KOVRR

2022 Cyber Roundup

Top 5 most costly data incidents

In recent times it has become clear to organizations that the handling of data is a very important matter, as the exposure or misuse of data are both a serious threat to an organization's financial standing and reputation, and must be accounted for in each organization's risk posture.
In terms of high-profile data breaches, this year has been no different than previous years, seeing its fair share of ransomware attacks and data exposure. In addition, there have also been several large fines handed out by regulators for mishandling of data.

Kovrr Insights
Kovrr's cyber incidents database contains extensive data not only on cyber attacks, but also on various types of data mishandling and exposure, and their impact. Using data from the database, we have summarized below the top 5 most costly data incidents in 2022, so far.

1 Sky Mavis Breach, $625M cryptocurrency theft

On March 23, Sky Mavis, the company developing the popular blockchain based video game Axie Infinity suffered a data breach, following a sophisticated social engineering scheme in which a company engineer was lured into a fake job interview process, ending with him downloading a malicious phishing PDF into the company network. The attackers, named as the North Korean Lazarus Group by the FBI, then breached the company's infrastructure, and were able to steal around $625M worth of cryptocurrency. Following the breach, the company guaranteed to repay all of the stolen funds.

2 Instagram GDPR Violation, €405M fine

In September Instagram was fined €405M by Ireland's Data Protection Commission (DPC), after it was found that the company made the contact information of users aged between 13-17 public, including their email addresses and phone numbers. The investigation, which took two years to complete, handed Instagram the second highest GDPR fine to date. Meta, the parent company of Instagram, will appeal the fine.

KOVRR

3 Wormhole Breach, $325M cryptocurrency theft

On February 2nd the decentralized finance platform, Wormhole, was breached by an attacker which stole the equivalent of around $325M in cryptocurrency. The breach was caused by the attacker successfully exploiting a bug in the project. The bug might have been mistakenly disclosed to the attacker by an update released to the project's Github repository, which included a bug fix which was not yet deployed to the project itself.

4 Nomad Theft, $190M cryptocurrency theft

In August, an accidental vulnerability introduced to the cryptocurrency platform Nomad led to the loss of over $190M from the platform. A bug in the validation process of transactions enabled users, through a simple exploit, to transfer funds from the project to their wallets. This quickly caused a loss of over $190M from Nomad, leading to the balance in the Nomad project to drop from over $190M to around $16K. After the hack, around $36M of the stolen funds were returned to the project.

5 Hanesbrands Ransomware Attack, $100M lost income, $15M response costs - total $115M.

On May 24 Hanesbrands detected a ransomware attack on its system, which led to a serious disruption in the company's global supply chain. At the end of Q2, the company revealed that the ransomware attack disrupted its supply chain for around 3 weeks, causing it to lose $100M in lost sales. In addition, the company paid $15M in response costs, and it is unclear whether the ransom was paid to the unnamed attackers.

There have been many breaches and hacks targeting various types of cryptocurrency platforms, many of them causing very high and potentially catastrophic losses to these platforms.

KOVRR

Top 5 attempted vulnerabilities

Over 22,000 new vulnerabilities have been found this year, with many new exploits appearing as well. While many vulnerabilities are found, not all are actively exploited by attackers, as they might be difficult to exploit, or are exposed in products and services which are not widely used. It is important to understand which vulnerabilities are those most targeted by attackers in order for organizations to prioritize their patching and defense efforts only on the vulnerabilities which cause the highest potential risk to companies.

Kovrr Insights

Based on data analysis from Kovrr's extensive cyber incidents database, below are the top 5 vulnerabilities which attackers have attempted to exploit in 2022. The data is accurate as of mid-November 2022.

1 CVE-2022-26134

This is a remote code execution vulnerability in an Atlassian Confluence Server and Data Center, which allows an unauthenticated attacker to perform remote code execution.

2 CVE-2022-1388

This vulnerability is caused by missing authentication in F5 BIG-IP, which can allow an attacker to successfully exploit the vulnerability's remote code execution, creation or deletion of files, or disabling services.

3 CVE-2022-40684

An authentication bypass vulnerability exists in Fortinet FortiOS, FortiProxy, and FortiSwitchManager. This vulnerability can allow an unauthenticated attacker to perform operations on the administrative interface of these products.

4 CVE-2022-22965

Spring MVC or Spring WebFlux applications running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.

5 CVE-2022-26138

There were hard coded credentials in Atlassian Questions For Confluence App, meaning the username and password for these programs were exposed. A remote unauthenticated attacker can use these credentials to log into Confluence and access all content accessible to users in the confluence-users group.

