Introduction

Greetings! Welcome to Verizon's 2024 Data Breach Investigations Report (DBIR). This year marks the 17th edition of this publication, and we are thrilled to welcome back our old friends and say hello to new readers. As always, the aim of the DBIR is to shine a light on the various Actor types, the tactics they utilize and the targets they choose. Thanks to our talented, generous and civic-minded contributors from around the world who continue to stick with us and share their data and insight, and deep appreciation for our very own Verizon Threat Research Advisory Center (VTRAC) team (rock stars that they are). These two groups enable us to examine and analyze relevant trends in cybercrime that play out on a global stage across organizations of all sizes and types.

From year to year, we see new and innovative attacks as well as variations on tried-and-true attacks that still remain successful. From the exploitation of well-known and far-reaching zero-day vulnerabilities, such as the one that affected MOVEit, to the much more mundane but still incredibly effective Ransomware and Denial of Service (DoS) attacks, criminals continue to do their utmost to prove the old adage "crime does not pay" wrong.

The shifting landscape of cyber threats can be confusing and overwhelming. When, in addition to the attack types mentioned above, one throws in factors such as the human element and/or poorly protected passwords, things become even more confused. One might be forgiven for viewing the current state of cybersecurity as a colorful cyber Mardi Gras parade. Enterprise floats of all shapes and sizes cruising past a large crowd of threat actors who are shouting out gleefully "Throw me some creds!" Of course, human nature being what it is, all too often, the folks on the floats do just that. And, as with all such parades, what is left in the aftermath isn't necessarily pretty. The past year has been a busy one for cybercrime. We analyzed 30,458 real-world security incidents, of which 10,626 were confirmed data breaches (a record high!), with victims spanning 94 countries.

While the general structure of the report remains the same, long-time readers may notice a few changes. For example, the "first-time reader" section is now located in Appendix A rather than at the beginning of the report. But we do encourage those who are new to the DBIR to give it a read-through before diving into the report. It should help you get your bearings.

Last, but certainly not least, we extend a most sincere thanks yet again to our contributors (without whom we could not do this) and to our readers (without whom there would be no point in doing it).

Sincerely,

The Verizon DBIR Team
C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup

Very special thanks to:
– Christopher Novak for his continued support and insight
– Dave Kennedy and Erika Gifford from VTRAC
– Kate Kutchko, Marziyeh Khanouki and Yoni Fridman from the Verizon Business Product Data Science Team

Helpful guidance

About the 2024 DBIR incident dataset

Each year, the DBIR timeline for in-scope incidents is from November 1 of one calendar year through October 31 of the next calendar year. Thus, the incidents described in this report took place between November 1, 2022, and October 31, 2023. The 2023 caseload is the primary analytical focus of the 2024 report, but the entire range of data is referenced throughout, notably in trending graphs. The time between the latter date and the date of publication for this report is spent in acquiring the data from our global contributors, anonymizing and aggregating that data, analyzing the dataset, and finally creating the graphics and writing the report. The jokes, sadly, do not write themselves.

Credit where credit is due

Turns out folks enjoy citing the report, and we often get asked how to go about doing it.

You are permitted to include statistics, figures and other information from the report, provided that (a) you cite the source as “Verizon 2024 Data Breach Investigations Report” and (b) the content is not modified in any way. Exact quotes are permitted, but paraphrasing requires review. If you would like to provide people a copy of the report, we ask that you provide them a link to verizon.com/dbir rather than the PDF.

Questions? Comments? Concerns? Love to share cute pet pictures?

Let us know! Send us a note at dbir@verizon.com, find us on LinkedIn, tweet @VerizonBusiness with #dbir. Got a data question? Tweet @VZDBIR!

If your organization aggregates incident or security data and is interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at **dbircontributor@verizon.com**.

