Top 10 security incidents of 2023

DUBAI , DUBAI, UNITED ARAB EMIRATES, January 3, 2024 /EINPresswire.com/ -- Phil Muncaster, guest writer at ESET says as we draw the curtain on another eventful year in cybersecurity, here are some of the high-profile cyber-incidents that occurred in 2023.

It's been another monumental year in cybersecurity. Threat actors thrived against a backdrop of continued macroeconomic and geopolitical uncertainty, using all the tools and ingenuity at their disposal to make their way past corporate defenses. For consumers, it was another year spent anxiously clicking through on the headlines to see if their personal information had been impacted.

According to Verizon's Data Breach Investigations Report (DBIR), external actors are responsible for the vast majority (83%) of breaches, and financial gain accounts for almost all (95%) breaches. That's why most of the incidents featured in this list will be down to ransomware or data theft extortionists. But that's not always the case. Occasionally the cause can be human error, or a malicious insider. And sometimes the attacks have an outsized impact, even if the number of victims is relatively small.

So in no particular order, here's our pick of the 10 biggest attacks of 2023.

1. MOVEit

Traced back to the Lace Tempest (Storm0950) Clop ransomware affiliate, this attack had all the hallmarks of the group's previous campaigns against Accellion FTA (2020) and GoAnywhere MFT (2023). The MO is simple: use a zero-day vulnerability in a popular software product to gain access to customer environments, and then exfiltrate as much data as possible to hold to ransom. It's still unclear exactly how much data has been taken and how many victims there are. But some estimates suggest more than 2,600 organizations and in excess of 83 million individuals. The fact that many of these organizations were themselves suppliers or service providers to others has only added to the downstream impact. Progress Software, the company behind MOVEit, published details about the critical security loophole and released a patch for it

on May 31st, 2023, urging customers to deploy it immediately or take mitigation steps outlined in the company's advisory.

2. The UK Electoral Commission
The UK's independent regulator for party and election finance revealed in August that threat actors had stolen personal information on an estimated 40 million voters on the electoral register. It claimed a "complex" cyberattack was responsible but reports have since suggested its security posture was poor – the organization having failed a Cyber Essentials baseline security audit. An unpatched Microsoft Exchange server may have been to blame, although why it took the commission 10 months to notify the public is unclear. It also claimed threat actors may have been probing its network since August 2021.

3. The Police Service of Northern Ireland (PSNI)
This is an incident that falls into the category of both insider breach and one with a relatively small number of victims who may suffer an outsized impact. The PSNI announced in August that an employee accidentally posted sensitive internal data to the WhatDoTheyKnow website in response to a Freedom of Information (FOI) request. The information included the names, rank and department of about 10,000 officers and civilian staff, including those working in surveillance and intelligence. Although it was only available for two hours before being taken down, that was enough time for the information to circulate among Irish republican dissidents, who further disseminated it. Two men were released on bail after being arrested on terrorist offenses.

4. DarkBeam
The biggest data breach of the year saw 3.8 billion records exposed by digital risk platform DarkBeam after it misconfigured an Elasticsearch and Kibana data visualization interface. A security researcher noticed the privacy snafu and notified the firm, which corrected the issue quickly. However, it's unclear how long the data had been exposed for or if anyone had accessed it previously with nefarious intent. Ironically, the data haul contained emails and passwords from both previously reported and unreported data breaches. It's another example of the need to closely and continuously monitor systems for misconfiguration.

5. Indian Council of Medical Research (ICMR)
Another mega-breach, this time one of India's biggest, was revealed in October, after a threat actor put up for sale personal information on 815 million residents. It appears that the data was exfiltrated from the ICMR's COVID-testing database, and included name, age, gender, address, passport number and Aadhaar (government ID number). That's particularly damaging as it could give cybercriminals all they need to attempt a range of identity fraud attacks. Aadhaar can be used in India as digital ID and for bill payments and KYC checks.

6. 23andMe
A threat actor claimed to have stolen as many as 20 million pieces of data from the US-based genetics and research company. It appears that they first used classic credential stuffing

techniques to access user accounts – basically using previously breached credentials that these users had recycled on 23andMe. For those users who had opted into the DNA Relatives service on the site, the threat actor was then able to access and scrape many more data points from potential relatives. Among the information listed in the data dump was profile photo, gender, birth year, location, and genetic ancestry results.

7. Rapid Reset DDoS attacks
Another unusual case, this one involves a zero-day vulnerability in the HTTP/2 protocol disclosed in October which enabled threat actors to launch some of the biggest DDoS attacks ever seen. Google said these reached a peak of 398 million requests per second (rps), versus a previous largest rate of 46 million rps. The good news is that internet giants like Google and Cloudflare have patched the bug, but firms that manage their own internet presence were urged to follow suit immediately.

8. T-Mobile
The US telco has suffered many security breaches over recent years, but the one it revealed in January is one of its biggest to date. It impacted 37 million customers, with customer addresses, phone numbers and dates of birth stolen by a threat actor. A second incident disclosed in April impacted just 800-odd customers but included many more data points, including T-Mobile account PINs, social security numbers, government ID details, dates of birth, and internal codes that the firm uses to service customer accounts.

9. MGM International/Cesars
Two of the biggest names in Las Vegas were hit within days of each other by the same ALPHV/BlackCat ransomware affiliate known as Scattered Spider. In the case of MGM they managed to gain network access simply via some LinkedIn research and then a vishing attack to the individual in which they impersonated the IT department and asked for their credentials. Yet the compromise took a major financial toll on the firm. It was forced to shut down major IT systems which disrupted slot machines, restaurant management systems and even room key cards for days. The firm estimated a $100m cost. The cost to Cesars is unclear, although the firm admitted paying its extorters $15m.

10. The Pentagon Leaks
The final incident is a cautionary tale for the US military and any large organization worried about malicious insiders. A 21-year-old member of the intelligence wing of the Massachusetts Air National Guard, Jack Teixeira, leaked highly sensitive military documents to gain bragging rights with his Discord community. These were subsequently shared on other platforms and reposted by Russians tracking the war in Ukraine. They gave Russia a treasure trove of military intelligence for its war in Ukraine and undermined America's relationship with its allies. Incredibly, Teixeira was able to print out and take top secret documents home with him to photograph and subsequently upload.

Let's hope these stories provide some useful lessons learned. Here's to a more secure 2024.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here