing and password spraying to access service accounts**. This type of account is typically used to run and manage applications and services. There is no human user behind them so they cannot be easily protected with multi-factor authentication (MFA), making these accounts more susceptible to a successful compromise.

    - **SVR campaigns have also targeted dormant accounts** belonging to users who no longer work at a victim organization but whose accounts remain on the system. Following an enforced password reset for all users during an incident, SVR actors have also been observed logging into inactive accounts and following instructions to reset the password. This has allowed the actor to regain access following incident response eviction activities.

INSIGHT #9: CLEAN UP OLD SERVICE ACCOUNTS; DISABLE DORMANT USER ACCOUNTS.

- Account access is typically authenticated by either username and password credentials or system-issued access tokens. The NCSC and partners have observed **SVR actors using tokens to access their victims' accounts**, without needing a password. The default validity time of system-issued tokens varies dependent on the system; however, cloud platforms should allow administrators to adjust the validity time as appropriate for their users.

INSIGHT #10: EVALUATE YOUR AUTHENTICATION TOKENS/COOKIE ACTIVITY TO VERIFY THE ACCOUNT OWNER IS THE USER ACCESSING THEIR ACCOUNT.

- On multiple occasions, the **SVR have successfully bypassed password authentication** on personal accounts using password spraying and credential reuse. SVR actors have also then bypassed MFA through a technique known as "MFA bombing" or "MFA fatigue," in which the actors repeatedly push MFA requests to a victim's device until the victim accepts the notification. Once an actor has bypassed these systems to gain access to the cloud environment, SVR actors have been observed registering their own device as a new device on the cloud tenant. If device validation rules are not set up, SVR actors can successfully register their own device and gain access to the network.

INSIGHT #11: ONE-TIME-PASSWORDS AND PASSCODES CAN BE BYPASSED BY SKILLFUL THREAT ACTORS; USER ACCOUNT HYGIENE IS THE RESPONSIBILITY OF THE ACCOUNT OWNER, BUT ORGANIZATIONS NEED TO ENSURE BEST PRACTICES ARE FOLLOWED.

- As network-level defenses improve detection of suspicious activity, SVR actors have looked at other ways to stay covert on the internet. A TTP associated with this actor is the **use of residential proxies**. Residential proxies typically make traffic appear to originate from IP addresses within internet service provider (ISP) ranges used for residential broadband customers and hide the true source. This can make it harder to distinguish malicious connections from typical users. This reduces the effectiveness of network defenses that use IP addresses as indicators of

compromise, and so it is important to consider a variety of information sources such as application and host-based logging for detecting suspicious activity.

- The New Zealand National Cyber Security Centre (**NCSC**) posted on March 20, 2024 a security advisory regarding both the observed activities of the People's Republic of China (PRC)-linked state sponsored actor '**Volt Typhoon**', and how network defenders can mitigate these efforts. Today, the NCSC along with 10 international partners are publishing an additional fact sheet relating to this actor specifically for the owners and operators of critical national infrastructure so they can better secure their assets against this activity.

- This fact sheet provides an overview for executive leaders on the urgent risk posed by the **PRC state-sponsored cyber actors known as 'Volt Typhoon**.' Previous advisories released by CISA warned cyber security defenders that Volt Typhoon has been pre-positioning themselves on U.S. critical infrastructure organizations networks to enable disruption or destruction of critical services in the event of increased geopolitical tensions and/or military conflict with the United States and its allies. This is **a critical business risk for every organization in the United States and allied countries. See fact sheet here:** https://www.ncsc.govt.nz/assets/Uploads/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c_0-updated.pdf

INSIGHT #12: CHINA AND RUSSIAN STATE SPONSORED THREAT ACTORS ARE AGGRESSIVELY PURSUING UNITED STATES TARGETS & ORGANIZATIONS.

HOW TO PROTECT YOUR BUSINESS

To stay ahead of the evolving fraud trends, Cybersecurity program best practices include the following elements and vary greatly in implementation and maturity. Security Teams that are comprised of Security Operations, Application Security, Fraud Operations, and Security Governance are key pillars of a modern security team. As the first edition, we are beginning with the basics and will provide more comprehensive details in future reports:

- Implement robust security awareness training programs for employees.

- Employ multi-factor authentication (MFA) to secure access to critical systems.
- Conduct regular risk assessments to evaluate your vulnerability to attacks
- Regularly patch and update software and systems.
- Segment networks to limit the impact of a breach.
- Invest in threat intelligence and monitoring capabilities.
- Remediate application security vulnerabilities and drive secure coding best practices to reduce your application's attack surface.
- Build and report security metrics and operational intelligence.
- Have a comprehensive incident response plan in place and run simulation exercises. Practice, practice, practice!

