cybervergent

ANNUAL REPORT 2023

The Great Data Heists

A Recap of 2023's Cybersecurity Breaches

JAN In January 2023, T-Mobile found itself in the crosshairs of a security breach where unauthorized parties accessed personal data like names, emails, and birthdays of 37 million customers. The aftermath was severe, with T-Mobile facing substantial financial losses amounting to hundreds of millions of dollars. This breach also tarnished their reputation, eroding trust due to multiple incidents involving customers' private information.

FEB February witnessed Moscow-based Elevel grappling with a massive data breach exposing 1.1TB of personal information, including customer names, phone numbers, email addresses, and delivery details. Particularly concerning was the exposure of usernames and passwords, potentially granting threat actors access to more sensitive data for fraudulent activities.

MAR March saw TechNet, one of the globe's largest technology conglomerates, succumbing to a breach that affected 250 million users. This highlighted the urgent need for robust security measures to shield sensitive user data, as the breach exploited vulnerabilities in TechNet's customer database.

In a startling revelation, OpenAI's ChatGPT account credentials surfaced on illicit dark web platforms. India took the hardest hit, with 12,632 stolen credentials linked to the country. The breach impacted several other nations, including Pakistan, Brazil, Vietnam, Egypt, the U.S., France, Morocco, Indonesia, and Bangladesh, totaling 100,000 stolen credentials. This underscored the urgent requirement for strengthened security measures in an increasingly AI-dependent world, emphasizing the need for users to follow stringent password safety practices like fortifying accounts with two-factor authentication (2FA) against account takeover attacks.

APR April witnessed the most significant breach at Shields Health Care Group, affecting 2.3 million individuals. The cybercriminals had access to sensitive information for two weeks, including patients' Social Security numbers, medical histories, and financial details. Shields Health Care Group initiated reconstruction of specific systems and continuously reviewed and enhanced safeguards to uphold data protection.

MAY May revealed a breach exposing personal information of 237,000 federal government workers associated with the United States Department of Transportation (USDOT). Following the hack, USDOT launched an investigation and temporarily halted access to the transit benefit system, reinstating it only after ensuring enhanced security.

JUN June marked the MOVEit breach as the largest of 2023, affecting 60,144,069 individuals and costing nearly $10 billion. The U.S. State Department announced a $10 million bounty for information related to the Clop ransomware group responsible for compromising records. U.S.-based organizations formed the majority of victims, highlighting vulnerabilities across various sectors.

JUL In July, the Roblox data breach exposed sensitive information of 3943 Roblox creators, raising concerns about data security. Roblox Corporation confirmed the breach, initiated an investigation, and offered support to those affected while urging users to bolster security measures.

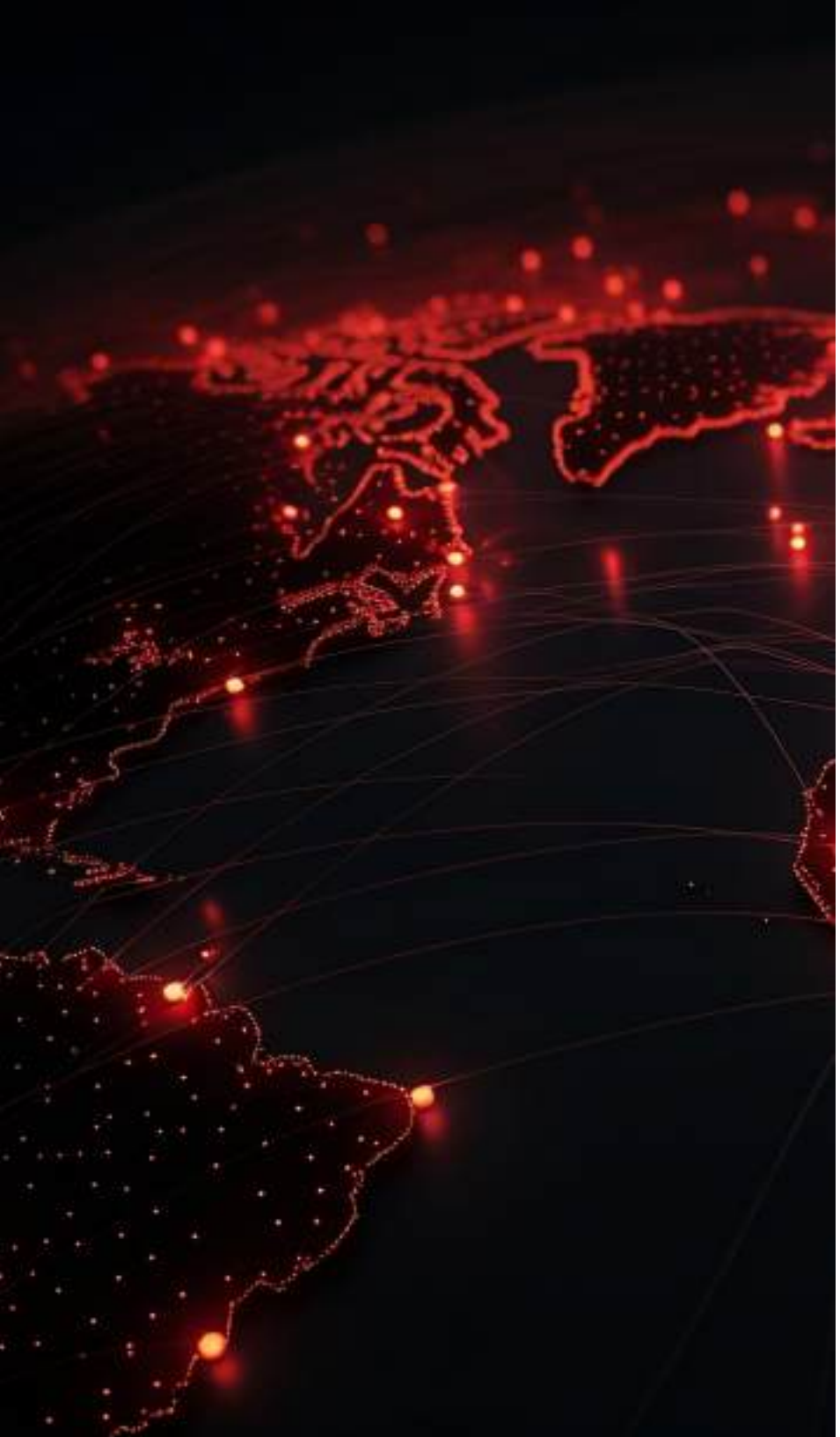
AUG August witnessed Discord.io's data breach affecting 760,000 users due to a vulnerability exploited by a hacker known as 'Akhirah.' Discord.io ceased operations, investigated the incident, and disclosed the flaw in their website's code that led to the breach.

SEP In September, travel giant Sabre fell victim to a data breach affecting ticket sales, passenger records, employee information, and financial data. Meanwhile, the humanitarian organization Save The Children experienced a ransomware attack compromising international HR files, personal information, and financial records.

OCT The Indian Council of Medical Research (ICMR) faced the highest data breach in October, involving sensitive data from Indian residents, including names, ages, addresses, passport numbers, and Aadhaar numbers, affecting 815 million individuals.

NOV In a flurry of November data breaches, TmaxSoft, a South Korean IT powerhouse, took the lead with an inadvertent exposure of a staggering 2 terabytes of data via an online Kibana dashboard. This massive spillage included a treasure trove of company information, emails, and sensitive particulars like employee names, phone numbers, employment contract details, and even email attachments. The breach sent shockwaves through the digital realm, impacting a whopping 56 million records.

Following closely on the heels of this breach, McLaren Health Care found itself embroiled in the second most significant breach of November. The breach at McLaren delved deep, compromising names, dates of birth, and Social Security numbers. But it didn't stop there. This cyber incursion reached into the core of medical details, laying bare billing particulars, claims data, diagnosis information, prescription specifics, and even diagnostic results and treatments. The breach, affecting 2.2 million patients, cast a cloud over McLaren, resulting in several class-action lawsuits in the wake of the data security debacle.



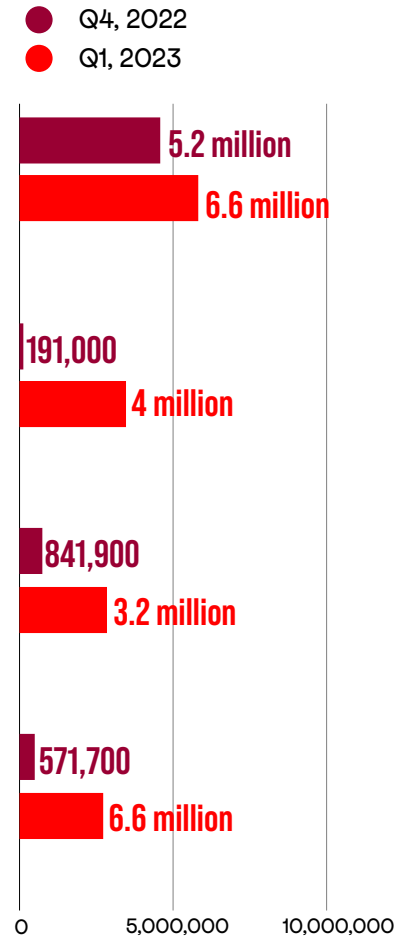
Top Breaches in Q1 2023

Russia: The data breaches surged by 27.4%, with 6.6 million accounts breached in Q1 2023 compared to 5.2 million in Q4 2022.