Summary of findings

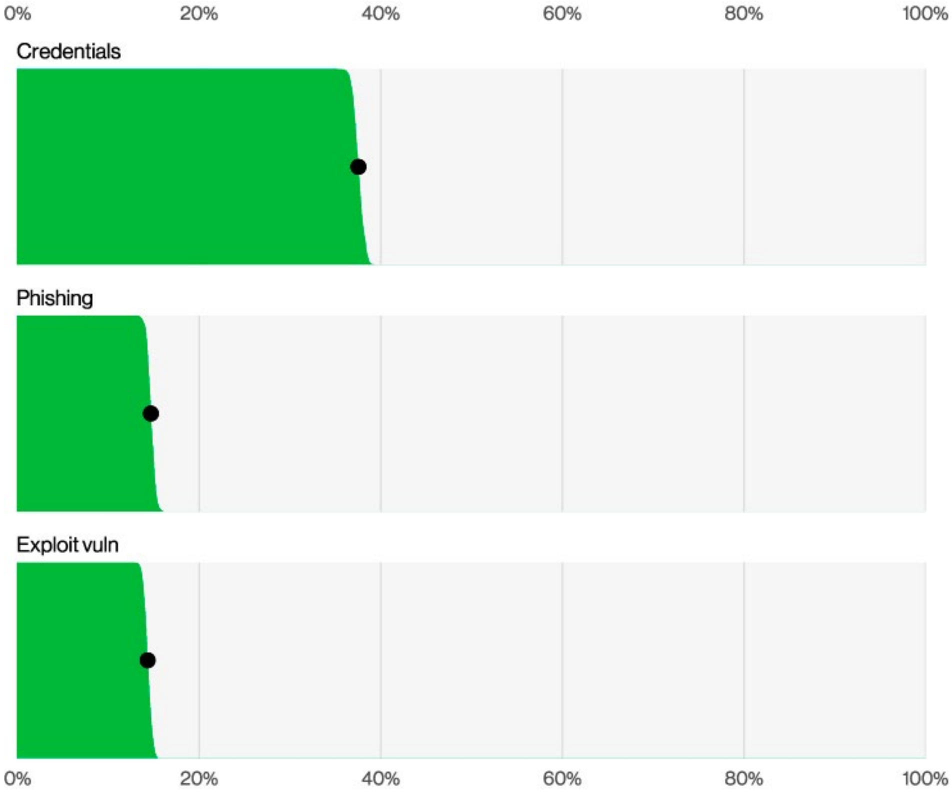

Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year, which will come as no surprise to anyone who has been following the effect of MOVEit and similar zero-day vulnerabilities. These attacks were primarily leveraged by Ransomware and other Extortion-related threat actors. As one might imagine, the main vector for those initial entry points was Web applications.

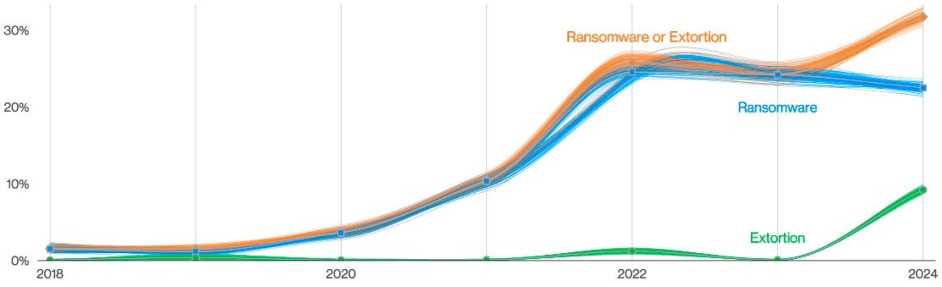

Figure 2. Ransomware and Extortion breaches over time

Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches. The shift of traditional ransomware actors toward these newer techniques resulted in a bit of a decline in Ransomware to 23%. However, when combined, given that they share threat actors, they represent a strong growth to 32% of breaches. Ransomware was a top threat across 92% of industries.