PEOPLE & PROCESSES:

Security Awareness Training: Regularly train employees on cybersecurity best practices, including identifying phishing attempts, password hygiene, and reporting suspicious activity. Make training engaging and role-play real-world scenarios to enhance effectiveness.

Least Privilege Access Control: Implement the principle of least privilege, granting users only the minimum level of access required to perform their jobs. This reduces the potential damage caused by compromised accounts.

Segregation of Duties: Separate critical tasks (e.g., transaction initiation and approval) among different employees to prevent a single individual from perpetrating fraud.

Incident Response Plan: Develop and regularly test a comprehensive incident response plan outlining procedures for detecting, containing, and recovering from a cyberattack.

Third-Party Risk Management: Rigorously assess the cybersecurity posture of third-party vendors and partners before granting them access to corporate systems or data.

TECHNOLOGY & SECURITY MEASURES:

Multi-Factor Authentication (MFA): Enforce MFA for all access attempts to critical systems and cloud-based applications. MFA adds an extra layer of security beyond traditional passwords.

Email Security Solutions: Implement robust email security solutions that can detect and filter out phishing attempts, spam emails, and malware attachments.

Endpoint Detection and Response (EDR) Systems: Deploy EDR solutions to continuously monitor endpoints for malicious activity and enable rapid response to threats.

Data Loss Prevention (DLP) Systems: Utilize DLP tools to prevent sensitive data from being exfiltrated from the corporate network.

Network Segmentation: Segment your network to limit the lateral movement of attackers within your infrastructure if a breach occurs.

Regular Patching and Updates: Maintain a rigorous patching schedule to address vulnerabilities in operating systems, applications, and firmware as soon as updates become available.

SDLC & Secure Coding: Build security into development from the start to prevent vulnerabilities.

Input Validation & Access Control: Block common attacks and limit data access based on user needs.

Encryption: Protect sensitive data in transit and at rest.

Cloud Security Best Practices: If leveraging cloud-based services, ensure you follow best practices for securing cloud configurations and access controls.

ADDITIONAL STRATEGIES:

Threat Intelligence: Subscribe to threat intelligence reports (the Fraud Intelligence Report you are reading now is a very cost effective, quarterly starting point) and feeds to stay informed about the latest attack methods used by cybercriminals.

Penetration Testing: Conduct regular penetration testing to identify vulnerabilities in your systems and network before attackers do.

Cybersecurity Insurance: Consider purchasing cyber insurance to help offset the financial costs associated with a cyberattack.

REMEMBER:

- **Constant Vigilance is Key:** The cybersecurity landscape is constantly evolving, so continuous improvement and adaptation of your security posture is essential.

- **Focus on Prevention and Early Detection:** Prioritize preventative measures and early detection mechanisms to minimize the impact of potential fraud attempts.

- **Culture of Security:** Foster a culture of security within your organization where employees are encouraged to report suspicious activity without fear of reprisal.

NIST CYBERSECURITY FRAMEWORK 2.0 IS HERE!

https://csrc.nist.gov/news/2024/the-nist-csf-20-is-here

By implementing best practices and maintaining a proactive approach to cybersecurity, global corporations can significantly enhance their defenses against fraud-motivated attacks.

KEY TAKEAWAYS/ ACTION ITEMS

TAKEAWAY #1 ANALYZE YOUR DATA: Financial motives is driving fraudulent activity, all organizations are targets of criminal and state-sponsored threat actors, organizations that do business online are easy targets for abuse, both as a platform for fraud AND as a source of cash and assets for fraudsters. You need to analyze your incoming traffic and transactional data to find the suspicious patterns of activity, deep analysis will reveal the fake/ fraudulent activity. Look and you will find! The more you look, the more you will find!! Start training ML and AI models to help you uncover the risks within your datasets.

TAKEAWAY #2 MANAGE USER ACCOUNTS: Fraudsters will create fake accounts to gain a foothold into your business, they will work hard to crack passwords to takeover user accounts, they will buy stolen credentials and authentication cookies to gain access to your user accounts. Be aware and prepare by analyzing your account usage, define and disable dormant users, identify and disable abusive and fake users, and of course, remove unused service accounts to reduce your attack surface!

TAKEAWAY #3 ENFORCE ACCESS CONTROLS: Help your users maintain secure accounts by enforcing best practices and features for account hygiene; use activity notifications to keep account owners aware of activity; enforce strong password practices; allow users to opt into MFA (or require) to better secure accounts; bind authentication cookies to user fingerprints to ensure the account owner who logged into the account, is the user returning to their account!

TAKEAWAY #4 SECURE WEB APPLICATIONS: Web application attacks is the top risk vector in both breaches and incidents. Identifying and remediating web application vulnerabilities is necessary to better secure your applications and practicing secure coding and software development best practices is key to building security into software designs and driving long lasting improvements.