Taiwan: There was a 95% increase with 4 million breached accounts in Q1 2023 compared to 191,000 breached accounts in Q4 2022.

France: There was a 74% increase with 3.2 million breached accounts in Q1 2023 compared to 841,900 breached accounts in Q4 2022.

Spain: There was an 82% increase with 3.1 million breached accounts in Q1 2023 compared to 571,700 breached accounts in Q4 2022.



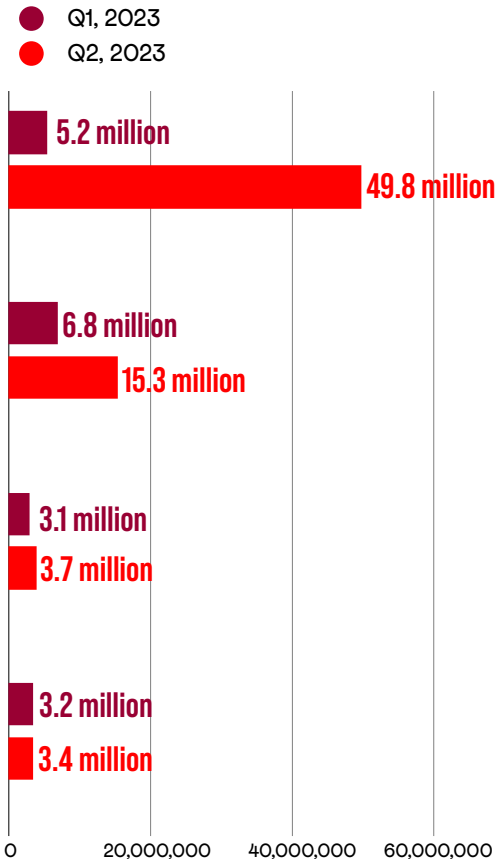
Top Breaches in Q2 2023

US: There was an 830% increase with 49.8 million breached accounts in Q2 2023 compared to 5.4 million breached accounts in Q1 2023.

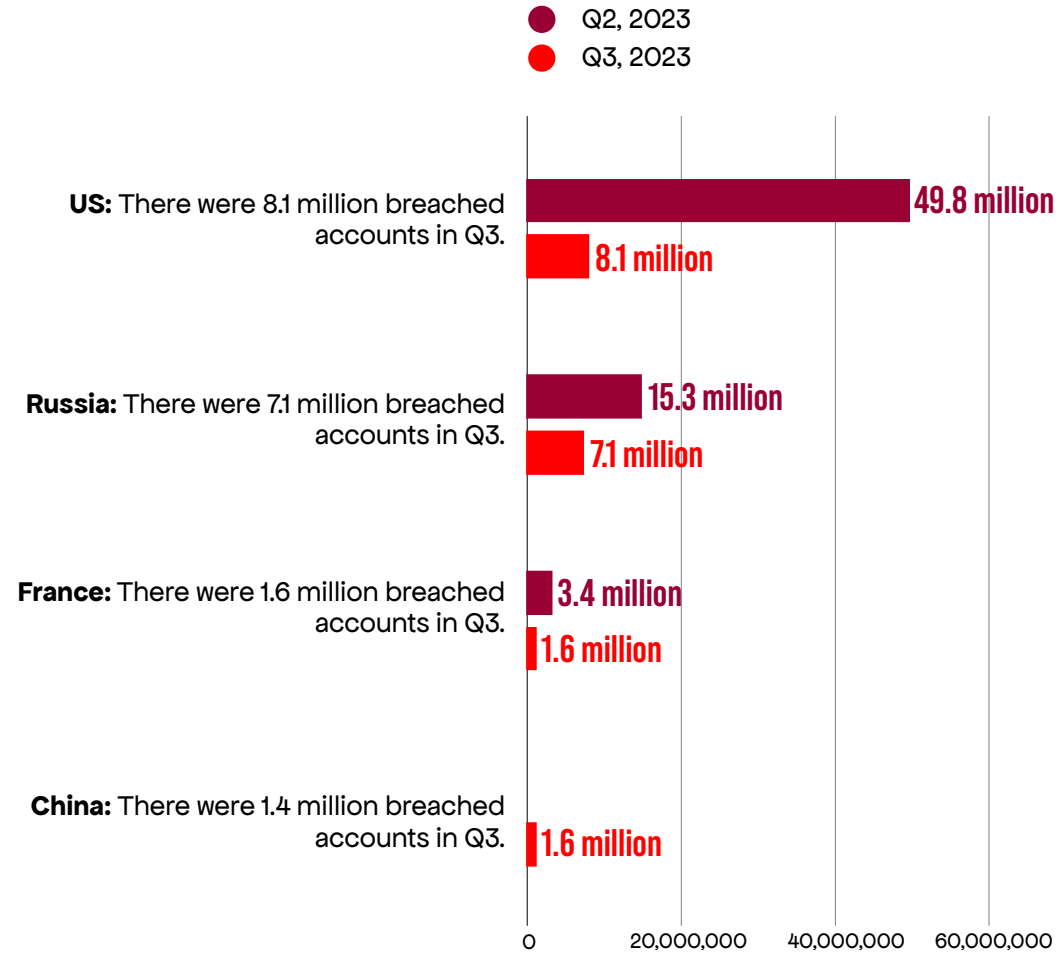
Russia: There was a 55% increase with 15.3million breached accounts in Q2 2023 compared to 6.8million breached accounts in Q1 2023.

Spain: There was a 19% increase with 3.7million breached accounts in Q2 2023 compared to 3.1 million breached accounts in Q1 2023.

France: There was a 6% increase with 3.4million breached accounts in Q2 2023 compared to 3.2 million breached accounts in Q1 2023.



Top Breaches in Q3 2023



Data Breaches in Nigeria

Data breaches have become increasingly common in Nigeria, with several high-profile incidents reported in 2023. These breaches have exposed sensitive personal information of millions of Nigerians, raising concerns about data security and privacy.

One of the most significant data breaches in Nigeria in 2023 was the attack on the National Identity Management Commission (NIMC). In March 2023, hackers gained unauthorized access to the NIMC database, compromising the personal information of over 140 million Nigerians. The exposed data included names, addresses, phone numbers, email addresses, and National Identification Numbers (NINs).

Another major data breach occurred at the Independent National Electoral Commission (INEC) in February 2023. Hackers infiltrated the INEC database and stole the personal information of over 84 million registered voters. This breach raised concerns about the security of the upcoming general elections in Nigeria, scheduled for February 25, 2023.

In addition to these large-scale breaches, there have been numerous reports of data breaches at banks, telecommunications companies, and other private organizations in Nigeria. These breaches have exposed the personal information of millions of Nigerians, including financial details, medical records, and other sensitive data.

The Nigerian government has taken some steps to address the issue of data breaches, including the enactment of the Nigeria Data Protection Regulation (NDPR) in 2019. However, more needs to be done to enforce the NDPR and hold organizations accountable for data breaches.

To protect yourself from data breaches, it is important to take steps to secure your personal information. This includes using strong passwords, being cautious about clicking on links in emails or text messages, and regularly monitoring your credit report for any suspicious activity

Top Application Vulnerabilities For 2023

As we look back on the year 2023, it is imperative to recognize the dynamic nature of cybersecurity threats and to avoid underestimating vulnerabilities present in day-to-day work environments. This report provides an analysis of critical vulnerabilities identified during investigations conducted in our clients' environments throughout the year.

Outlined below are the key findings and insights derived from our threat intelligence team's thorough assessment of vulnerabilities observed in 2023.

1. Zabbix agent

In a bustling city, there was a massive building that held the secrets to keep everything running smoothly. This building wasn't just any ordinary place; it was the heart of the city's infrastructure. It watched over the networks, servers, and cloud services that made the city tick.

