FLYCAST PARTNERS valencia

☎ 844FLYCAST flycastpartners.com info@flycastpartners.com

Cybersecurity Threat

August 2023 Newsletter

Reflecting on Last Year's IT Security Lessons

Cybersecurity Takeaways

As 2023 unfolds and the threat landscape evolves, IT security experts are reflecting last year's trends. 2022 was a breakout year for ransomware, with Verizon estimating that it amounts to over a quarter of the year's breaches. Last year also saw the rise of supply chain attacks (with attackers focusing on collaborative networks as opposed to single victims), double extortion (whereby attackers pair holding data ransom with its exfiltration to separate locations), and ransomware as a service (RaaS) (meaning that attackers no longer had to develop their own code to encrypt targets' data).

Most Exploited Vulnerabilities

Earlier this month, the cybersecurity agencies of the United States, Australian, Canada, New Zealand, and the United Kingdom have published an advisory on 2022's top exploited vulnerabilities. Listing the top 12 most abused vulnerabilities, the advisory also highlights that older software vulnerabilities were used the most by threat actors, who also showed a preference for unpatched, internet-facing systems in 2022. Threat actors have prioritized exploits for severe and prevalent CVEs; these bring them low cost and high impact techniques that can be used repeatedly.

Focusing On Top Threat Actors

Looking at the biggest culprits provides further insight on the threat landscape. Conti ransomware was prolific, but was overtaken by the LockBit group this year, which made headlines for holding the UK's Royal Mail ransom for 65 million pounds. Conti is rumored to have resurfaced in 2023 under the name of Karakurt. In this way, this ransomware activity can be seen as being carried out for disruption as well as profit.

What Should Organizations Do?

In their advisory, the Five Eyes countries point to areas of focus to prevent breaches. Expectedly, they highlight the importance of applying patches and keeping up with threat actors. What is new is the added focus that organizations should have on third parties, identity and access management, and thorough protective controls and architecture.

Google's Unending Privacy Misadventures

A California law firm has filed a class action lawsuit suing Google for invasion of privacy, larceny, copyright infringement, and profiting from personal data that was illegally obtained. This comes on the heels of Google updating its privacy policies last week to state that public data can be used to train its AI. In its lawsuit, Clarkson law characterizes this as data scraping, whereby the tech giant is stealing user data without consent or compensation. Pools of data scraped by Google include datasets like the Common Crawl, a non-profit, which makes its data free for research and education purposes, and data from sites like Medium and Kickstarter. Google also uses its own data from Gmail and Google Search to feed its models. Other data scraped includes copyrighted works like e-books in digital libraries and even from piracy websites that the company is using without compensating artists and authors.

Hacking Critical Infrastructure

A former contractor at the City of Tracy in California has been charged with hacking a water treatment facility. It is alleged that the contractor installed an app that would allow him remote access that he used to "uninstall software that was the main hub of the facility's computer network and that protected the entire water treatment system, including water pressure, filtration, and chemical levels."

BlackBerry: Surge in Public Sector Attacks

As 2023 gears up to be a profitable year for hackers, BlackBerry's latest quarterly Global Threat Intelligence Report highlights that governmental bodies and public service entities are especially vulnerable. Infostealers live in infected devices and gather information, which can further be leveraged by attackers in other attacks. Malware families used to target healthcare include Emotet, IcedID, and Smokeloader, which are notable for their ability to launch further malicious payloads. The company cites increasing North Korean and Russian backed threat actors as contributing factors, highlighting an average of 1.7 novel malware samples being deployed per minute. This has led to an increase of 40% in cyberattacks targeting public sector agencies between March and May 2023. BlackBerry advises keeping current with threat actor profiles and tactics; prevention will be key to stay out of reach.

MOVEit Dominates Ransomware Disclosures

A few months after its disclosure, the MOVEit breach has recently dominated ransomware public disclosures while the overall number of reported ransomware attacks fell. The total number of MOVEit victims now amounts to 566 organizations and 40 million users worldwide. MOVEit disclosures for municipalities have risen sharply, including cities in California, North Carolina, Utah, and Wisconsin as of now. Issues faced by healthcare groups run the gamut from oversight issues to inadequate knowledge of IT security. The working group hopes to issue actionable recommendations for healthcare providers of all sizes to secure their systems.