FIR RISK ADVISORY PRODUCTS AND SERVICES

FRAUD INTELLIGENCE REPORTING (FIR)

Our fraud intelligence reporting services provide businesses with real-time insights into potential fraud threats, allowing them to take proactive measures to prevent fraud. We publish a in-depth Quarterly Fraud Intelligence Report (FIR) via a paid annual subscription and a free monthly newsletter to keep you informed and give you actionable intelligence to help you protect your business!

FRAUD STRATEGY & IMPLEMENTATION

We develop and implement a comprehensive fraud prevention plan that is tailored to your business needs and risks, ensuring that your organization is protected from potential fraud threats.

RISK ASSESSMENTS

Our risk assessment services provide businesses with a comprehensive understanding of their existing risks and vulnerabilities, allowing them to develop effective risk mitigation strategies.

COMPLIANCE MANAGEMENT

We provide comprehensive compliance management services that help businesses stay compliant with regulatory requirements and avoid potential legal and financial risks.

RESOURCES

We rely on open-source information provided by government sponsored organizations and agencies as trusted sources, the below represents a partial listing of those agencies or departments that share quality intelligence.

Cybersecurity and Infrastructure Security Agency (CISA): Established in 2018 within the Department of Homeland Security (DHS), CISA is the national hub for cybersecurity coordination. They provide resources, tools, and guidance to businesses, government agencies, and individuals to strengthen their cybersecurity posture.

Federal Bureau of Investigation (FBI): The FBI investigates cybercrime activities, including hacking, data breaches, and online fraud. They also work to disrupt cyberattacks and bring cybercriminals to justice.

European Union Agency for Cybersecurity (ENISA): ENISA is an agency of the European Union (EU) focused on achieving a high common level of cybersecurity across the member states. They provide advice and expertise to EU institutions and member states, develop cybersecurity tools and methods, and help to raise awareness of cybersecurity risks.

Australia's Australian Cyber Security Centre (ACSC): Part of the Australian Signals Directorate (ASD), the ACSC provides cybersecurity advice and assistance to Australian businesses and individuals. They also work with international partners to combat cybercrime.

Canada's Canadian Centre for Cyber Security (CCCS): The CCCS is a government agency that leads Canada's national effort to combat cyber threats. They offer a variety of resources and services to help businesses and individuals stay safe online.

The United Kingdom's National Cyber Security Centre (NCSC): A part of GCHQ, the NCSC leads the UK government's response to cyber threats. They provide advice and guidance to businesses, government, and the public on how to protect themselves from cyberattacks.

Singapore's Cyber Security Agency (CSA): The CSA is the lead agency for cybersecurity in Singapore. They develop and implement national cybersecurity strategies, oversee incident response activities, and promote cybersecurity awareness.

Interpol: Formally known as the International Criminal Police Organization, is the world's largest international police organization. Founded in 1923, it acts as a network connecting law enforcement agencies from 196 member countries.

We also review and source from various authoritative for-profit entities, who provide products and services to help secure business. Those vendors mentioned within this report include:

Verizon DBIR: The Verizon Data Breach Investigations Report (DBIR) is a highly respected annual publication produced by Verizon. It's a valuable resource for anyone interested in understanding cybersecurity threats and trends. While the 2024 Verizon DBIR isn't available yet (as of April 18, 2024), Verizon is hosting several DBIR webinars on May 1, 2024. You can register for events and find the most recent DBIR and previous editions: **verizon.com/dbir/**

CrowdStrike: CrowdStrike is a prominent American cybersecurity company headquartered in Austin, Texas. They specialize in Cloud Workload & Endpoint Security; Threat Intelligence; and Cyberattack Response Services. **https://www.crowdstrike.com/en-us/**

Zscaler: Zscaler is a prominent cloud security company headquartered in San Jose, California. They offer a suite of enterprise cloud security services designed to protect businesses in today's increasingly digital world. **https://www.zscaler.com/**

Resources to help you evaluate your security posture and advise on best practices to protect your business (all the Government sponsored sites listed above also provide security guidance and best practices):

National Institute of Standards and Technology (NIST): NIST develops cybersecurity frameworks and standards that businesses and government agencies can use to improve their cybersecurity posture. They also conduct research on cybersecurity technologies and best practices. **https://www.nist.gov/**

The Center for Internet Security (CIS): CIS is a non-profit organization founded in 2000 that works to improve cybersecurity for everyone. They develop and share best practices to help individuals, businesses, and governments defend against cyber threats. CIS achieves this through CIS Controls and CIS Benchmarks. **https://www.cisecurity.org/**

Open Worldwide Application Security Project (OWASP). OWASPis a non-profit organization that acts as a global community for web security. They provide free resources like articles, tools, and documentation to improve software security, with a focus on web applications and Internet of Things (IoT) devices. Their most well-known project is the OWASP Top 10, which is a regularly updated list of the most critical web application security risks. **https://owasp.org/**