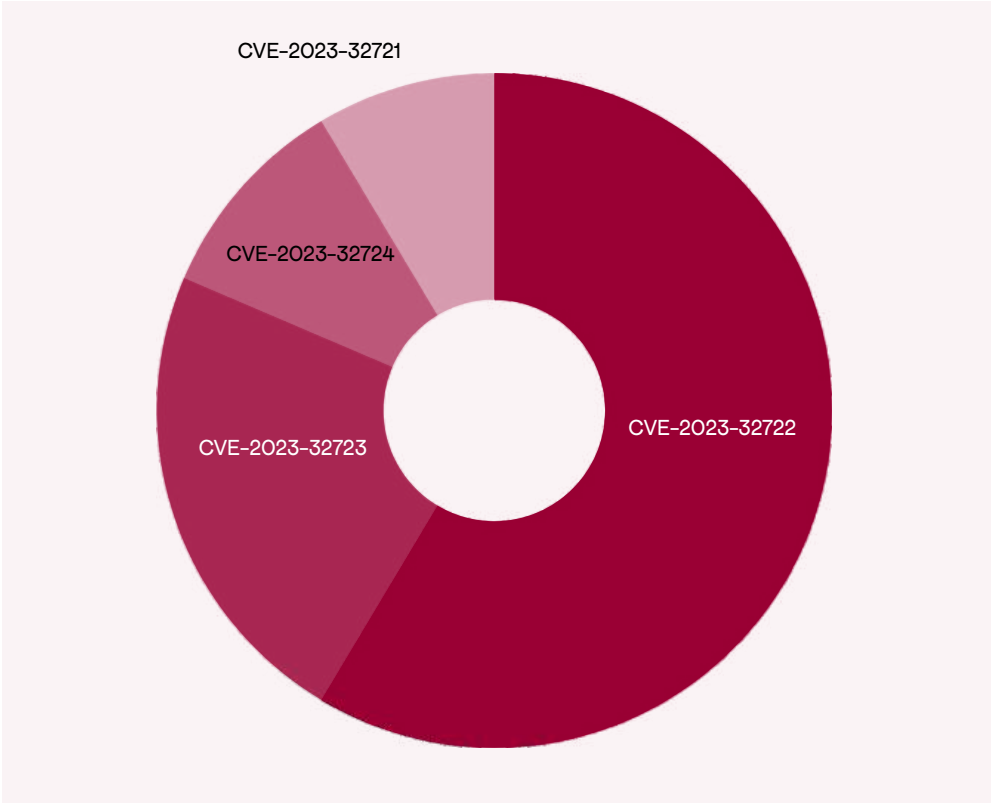
Now, in this building, there was a special tool called Zabbix. Think of it like the eyes and ears of the entire system. Zabbix had a crucial job – it monitored and kept track of how everything was doing. It collected important information, sort of like how a superhero might gather clues to keep the city safe.

But one day, trouble brewed within this superhero tool. Some sneaky villains found holes, like secret passages (vulnerabilities), within Zabbix. These gaps weren't good news; they were serious business. They could let the villains do something really scary – like sneaking their own secret codes into the system!

These gaps weren't just in one part of Zabbix; they were in the server, the agent software (think of them as key players), even in the API, proxy, and the web frontend (the city's communication system). If these gaps fell into the wrong hands, it would be like giving the villains the keys to the city.

In the worst-case scenario, these holes (vulnerabilities)could let the villains not just peek into the system, but control parts of it. It was like giving them the power to run wild in the city without anyone noticing.

Here are the vulnerabilities (In their CVE's) found in Zabbix agent below:



Vulnerabilities:

- **CVE-2023-32722:** The zabbix/src/libs/zbxjson module is vulnerable to a buffer overflow when parsing JSON files.
- **CVE-2023-32724:** Memory pointer is in a property of the Ducktape object
- **CVE-2023-29453:** Templates do not properly consider backticks (`) as Javascript string delimiters, and do not escape them as expected.
- **CVE-2023-32723:** Request to LDAP is sent before user permissions are checked.
- **CVE-2023-32721:** A stored XSS has been found in the Zabbix web application in the Maps element if a URL field is set with spaces before URL

2. Redis:

In a town, there lived a community of shopkeepers, each with their own store filled with treasures. Now, to keep their shops running smoothly, they had a magical helper named Redis.

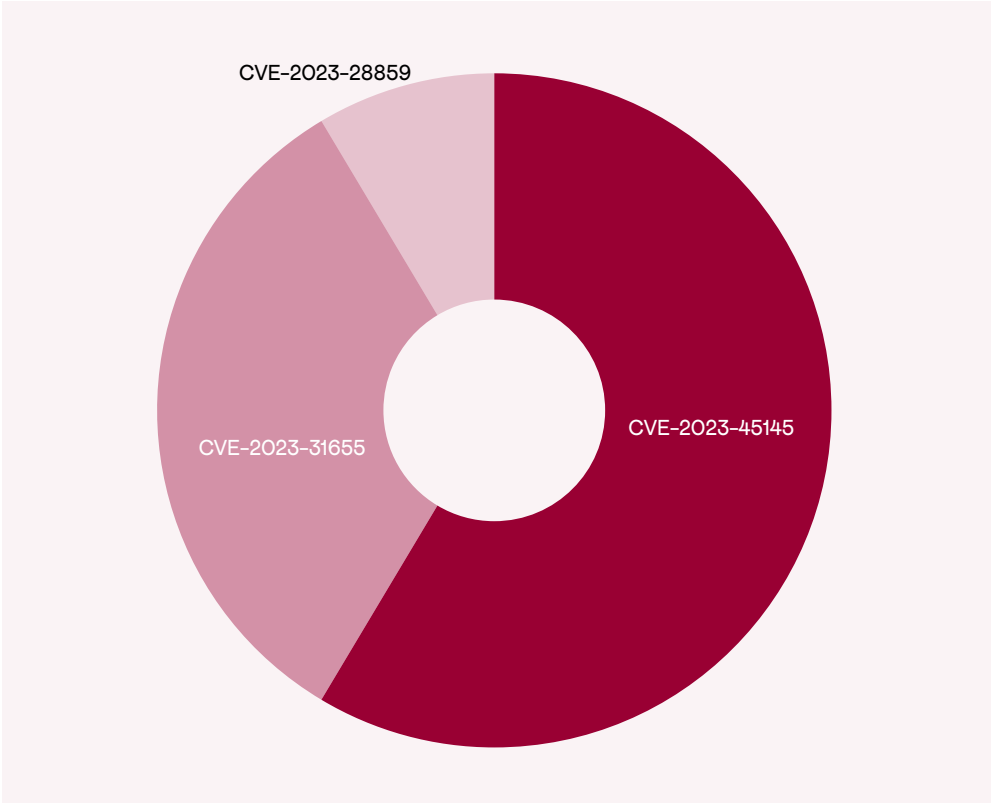
Redis was like a super-fast memory bank, keeping track of all the keys to their treasures and helping the shopkeepers store their valuable items in a special way. Think of it as a magical storage chest that instantly knows where everything is placed.

This magical helper didn't just store items; it also had another special power – it could turn into a messenger! Whenever a shopkeeper needed to send a message to another shop, Redis could quickly carry it between them. It was like having a fleet-footed messenger darting through the town at lightning speed.

But Redis isn't just a messenger; it is also a guardian. It made sure that the shopkeepers' treasures were safe, protecting them from being lost or stolen. One day, the shopkeepers discovered something amazing about Redis – it didn't justremember things quickly, it also had a trick up its sleeve called "optional durability." This meant that even if there was a commotion in the town or something unexpected happened, Redis could make sure nothing was lost. It was like having a magical shield that kept everything secure.

However, there was a challenge. Some tricky rascals tried to find ways to sneak into Redis and cause trouble. They wanted to disrupt the peace of the town by playing with the treasures or delivering fake messages.

Vulnerabilities (In their CVE's) found in Redis below



Vulnerabilities:

- **CVE-2023-45145:** Redis is an in-memory database that persists on disk. This is an in-memory database that persists on disk.
- **CVE-2023-28859:** redis-py before 4.4.4 and 4.5.x before 4.5.4 leaves a connection open after canceling an async Redis command at an inopportune time and can send response data to the client of an unrelated request.
- **CVE-2023-31655:** redis-7.0.10 was discovered to contain a segmentation violation.

3. libcurl:

Imagine a mystical world, where a magical bridge called libcurl connects diverse lands and unlocks endless possibilities. This extraordinary structure isn't just an ordinary walkway; it's a gateway for sharing messages, treasures, and captivating stories.

Imagine libcurl as a grand, versatile bridge that transcends conventional boundaries. It weaves intricate pathways for letters, treasures, music, and so much more. This enchanting bridge possesses the power to handle any item you wish to send or receive.