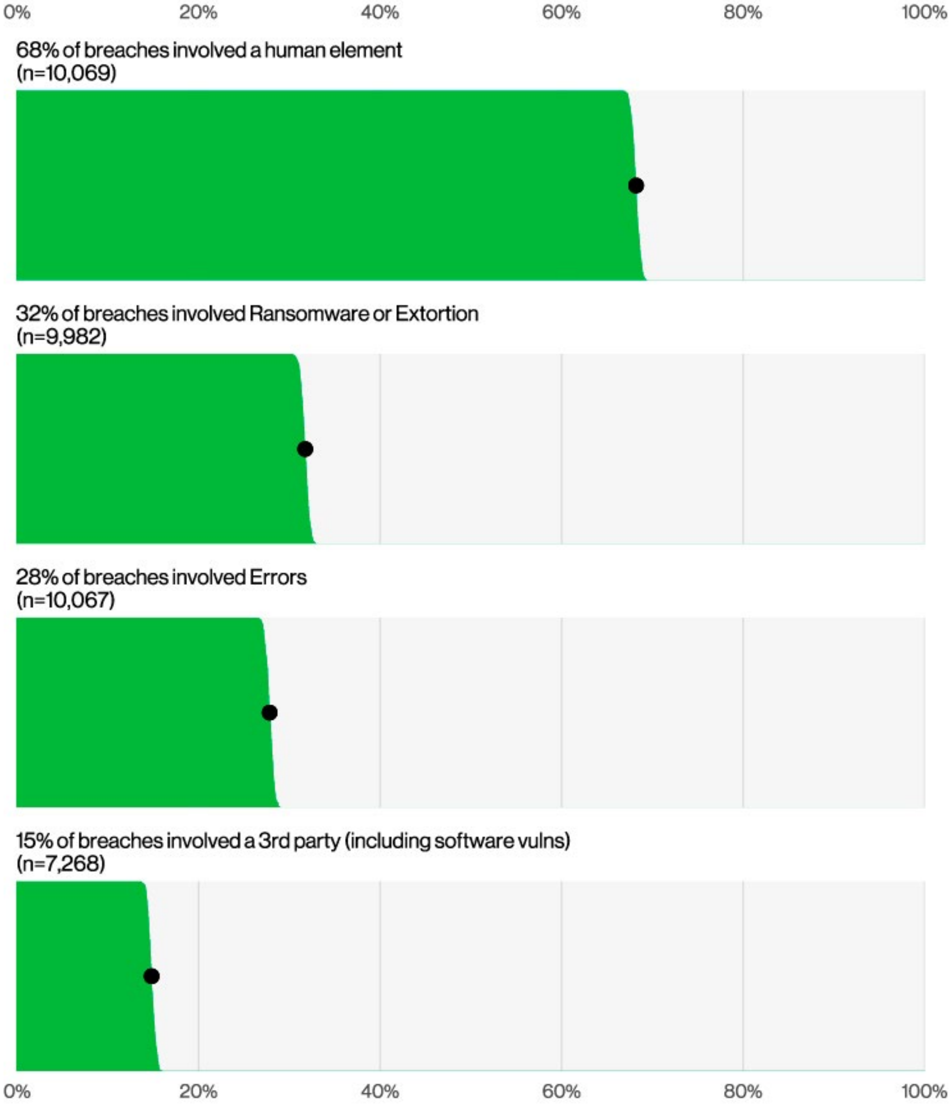

Figure 3. Select key enumerations in breaches

We have revised our calculation of the involvement of the human element to exclude malicious Privilege Misuse in an effort to provide a clearer metric of what security awareness can affect. For this year's dataset, the human element was a component of 68% of breaches, roughly the same as the previous period described in the 2023 DBIR.

In this issue, we are introducing an expanded concept of a breach involving a third party that includes partner infrastructure being affected and direct or indirect software supply chain issues – including when an organization is affected by vulnerabilities in third-party software. In short, those are breaches an organization could potentially mitigate or prevent by trying to select vendors with better security track records. We see this figure at 15% this year, a 68% increase from the previous year, mostly fueled by the use of zero-day exploits for Ransomware and Extortion attacks.

Our dataset saw a growth of breaches involving Errors, now at 28%, as we broadened our contributor base to include several new mandatory breach notification entities. This validates our suspicion that errors are more prevalent than media or traditional incident response-driven bias would lead us to believe.