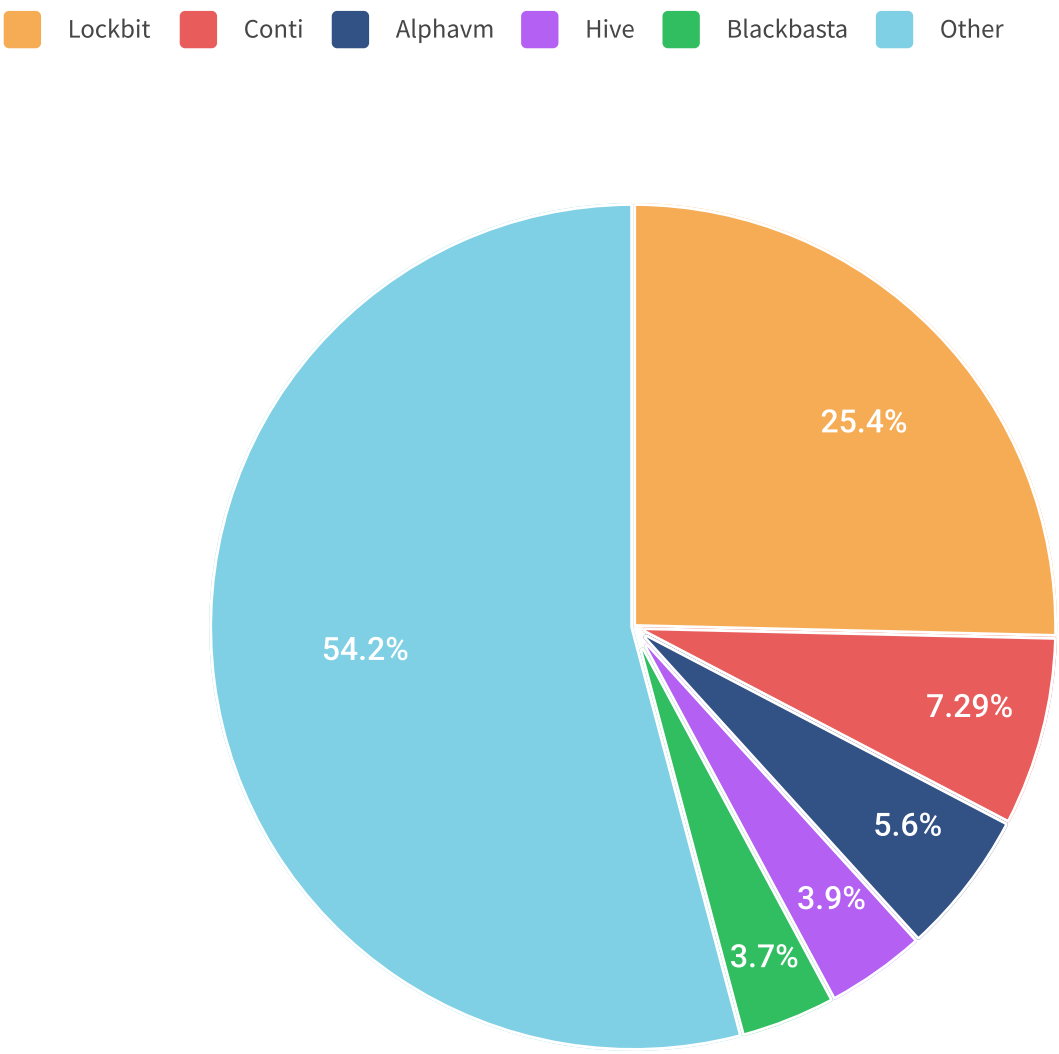
KOVRR

Top 5 active ransomware groups

This year was a turbulent year for ransomware groups. Extremely high profile attacks, such as the Conti attack on the Costa Rica Government, were intertwined with extensive global law enforcement efforts, which led to the arrest of several ransomware group members, including the recent arrest of a suspected Lockbit group operator.[1]

Kovrr Insights

Analysis of cyber incidents and ransomware attacks from Kovrr's cyber incidents database has helped identify the top 5 most active ransomware groups of 2022 (so far). The chart below breaks down the percentage of attacks each group is responsible for, out of the total attacks observed in our incidents database in 2022.



[1] https://www.justice.gov/opa/pr/man-charged-participation-lockbit-global-ransomware-campaign

Main breach trends of 2022

This section will overview the main breach related trends which we have seen in 2022.

Law enforcement activity makes life difficult for ransomware actors

2022 saw an increased level of coordinated global law enforcement activity, aimed at slowing or taking down ransomware groups. This has led to the arrests of several suspected members of ransomware groups, including Lockbit (footnote 1) and Revil.

Kovrr Insights: From our data we can also see a very large drop in ransomware attacks reported in 2022 compared to 2021, with a drop of around 45% in reported attacks. It should be noted that this drop can also be attributed to the war in Ukraine, and not only to the increased operational difficulty caused by law enforcement actions.

Cryptocurrency-targeted hacks have led to very high losses

There have been many breaches and hacks targeting various types of cryptocurrency platforms, many of them causing very high and potentially catastrophic losses to these platforms. Several of these breaches, including Sky Mavis, Wormhole, and Nomad, are mentioned in the top 5 most costly incidents section. As cryptocurrency is adopted and used by more and more companies and products, this trend is expected to continue.

Drop in number of reported data breaches compared to 2021

The number of breaches reported in 2022 is currently lower than in 2021. Breaches are still being reported and the total is increasing, as there is a delay between a breach occurring and it being disclosed. We expect the total number of breaches reported in 2022 to be lower than in 2021, as the rate of reporting is slowing down.

[2] https://www.bbc.com/news/technology-59998925