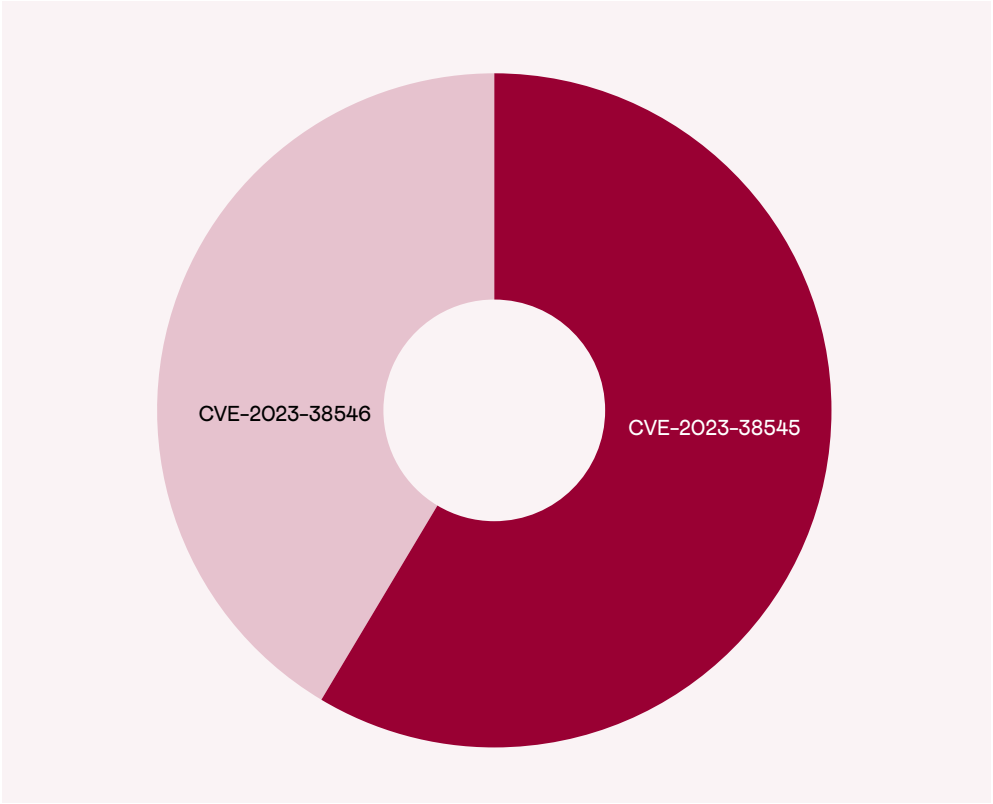
With libcurl, you can entrust your letters to the mystical SMTP post office path, ensuring their safe delivery. Share treasures far and wide using the specialized routes of SCP or FTP. And if security is your utmost concern, fear not! libcurl boasts secret tunnels like HTTPS and SFTP, safeguarding your valuable cargo throughout its journey.

But libcurl isn't just about transportation; it's about understanding the unique needs of each traveler. It accommodates those who communicate in mysterious languages like Kerberos and offers secret codes for unlocking treasure chests through user-plus-password authentication. Whatever your desires may be, libcurl has a solution tailored just for you.

This extraordinary bridge even harbors a library of paths for thrilling adventures. Climb mountains with FTP uploading, explore hidden caves through HTTP proxy tunneling, or embark on daring sea voyages via SMTP. libcurl holds the key to all these exhilarating escapades.

Yet, as with any grand structure, mischievous characters seek to disrupt the harmony. They aim to exploit libcurl's versatility for their own nefarious deed. 7088543428

Vulnerabilities (In their CVE's) found in libcurl below



Vulnerabilities:

- **CVE-2023-38545:** SOCKS5 heap buffer overflow vulnerability, a high severity flaw that affects both the libcurl library and the curl tool
- **CVE-2023-38546:** a cookie injection flaw, a low severity bug that only affects libcurl.

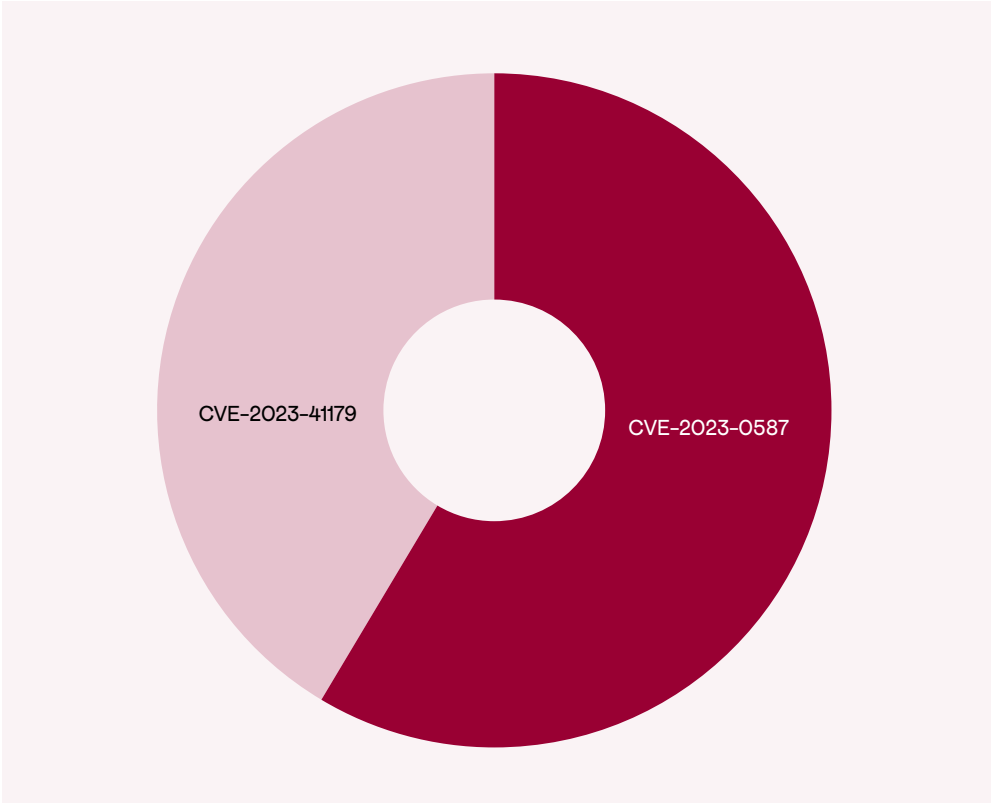
4. Apex one security:

In a city, a group of brave defenders known as the Guardians of Safety protects the citizens from unseen digital dangers. At the core of their defense lies a remarkable tool called Trend Micro Apex One. Think of it as a powerful shield surrounding every home and building, warding off sneaky threats that try to slip through the city's gates.

This shield comprises two essential parts. The Security Agent is a vigilant guardian residing inside each home and building, keeping watch to prevent any harmful intrusions. The other part, the Apex One server, acts as the commander-in-chief, managing and guiding all Security Agents in perfect harmony to defend against any approaching threats. Together, they form an unstoppable team, much like the Guardians of Safety themselves. Their mission is simple yet vital: safeguard the people and their homes from lurking digital dangers.

Just as the city gates have guards to protect against intruders, Trend Micro Apex One shields against internet troublemakers. It's an invisible force field repelling sneaky threats, ensuring the safety of the citizens as they go about their daily lives.But amidst the peace, threat actors attempt to breach the defenses, aiming to disrupt the harmony established by the Guardians of Safety.

Vulnerabilities (In their CVE's) found in Apex one security below



Vulnerabilities:

- **CVE-2023-0587:**
  A file upload vulnerability exists in Trend Micro Apex One server build.

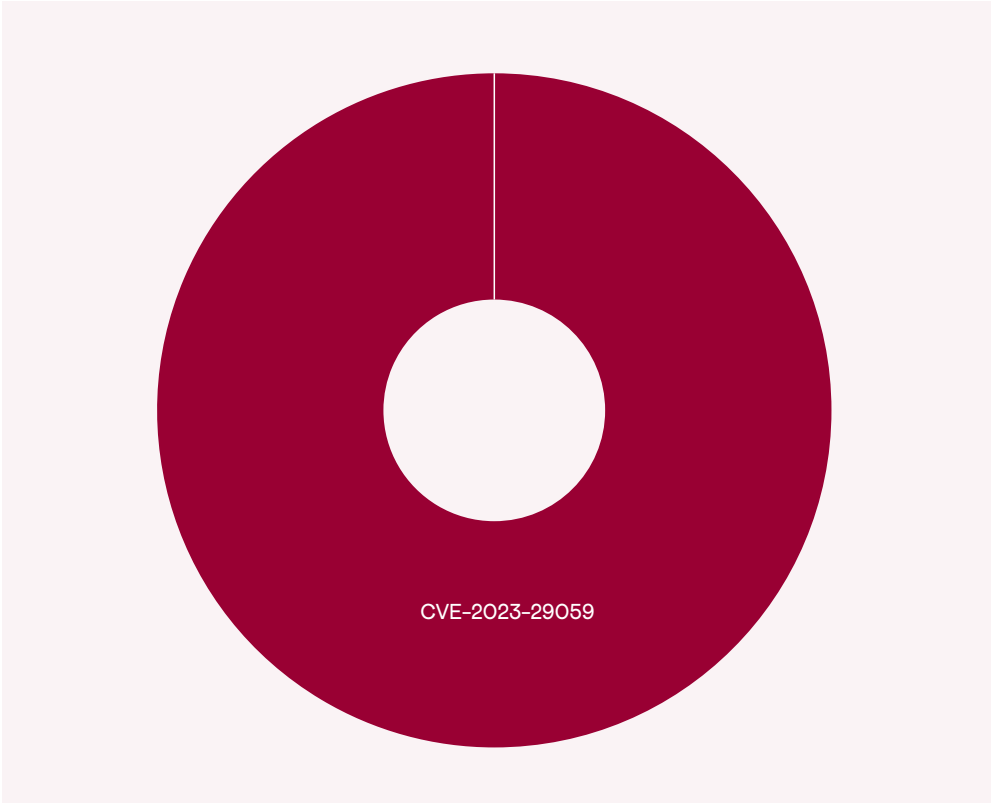
- **CVE-2023-41179:**
  A critical vulnerability in the third-party AV uninstaller module in Trend Micro Apex One, Worry-Free Business Security, and Worry-Free Business Security Services allows attackers to execute arbitrary commands on affected installations. Access to the administrative console on the target system is required for exploitation.