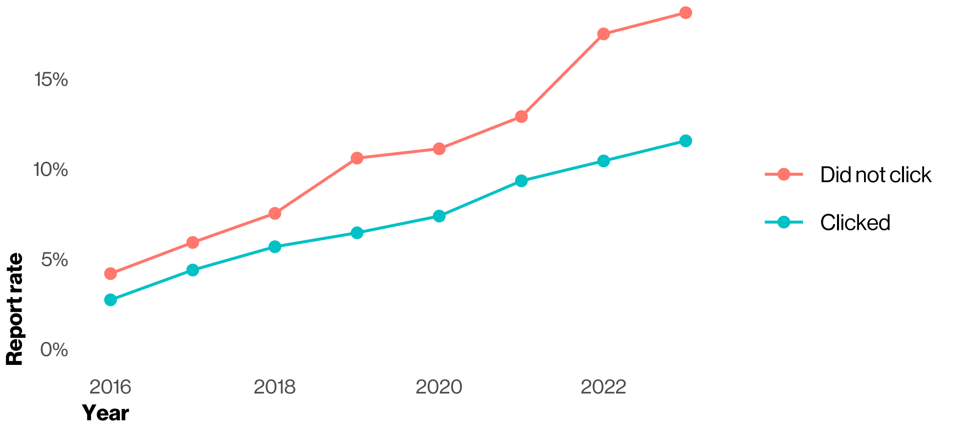

Figure 4. Phishing email report rate by click status

The overall reporting rate of Phishing has been growing over the past few years. In security awareness exercise data contributed by our partners during 2023, 20% of users reported phishing in simulation engagements, and 11% of the users who clicked the email also reported. This is welcome news because on the flip side, the median time to click on a malicious link after the email is opened is 21 seconds and then only another 28 seconds for the person caught in the phishing scheme to enter their data. This leads to an alarming finding: The median time for users to fall for phishing emails is less than 60 seconds.

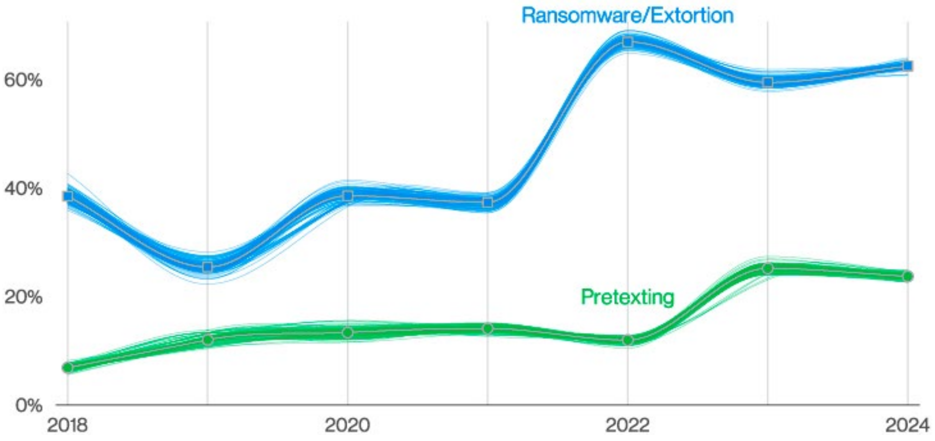

Figure 5. Select action varieties in Financial motive over time

Financially motivated threat actors will typically stick to the attack techniques that will give them the most return on investment.

Over the past three years, the combination of Ransomware and other Extortion breaches accounted for almost two-thirds (fluctuating between 59% and 66%) of those attacks. According to the FBI's Internet Crime Complaint Center (IC3) ransomware complaint data, the median loss associated with the combination of Ransomware and other Extortion breaches has been $46,000, ranging between $3 (three dollars) and $1,141,467 for 95% of the cases. We also found from ransomware negotiation data contributors that the median ratio of initially requested ransom and company revenue is 1.34%, but it fluctuated between 0.13% and 8.30% for 80% of the cases.

Similarly, over the past two years, we have seen incidents involving Pretexting (the majority of which had Business Email Compromise [BEC] as the outcome) accounting for one-fourth (ranging between 24% and 25%) of financially motivated attacks. In both years, the median transaction amount of a BEC was around $50,000, also according to the FBI IC3 dataset.