2022 in review: 10 of the year's biggest cyberattacks

DUBAI, UNITED ARAB EMIRATES, December 30, 2022 / EINPresswire.com/ -- Phil Muncaster, guest writer at ESET explains that the year has seen no shortage of disruptive cyberattacks – here's a round-up of some of the worst hacks and breaches that have impacted a variety of targets around the world in 2022

The past year has seen the global economy lurch from one crisis to another. As COVID-19 finally began to recede in many regions, what replaced it has been rising energy bills, soaring inflation and a resulting cost-of-living crisis – some of it spurred by Russia's invasion of Ukraine. Ultimately, these developments have opened the door to new opportunities for financially-motivated and state-backed threat actors.

They have targeted governments, hospitals, cryptocurrency firms and many other organisations with impunity. The cost of a data breach now stands at nearly US$4.4 million – and as long as threat actors continue to achieve successes like those below, we can expect it to rise even higher for 2023.

Here are 10 of the worst cyber-incidents of the year, be it for the damage they wrought, level of sophistication or geopolitical fallout. The list is in no particular order, but it makes sense to open it with malicious cyber-operations that took aim at Ukraine and immediately raised concerns about their wider ramifications and associated cyber-risks faced by the wider world.

Ukraine under (cyber)attack: Ukraine's critical infrastructure has found itself, yet again, in the crosshairs of threat actors. Early into Russia's invasion, ESET researchers worked closely with CERT-UA on remediating an attack that targeted the country's grid and involved destructive malware that Sandworm had attempted to deploy against high-voltage electrical substations. The malware – which ESET named Industroyer2 after an infamous piece of malware used by the group to cut power in Ukraine in 2016 – was used in combination with a new version of the

destructive CaddyWiper variant, most likely to hide the group's tracks, slow down incident response and prevent operators of the energy company from regaining control of the ICS consoles.

More wipers. CaddyWiper was far from the only destructive data wiper discovered in Ukraine just before or in the first few weeks of Russia's invasion. On February 23rd, ESET telemetry picked up HermeticWiper on hundreds of machines in several organizations in Ukraine. The following day, a second destructive, data-wiping attack against a Ukrainian governmental network started, this time delivering IsaacWiper.

Internet down. Barely an hour before the invasion, a major cyberattack against commercial satellite internet company Viasat disrupted broadband internet service for thousands of people in Ukraine and even elsewhere in Europe, leaving behind thousands of bricked modems. The attack, which exploited a misconfigured VPN device to gain access to the satellite network's management section, is believed to have been intended to impair the communication capabilities of the Ukrainian command during the first hours of the invasion. Its effects were felt far beyond Ukraine's borders, however.

Conti in Costa Rica: A major player on the cybercrime underground this year was ransomware-as-a-service (RaaS) group Conti. Once of its most audacious raids was against the small South American nation of Costa Rica, where a national emergency was declared after the government branded a crippling attack an act of "cyber terrorism." The group has since disappeared, although its members are likely to simply have moved on to other projects or rebranded wholesale, as RaaS outfits generally due to avoid scrutiny from law enforcers and governments.

Other ransomware actors were also in action in 2022. A CISA alert from September explained that Iran-affiliated threat actors compromised a US municipal government and an aerospace company, among other targets, by exploiting the infamous Log4Shell bug for ransomware campaigns, which isn't all that common for state-backed entities. Also intriguing was a US government compromise in November that was also blamed on Iran. An unnamed Federal Civilian Executive Branch (FCEB) organization was breached and cryptomining malware deployed.

Ronin Network was created by Vietnamese blockchain game developer Sky Mavis to function as an Ethereum sidechain for its Axie Infinity game. In March it emerged that hackers managed to use hijacked private keys to forge withdrawals to the tune of 173,600 Ethereum (US$592 million) and US$25.5 million from the Ronin bridge, in two transactions. The resulting US$618 million theft, at March prices, was the largest ever from a crypto firm. Infamous North Korean group Lazarus has since been linked to the raid. The hermit nation has been traced in the past to thefts worth billions of dollars, used to fund its nuclear and missile programs.

Lapsus$ burst onto the scene during 2022, as an extortion group using high-profile data thefts to force payment from its corporate victims. These have included Microsoft, Samsung, Nvidia,

Ubisoft, Okta and Vodafone. Among its many methods are bribery of insiders at firms and their contractors. Although the group had been relatively silent for a while, it re-emerged at the end of the year after hacking Grand Theft Auto developer Rockstar Games. Several alleged members of the group have been arrested in the UK and Brazil.

International Red Cross (ICRC): In January, the ICRC reported a major breach that compromised the personal details of over 515,000 “highly vulnerable” victims. Stolen from a Swiss contractor, the data included details of individuals separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention. It was subsequently blamed on an unnamed nation state and occurred when an unpatched system was exploited.

Uber: the ride-hailing giant was famously breached back in 2016 when details on 57 million users were stolen. In September it was reported that a hacker, potentially a member of Lapsus$, had compromised email and cloud systems, code repositories, an internal Slack account and HackerOne tickets. The actor targeted an Uber external contractor, most likely grabbing their corporate password from the dark web.

Medibank: All of the Australian health insurance giant’s four million customers has personal data accessed by ransomware actors in an attack which may end up costing the firm US$35 million. Those responsible are believed to be linked to infamous ransomware-as-a-service (RaaS) outfit REvil (aka Sodinokibi) with compromised privileged credentials responsible for initial access. Those impacted now face a potential barrage of follow-on identity fraud attempts.

Whatever happens in 2023, some of the cautionary tales from these 10 major incidents should stand everybody, including CISOs, in good stead. Get your cybersecurity processes and operations right, organize cybersecurity awareness trainings for all employees, and partner with reputable security companies whose solutions can stand up to the complex methods deployed by threat actors.

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