5. 3CX:

Imagine you built a fortress for your business communication, walls of code, towers of features. 3CX Phone System, your all-in-one hero, promised crystal-clear calls, video conferences that felt like teleportation, and chats that danced across Facebook and WhatsApp. Your team rejoiced, freed from the circus of scattered apps. But like any fortress, even the most magnificent can have hidden cracks. Security researchers, ever vigilant, discovered vulnerabilities in 3CX's code. Think of it like a tiny chink in the wall, invisible to most, but big enough for a sneaky thief to slip through.

These vulnerabilities, like tiny trapdoors, could potentially allow someone to eavesdrop on calls, listen in on meetings, and even hijack chatbots. Imagine, your confidential conversations floating out like whispered secrets, your team's brainstorming sessions laid bare to prying ears. Now, the good news is, 3CX is on the case. They're patching those cracks, sealing the trapdoors, and making sure your communication fortress stays strong. But it's a reminder that even in the most secure systems, vigilance is key.

Vulnerability (In the CVE) found in 3CX below



Vulnerability:

- **CVE-2023-29059:**
  3CX Desktop through 18.12.416 has embedded malicious code, as exploited in the wild in March 2023

Addressing The Spectrum of Cybersecurity

Exploring Positive

Nigeria emerges as the second most cyber-secure African country for business in 2023, as reported by leading application security company Indusface. Amidst the growing prevalence of remote and hybrid working models, the importance of cybersecurity awareness has surged, with recent research indicating that 68% of high-revenue growth companies worldwide have adopted a hybrid approach.

A comprehensive analysis, encompassing factors such as DDOS attacks, phishing sites, malware hosting sites, and compromised computers, positions Nigeria as a standout performer with an index score of 74.68 and the lowest number of compromised computers per 100,000 internet users among all African countries reviewed.

The Negative

On August 2nd, Anonymous Sudan, a hacktivist collective with pro-Russian leanings, issued a cautionary message to the Nigerian populace via its Telegram channel. Making a bold move, the group asserted its responsibility for a midday cyberattack on of the largest telecommunications company in the country. While never formally acknowledging the incident, the National Information Technology Development Agency (NITDA) confirmed the assault on its digital infrastructure through an official press release.

In response to this heightened threat, NITDA urged vigilance among Nigerian financial service providers, government entities, and telecommunications firms, advising them to fortify their defenses in anticipation of a potential series of cyber-attacks. The hacker group, citing Nigeria's proposed military intervention in Niger as a catalyst, boldly proclaimed this assault as the inaugural strike in a planned sequence.

Challenging Aspect

In the first eight months of this year, three Nigerian FinTech's encountered significant losses, surpassing N5 billion due to escalating cases of hacks and fraud within the industry. Concurrently, undisclosed incidents involving staggering amounts in the billions underscore the escalating complexity, with indications that some heists involved the complicity of fintech staff. This internal challenge has emerged as a major obstacle for Nigerian fintech companies. Furthermore, the interconnectivity of fintech platforms raises concerns, as a well-secured platform could be compromised through a connected platform with inadequate cybersecurity systems. A recent incident led a commercial bank to temporarily sever connections with multiple FinTech's, impeding financial transactions with affected entities, though the issue was eventually resolved.

There was a distressing incident where a fintech company lost N800 million to hackers in a single week, with suspicions of insider collaboration. Additionally, another case involving another top fintech unveiled a combination of hacker and insider involvement. Meanwhile, a tier payment platform encountered a N2.9 billion hack, initially denying any fund loss but later seeking police assistance to recover funds and freezing accounts linked to illegal transfers. This wave of cyber threats extends beyond fintechs, as commercial banks in Nigeria faced a 1,125.03% increase in fraud-related losses, totaling N5.79 billion in Q2 2023, with insider involvement emphasizing the need for heightened vigilance in staff recruitment and outsourcing.

Effective Governance

A Ticking Box or a Fortress? Rethinking PCI DSS in the Age of Advanced Threats

In the domain of Finance and FinTech, a widely recognized standard is the Payment Card Industry Data Security Standard (PCI DSS), established by the Payment Card Industry Security Standards Council (PCI SSC). This standard is designed to protect the handling of payment card data—such as PINs, expiration dates, CVVs, and PANs—by organizations involved in its storage, transmission, or processing. Compliance with PCI DSS is imperative for various entities, including banks, payment gateways, merchants, and service providers, as it is a non-negotiable requirement for organizations entrusted with payment card information.

From Humble Beginnings to Cutting-Edge Security:

The first version (1.0) of PCI DSS, released in 2004, emerged amidst a rapidly evolving technological landscape. Back then, the five major card brands – Mastercard, Visa, American Express, JCB International, and Discover Financial Services – recognized the need for a unified approach to data security. Fast forward to March 2022, and we have version 4.0, a testament to the standard's continuous adaptation.

This latest update reflects the rise of technologies such as cloud computing, AI, virtualization, quantum computing, and advanced threat detection technologies. PCIDSS equips organizations with specific guidelines to navigate these advancements while addressing the growing sophistication of cyberattacks, for example, the use of AI and Quantum computing for brute-force attack, breaking cryptography, stealing cryptographic keys, and circumventing biometrics security systems. These factors birthed the need to improve certain controls in the standard, such as increment in password length to 12 characters, the use of MFA for non-console admin access, e-commerce anti-phishing requirements, and others.

Beyond the Checkbox: Embracing a Security Culture:

The days of treating PCI DSS as a mere box-ticking exercise are over. The latest version of PCIDSS urges organizations to move beyond compliance certifications and build a genuine security culture. This means integrating robust security processes into the very fabric of everyday operations, rather than viewing it as a sprint towards the next audit. The latest version of PCI DSS has added some requirements to help organizations integrate their PCI DSS program into business-as-usual, some of the requirements include Establishing and updating policies and procedures, assigning responsibilities for requirements, performing risk analysis to determine frequency of activities, and the use of customized approach to meet the requirements of the standard.

Challenges on the Path to Compliance:

Implementing PCI DSS isn't without its hurdles. The standard's technical complexity, potential cost implications, lengthy implementation process, and the integration of security into daily routines can all present challenges. The technical intricacies of the 12 requirements with their numerous security controls can overwhelm those unfamiliar with information and cybersecurity. Some organizations may struggle to identify the controls which are applicable to them and incur expenses for things like anti-malware solution, SIEM solutions, ASV service, employee training, QSA service, and more depending on the organization's current IT posture.

Additionally, inadequate planning, staffing limitations, and insufficient technological resources can hinder seamless integration of PCI DSS into daily operations. E.g. A firm struggling with adhering to various compliance standards alongside PCI DSS, leading to confusion and inefficiency in integrating PCI DSS into their day-to-day operations.

Key Steps to Better Compliance

- Ensure Management Buy-in: Before embarking on the compliance journey, ensure full managerial support. Their commitment and leadership are essential for successful implementation.
- Start Small, Scale Smart: Don't get overwhelmed! Begin with a smaller scope, focusing on less complex aspects first. This reduces initial costs, minimizes personnel demands, and allows for smoother scaling later.
- Seek Expert Guidance: Consulting a PCI DSS expert saves you time, money, and potential breaches by ensuring efficient, accurate compliance from the start.
- Make Security Business-as-Usual: By integrating PCI DSS into an organization's daily operations, the organization avoids last-minute compliance scrambles and ensured continuous adherence to standard security guidelines. With these, there will be less compliance costs, a continuously protected brand, and happy customers.

PCI DSS compliance is not a destination, but a continuous journey. By recognizing the evolving landscape, anticipating challenges, and adopting proactive measures, organizations can navigate the path to effective security and safeguard the sensitive data entrusted to them.

Embracing a security culture is not just about meeting regulations, it's about building trust, protecting reputation, and ultimately enabling sustainable growth.

Unveiling NDPA: The Blueprint For Data Protection In Nigeria

On Monday, 12th June 2023, the Nigeria Data Protection Bill was signed into law by the President of the Federal Republic of Nigeria, His Excellency, Bola Ahmed Tinubu. The Nigeria Data Protection Act, 2023 (the Act), is the very first principal legislation on data protection in Nigeria. The signing of the Act was a positive response to the various campaigns by stakeholders in the Data Protection ecosystem for a unified primary legislation on data protection. It was believed that a unified primary legislation would help to position Nigeria as one of the progressive countries championing the Data Protection movement globally.

One of the significant features of the Act was the creation of the Nigeria Data Protection Commission (the NDPC) tasked with the responsibility of ensuring compliance with the provisions of the Act. The NDPA covers most of the NDPR. However, it does not go into the level of detail offered by the NDPR Implementation Framework.