Data Breach Cost: Dire Numbers

According to a report from IBM, the rising average cost of data breaches, standing at $4.45 million in 2023, amounts to half the average healthcare data breach cost, which is at about $11 million. Healthcare has the highest data breach cost of all industries with finance being a distant second at $6 million. This is due to healthcare still being an attractive target to hackers; halfway through 2023, 330 breaches befell healthcare organizations affecting 43 million people globally. These numbers are dangerously approaching 2022's peak of 52 million breached patients.

Exploits and Issued Patches

- Ivanti has issued security patches for Endpoint Manager Mobile (EPMM) to address a vulnerability allowing for unauthenticated access to specific API paths. EPMM versions 11.8 through 11.10 as well as older versions were affected by the vulnerability.

  Our Thoughts: We like seeing providers being proactive with patches, especially those with the user base of Ivanti Patch.

- Microsoft Cloud's issues continue with recent developments showing that Storm-0558 exposed more than emails. Millions of Azure AD apps were endangered by earlier APT intrusion. This also includes Microsoft apps such as Teams, SharePoint, and OneDrive.

  Our Thoughts: Like so many other hacks, this will likely turn out to be bigger than we initially thought. Promptly update Azure SDK to its latest version and ensure application caches are updated to make sure you avoid threat actors using compromised keys to breach you.

- Active flaws in PowerShell Gallery could be used by threat actors to conduct supply chain attacks against users in the registry. According to Aqua security, they also open users to typosquatting attacks.

  Our Thoughts: Typosquatting attacks are serious infection vectors. We are disappointed that Microsoft has not secured PowerShell gallery; we advise focusing on training to ensure spoofed packages are not downloaded or used.

- Threat actors have stepped up their phishing operations by hosting phishing pages on Cloudflare R2. Cloudflare R2, a data storage service for the cloud, is being exploited alongside Turnstile, a Clouflare offering that acts as a CAPTCHA replacement to evade detection.

  Our Thoughts: This is concerning, but not unexpected. Phishing campaigns have been growing more sophisticated with time. We recommend providing users with the latest cybersecurity awareness training regarding phishing.

- A critical vulnerability affecting Citrix NetScaler is being actively exploited by threat actors. Its exploit is said to be automatic and involves attackers placing web shells on vulnerable NetScalers to gain persistence, which allows them to execute remote commands even if NetScalers are patched or rebooted.

  Our Thoughts: There have been over 2000 instances being hacked globally through this backdoor. We advise scanning Citrix appliances; Mandiant has released an open-source tool to do so.

- Millions of programmable logic controllers (PLCs) are at risk of exploit for 15 critical vulnerabilities in the CODESYS V3 software development kit. Attackers are taking advantage of PLCs not being upgraded often for security fixes and pairing it with another flaw impacting CODESYS to exploit and evade authentication.

  Our Thoughts: If applicable to your organization, administrators should upgrade PLCS to V3.5.19 as soon as possible. Ideally, PLCs would also be disconnected from the internet.

Threat Actor Updates

- Cofense is reporting that hackers have leveraged QR codes in a phishing campaign targeting an important American energy organization. Hackers have created a convincing spoof of a Microsoft mail with QR codes asking users to verify their accounts.

  Our Thoughts: Campaigns like these remind us that threat actors constantly innovate on older tricks. Train and include image recognition tools as part of protective measures against phishing.

- Microsoft is alerting on a new version of the BlackCat/ALPHV ransomware. It is mobilizing tools such as RemCom and Impacket to facilitate lateral movement and get to remote code execution ultimately.

  Our Thoughts: Ransomware mutates fast - IBM alerted on a new version of BlackCat only two months ago! Train users, patch your apps, and deploy scanning and monitoring contingencies.