New Trends Around the Framework

Personal data:

The definition of ”personal data” under the NDPA is narrower than the NDPR definition as, under the NDPA, ”personal data” is data relating an individual who is identifiable by reference to an identifier, whereas, under the NDPR, ”reference to an identifier” is preceded with ”in particular”, which opens the means of identification of the data subject. The NDPA’s requirement for the use of an identifier may result in some artificial intelligence data not falling within the scope of the definition of ”personal data”.

Data processor:

The NDPR and its implementation framework do not provide a definition for ”data processor” although this term is used in both documents. The NDPA defines ”data processor” as ”an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor”.

Sensitive data:

The NDPA broadens the scope of sensitive data by including genetic data, biometric data and data related to the data subject’s conscience and philosophy.

Processing

The NDPA definition of ”processing” is narrower than the NDPR definition in that it now excludes transient data originating outside Nigeria.

Personal data breach:

The NDPA has broadened the meaning of ”personal data breach” by defining it as ”a breach of security of a data controller or data processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. The NDPR definition (which is identical to the NDPA definition) does not include ”likely to lead to”. As a consequence, controllers and processors will need to determine in what circumstances a breach of security is likely to lead to the situations listed in the definition. There is a risk that the interpretation of “likely to lead” differs from that of the data protection authority

Data controller or data processor of major importance:

This category of controllers and processors is a new concept introduced by the NDPA and it is defined as “a data controller or data processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate”. Data controllers and processors of major importance must have a local presence or operate locally. ”Operate” is not defined, but it is likely that the Commission will consider that processing personal data in Nigeria will constitute operations in Nigeria.

Territorial scope:

The NDPA has removed the NDPR references to the data subject’s nationality or lineage. By doing so, it limits the risks of conflicts of laws and conflicts of jurisdictions as, by being applicable to foreign residents of Nigerian lineage, the law of the data subject’s (individual of Nigerian descent) country of residence would have likely applied, in conjunction with the NDPR. In addition, determining an individual’s country of ancestry prior to processing their data would have been an insurmountable challenge to most data controllers.

Data Protection Authority:

The NDPA formally institutes the Data Protection Commission as the independent data protection authority. To ensure continuity, it is specified that the Nigeria Data Protection Bureau, created in 2022, would morph into the Data Protection Commission, with some adjustments to be made to comply with the new statutory requirements regarding its composition and organization.

Data protection officers (DPO):

While the NDPR required ”every data controller to designate a data protection officer”, the NDPA has limited this obligation to data controllers of major importance. The NDPA is silent with regard to the location of the DPO and the possibility of having a group wide DPO.

Common challenges faced within the standard locally.

- **Data Governance and Mapping:** Understanding the flow of personal data across systems, locations, and third parties, and maintaining a comprehensive inventory of this data can be challenging, particularly in complex organizational structures.
- **Consent Management:** Obtaining valid and explicit consent for data processing activities, ensuring it's freely given, specific, informed, and unambiguous. Managing and documenting consent, especially in digital environments, poses challenges.
- **Data Subject Rights:** Managing and responding to data subjects' requests concerning their rights (such as access, rectification, erasure) within the stipulated timeframes, particularly in organizations with extensive databases or dispersed data sources.
- **Security Measures:** Implementing robust security measures to protect personal data from breaches, unauthorized access, or accidental loss. Ensuring continuous monitoring and upgrading of security measures to align with evolving threats is challenging.
- **Third-Party Compliance:** Ensuring that third-party vendors, partners, or processors handling personal data also adhere to NDPA requirements. Establishing and monitoring contractual agreements and compliance standards with these entities can be complex.

Advisory and expectation to achieve better compliance

- **Data Mapping and Inventory:** Maintain a comprehensive inventory of all personal data collected, processed, and stored within your organization. Understand the flow of this data and document it accurately.
- **Consent and Transparency:** Obtain explicit consent before processing personal data. Ensure transparency by providing clear and easily understandable information to individuals about how their data is used, processed, and stored.
- **Data Minimization and Retention:** Collect only necessary data for specific, legitimate purposes. Avoid excessive data collection and retain data only for as long as necessary, adhering to the NDPA's principles of data minimization and storage limitation.
- **Security Measures and Breach Response:** Implement robust security measures to protect personal data against unauthorized access, breaches, or accidental loss. Have effective response plans in place to address and report data breaches promptly.
- **Documentation and Compliance Review:** Maintain detailed records documenting NDPA compliance efforts, including policies, procedures, assessments, and training programs. Regularly review and update these documents to ensure they align with evolving NDPA guidelines and your organization's practices.

By focusing on these areas and continuously assessing and improving data protection practices, organizations can work towards better compliance with the NDPA and ensure the protection of individuals' privacy rights.

Navigating the Hurdles in Implementing ISO 27001

ISO 27001

The first version of ISO 27001 was published in 2005 and underwent a revision in 2013. Recently, in 2022, the standard underwent another update to further refine its guidelines and align with contemporary information security needs and advancements.

New trends around ISO 27001

The alterations from ISO 27001:2013 to ISO 27001:2022 are mostly incremental rather than drastic. The fundamental structure with its 11 main clauses remains largely unchanged, maintaining consistency in the framework for managing Information Security Management Systems (ISMS).

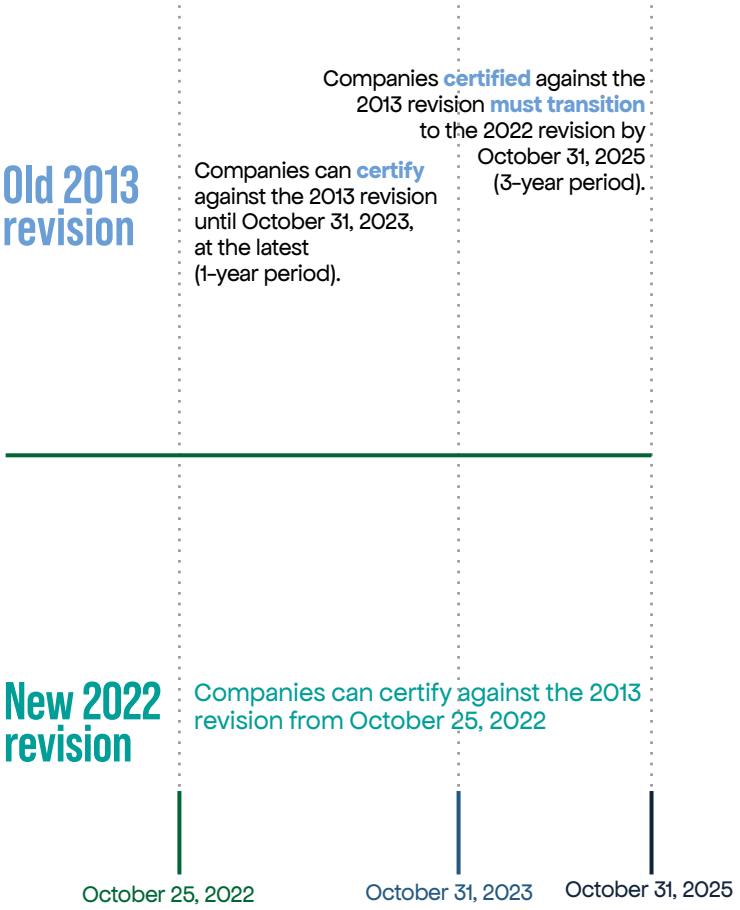
However, a notable shift is seen in Annex A, where the number of controls has decreased from 114 to 93. Furthermore, these controls have been reorganized into four sections, a significant shift from the previous version's 14 sections.

This revision indicates a more refined and streamlined approach to information security controls, possibly aiming for increased relevance, efficiency, and alignment with the evolving landscape of cybersecurity threats and best practices.

Changes to the management system

The move from ISO 27001:2013 to ISO 27001:2022 brought about notable changes within specific clauses:

- **Understanding the needs and expectations of interested parties (Clause 4.2):** added a new requirement (c) for analyzing which stakeholder needs should be integrated into the ISMS.
- **Information security management system (Clause 4.4):** emphasized the necessity of planning processes and their interactions within the ISMS.
- **Organization roles, responsibilities and authorities (Clause 5.3):** clarified that role communication occurs internally within the organization.
- **Information security objectives and planning to achieve them (Clause 6.2):** included a new point (d) that mandates the monitoring of objectives.
- **Planning of changes (Clause 6.3):** Introduced a requirement for planned execution of any changes in the ISMS.
- **Communication (Clause 7.4):** Removed the requirement for setting up communication processes.
- **Operational planning and control (Clause 8.1):** Added criteria for establishing and implementing security processes, removing the need to implement plans for achieving objectives.
- **Management review (Clause 9.3):** added a new requirement for stakeholders' input to align with their needs and expectations relevant to the ISMS.
- **Improvement (Clause 10):** Reorganized subclauses, positioning Continual Improvement (10.1) before Non-conformity and Corrective Action (10.2), without altering the content.

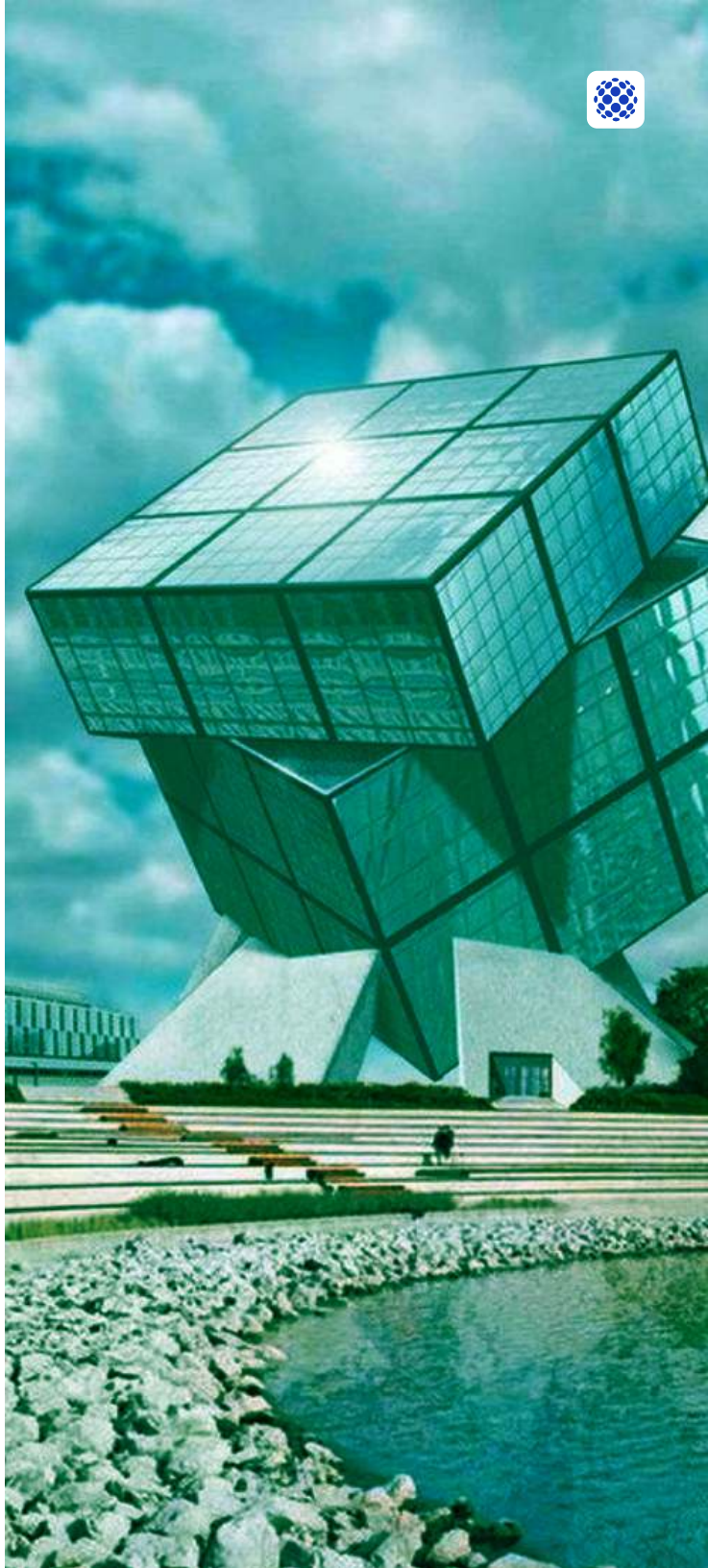


Changes to the Annex A Controls

- **Unchanged Controls:** 35 controls remained the same, carrying over from ISO 27001:2013 to ISO 27001:2022 without substantial alterations to their content.
- **Renamed Controls:** Around 23 controls were subject to name changes between the versions. However, these changes predominantly involved altering the label or title of the control rather than revising the core requirements significantly.
- **Merged Controls:** Approximately 57 controls were merged, leading to a reduction in the total number of controls.
- **New Controls:** 11 new controls were introduced in the new version, ISO 27001:2022.

11 new controls introduction in the ISO 27001 : 2022 revision

- A.5.7 Threat Inteligence
- A.5.23 information security for use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Information deletion
- A.8.11 Data masking
- A.8.12 Data leakage prevention
- A.8.16 Monitoring activities
- A.8.23 Web filtering
- A.8.28 Secure coding



Common Challenges faced with ISO 27001

- **Limited Resources and Budget Constraints:**

  The investment required for technology, training, and personnel can strain organizations with limited budgets, restricting access to necessary resources.

- **Lack of Awareness and Training:**

  Insufficient training among those involved in the Information Security Management System can lead to improper implementation and a lack of understanding about their roles in maintaining a secure environment.

- **Establishing Responsibilities and Ownership:**

  ISO 27001 spans beyond just the IT team, necessitating clear delineation of responsibilities across various teams within an organization to ensure proper management of the system.

- **Documentation Overload:**

  The multitude of policies and procedures required by the standard can overwhelm organizations, making it challenging to maintain and keep track of documentation.

- **Continuous Monitoring:**

  The need for ongoing monitoring of the ISMS, encompassing processes, procedures, and controls, is vital to ensure its ongoing effectiveness within the organization.

Advisory and expectation to meet better compliance

- Securing stakeholder support stands as a pivotal element for a successful certification process. Obtaining commitment, guidance, and resources from all stakeholders becomes imperative to identify essential changes, prioritize and execute remedial actions, and ensure consistent reviews and enhancements of the ISMS.

- Analyzing the impact of ISO 27001 on the organization involves considering the needs and expectations of various stakeholders, including regulators and employees. Examining both internal and external factors that influence information security is crucial in understanding the comprehensive impact.

- Developing a Statement of Applicability becomes necessary to outline precisely which ISO 27001 controls are pertinent to the organization's operations and systems.

- Conducting regular risk assessments and subsequent remediation is vital. Each assessment should result in a meticulously detailed risk treatment plan, specifying whether each risk will be addressed, accepted, terminated, or transferred.

- Continuous assessment of the ISMS performance is essential. Regular monitoring and measurement of the ISMS and associated controls help maintain effectiveness.

- Implementing comprehensive training and awareness programs is critical. Provision of security process and procedure training to all employees and contractors, coupled with efforts to elevate data security awareness across the organization, proves instrumental.

- Regular internal audits serve as proactive measures. Identifying and resolving issues internally before they are flagged by external audits is an essential strategy to maintain compliance and rectify shortcomings promptly.

The Game of Cyber Defense

“Imagine a world without cybersecurity solutions - a world where cybercriminals can easily hack into your personal and financial information, causing chaos and destruction. It's a terrifying thought!”

Thankfully, we don’t have to live in that world. With cutting-edge cybersecurity advisory/assurance services, cyber defense mechanisms, and cyberoffense tactics, we can protect ourselves from these threats and keep our data and systems safe.

Cybersecurity solutions are like the superheroes of the digital world, tirelessly working behind the scenes to keep us safe from harm.

Constantly evolving and adapting to new threats, making it harder for cybercriminals to get the upper hand.

So rest easy knowing that the cybersecurity experts are on the case, keeping you and your data safe from harm!

First, let’s open us challenges and incidents we have come across from the beginning of the year till date through investigation and analysis, you might see a similar problem your organization is facing, come along!”

Reflecting on the past year, their unwavering dedication is akin to a seasoned chess player’s commitment to studying past games for improvement.

Challenges Seen During Threat Analysis

Path Traversal Attack (Pawn's Gambit)

Imagine a pawn sneaking through the opponent's defenses. This attack aims to exploit vulnerabilities in web server software, manipulating URLs to access sensitive files. Like a pawn, it might seem innocuous, but it has potential for severe consequences. The Cyber Defense Team observed multiple attempts (pawn moves) to access critical system files, a vulnerability akin to a well-known opening strategy in chess.

Solutions (Counter Moves): To counter this attack, the team employs strategies:

- Blocking malicious IPs (protecting key squares)
- Patching servers (fortifying defenses)
- Protecting sensitive files (guarding valuable pieces)
- Strengthening security measures (strengthening overall position

Global Status
When it comes to cybersecurity, not every vulnerability diminishes over time. **CVE-2021-41773,** despite its age, continues to demand attention due to its tangible consequences in the real world.

SQL Injection Attempt (Bishop's Maneuver)

This technique attempts to manipulate databases, akin to a bishop moving diagonally across the board. Improper handling of queries could grant unauthorized access or compromise data, much like an opponent maneuvering to exploit a diagonal weakness.

Solutions (Defensive Maneuvers): Strategies include:

- Sanitizing input data (protecting against diagonal threats)
- Keeping software updated (maintaining a solid position)
- Avoiding shared database accounts (ensuring individual piece protection)
- Configuring error handling (preventing vulnerable spots)

Global Status

MOVEit Transfer developers recently made headlines after uncovering multiple SQL injection vulnerabilities in their product. Among these vulnerabilities is a critical one, known as **CVE-2023-36934**, which can be exploited without requiring user authentication, making it particularly concerning. Another SQL injection flaw, identified as **CVE-2023-36932**, has received a high-severity rating as it can be exploited by authenticated attackers.

JAWS Webserver Unauthenticated RCE (Queen's Gambit)

A significant number of attempts to exploit a specific server vulnerability. Here, attackers attempt to execute arbitrary commands without authentication, like a queen's powerful reach across the board.

Solutions (Queen's Defense): Countermeasures involve:

- Swiftly blocking suspicious IPs (eliminating opponent's influential pieces)
- Updating server software (fortifying the queen's position)
- Strengthening input validation (defending against powerful attacks)

Global Status

In April 2023, a critical level of attack attempts aimed at exploiting the Authentication Bypass Vulnerability in TBK DVR devices (specifically the 4104/4216 models) was observed, with over 50,000 unique IP detections. This surge could be attributed to the public availability of proof-of-concept (PoC) code.

Additionally, Fortinet has also cautioned about an increase in exploitation attempts targeting the JAWS Webserver RCE vulnerability **(CVE-2016-20016)** in MVPower CCTV DVR models, with a history of attacks dating back to 2017.

The Imperative Role of Web Application Firewalls

In an era dominated by digital interactions, web applications have emerged as both the lifeblood and Achilles' heel of organizations worldwide. Alarming statistics reveal that more than 43% of reported cyber breaches are attributed to web application attacks, establishing them as the primary target for malicious actors. As web traffic and the prevalence of internet-accessible applications continue to soar, the urgency to fortify these web applications against evolving threats has never been more pressing.

Challenges

Securing web applications presents a myriad of challenges for organizations, including:

- **Addressing Known Vulnerabilities:** Unpatched systems remain susceptible to known vulnerabilities such as SQL injections (SQLi), cross-site scripting (XSS), and command injections.
- **Zero-Day Exploits:** Emerging vulnerabilities, often exploited through zero-day exploits, demand proactive defenses to counteract the latest attack methods.
- **API Protection:** The critical role of Application Programming Interfaces (APIs) in facilitating interactions between internal software and web-based services necessitates robust protective measures.
- **Regulatory Compliance:** Meeting stringent compliance mandates, particularly those outlined in standards such as PCI DSS, requires a comprehensive approach to application security controls.
- **Visibility Gaps:** Incomplete visibility into application traffic leaves organizations vulnerable to undetected threats.

Local View and the Case of A New Financial Institution:

Reflecting on local insights, a recent incident involving a new financial institution entering the market exemplifies the urgency. Within 24 hours of announcing their digital presence, the institution faced a massive web attack. The onslaught included a Distributed Denial of Service (DDoS) attack and malicious code injections attempting directory traversal and querying for the "etc/passwd" from their servers. Fortunately, our Web Application Firewall (WAF) shielded the institution's web app, successfully blocking all these attacks.

Consequences Without the WAF:

Had the WAF not been in place, the consequences for the new financial institution would have been dire. The DDoS attack would have overwhelmed their servers, rendering the website inaccessible to potential customers. This downtime could have resulted in financial losses, tarnished reputation, and frustrated clients unable to access the newly launched digital banking services. The malicious code injections, if successful, could have compromised sensitive customer data, leading to legal repercussions and a loss of trust.

Global View and Stats

A glimpse into global cybersecurity trends underscores the severity of the situation. Recent studies, such as the 2023 Threat Detection and Response Report by CrowdStrike, highlight the dominance of web application attacks on a global scale. The pervasive nature of these attacks necessitates a strategic and all-encompassing security solution.

Solution

Enter the Web Application Firewall (WAF), a paramount line of defense that inspects all incoming web traffic for signs of malicious activity, thwarting attacks in real time. Deploying a robust WAF solution empowers organizations to:

- **Deep Visibility:** Attain comprehensive visibility into web application traffic, irrespective of its source, ensuring a proactive stance against potential threats.
- **Threat Detection and Filtering:** Identify and filter threats outlined in the OWASP Top 10, including injections, scripting attacks, and unauthorized access attempts.
- **Zero Day Exploit Defense:** Recognize anomalies and proactively block zero day application exploits, safeguarding against emerging vulnerabilities.
- **Regulatory Compliance Adherence:** Fulfill regulatory requirements such as PCI DSS, thereby enhancing the organization's overall security posture.
- **Data and Transaction Protection:** Safeguard customer data and transactions from web-based threats, reinforcing trust in digital interactions.

THE APT APOCALYPSE

Cybercriminals come in different forms. Some are inexperienced ransomware gangs, while others are well-funded and sophisticated state-sponsored groups with long-term goals. Advanced Persistent Threats (APT) groups are an example of the latter.

They target high-value entities and use complex tactics to infiltrate them. Small-to-medium-sized businesses (SMBs) may think they are not a target for APT groups, but they can be used as stepping-stones to larger targets, especially if they're part of a supply chain or serve larger entities. In fact, 93% of SMB executives believe that nation-state hackers use businesses like theirs as a backdoor into the country's digital defenses.

APTs differ from typical cybercriminals in three main ways:

- Sanitizing input data (protecting against diagonal threats)
- Tools: APTs use advanced tools and vulnerabilities, only using destructive malware when necessary.
- Crew: APTs are made up of experienced and motivated individuals who work closely together, in contrast to traditional cybercriminals who often have trust issues.

How an APT works its dark magic:

- Reconnaissance: Find valuable data and create a hit list.
- Infiltration: Tricky social engineering or custom malware delivery.
- Foothold: Get someone inside the target's network to run their malware.
- Expand: Deploy more malware, scout the network, and consolidate position.
- Data acquisition: Obtain desired data, requiring more network access.
- Maintain presence: Create entry points or leave back doors and cover tracks when done.

Unveiling the Supreme APT Groups for 2023

AFRICAN APT Groups

While there was no active APT group in Nigeria in 2023, there were external APT group attacks.

One of these attacks was carried out by the Sudanese Advanced Persistent Threat (APT) group known as Anonymous Sudan.

Anonymous Sudan (Mtn Nigeria): Anonymous Sudan took responsibility for a cyber-attack on the website of the Nigerian mobile telecommunication company, MTN, on August 2, 2023. The hacker group officially announced and shared details about the cyber-attack on MTN's website through their Telegram channel serving as a warning to service providers, government bodies, and telecommunications companies to prepare for a potential series of future attacks.

The hackers stated that a multitude of Nigerians reported experiencing a decline in network quality, purportedly attributable to the cyber-attack on MTN.

The following services, among others, were impacted: Internet, data calls, SMSes, Customer care panel, Recharge line system, Internal infrastructure, Bank top-up system, Balance, airtime systems, and MTN app and website.

They asserted that the company underwent a complete system outage, leading to the disruption of all systems and websites nationwide.

IRANIAN APT Groups

In the ever-evolving landscape of Iranian Advanced Persistent Threats (APTs), Iranian APT groups primarily use spear-phishing emails, vulnerability exploitation, and password-spraying techniques.

They target Middle Eastern and European countries for espionage purposes. APT35, widely known as Charming Kitten, secured its position as the most active Iranian APT group throughout the year 2023.

Charming Kitten is a notorious threat actor, engaged in various activities. They initiated by focusing on Iranian dissidents in Germany, employing social engineering to gain trust among legal experts, journalists, and human rights activists. Their objective was to penetrate Iranian opposition groups situated in Germany.

Charming Kitten employed spear-phishing methods to obtain sensitive information. They dispatched highly persuasive bogus messages to potential victims, with the goal of breaching their online services, such as email accounts and cloud storage. By thoroughly researching their targets' interests and political ties, the hackers fostered trust and enticed victims into virtual video conversations. Within these chats, victims were deceived into divulging their login credentials.

In September, Charming Kitten broadened its scope, seizing opportunities to target unpatched Microsoft Exchange servers in Israel, Brazil, and the United Arab Emirates. Their tactics involved exploiting well-documented vulnerabilities in publicly accessible servers across different sectors.

Their initial access was secured by exploiting a critical Exchange vulnerability, **CVE-2021-26855**. Simultaneously, Charming Kitten enhanced its malware, particularly the Powerstar backdoor, recognized as CharmPower. This updated malware boasts advanced functionalities, including seamless integration with the InterPlanetary File System. Additionally, its decryption capabilities and configuration details are now hosted remotely.

NORTH KOREAN APT Groups

In the dynamic environment of North Korean Advanced Persistent Threats (APTs), The North Korean APT groups focus on cyber espionage, particularly in maritime and aerospace technology acquisition. The two most prominent and active North Korean APT groups for the year 2023 were LAZARUS GROUP (UNC4899) and KIMSUKY (APT43).

LAZARUS GROUP, UNC4899: UNC4899, is a threat actor associated with North Korea, known for targeting cryptocurrency-related firms. These state-sponsored North Korean groups have infamously siphoned off billions, funding their nuclear missile program. In July, a significant supply chain compromise was revealed, targeting a U.S. software solutions provider. This sophisticated attack began with spear-phishing campaigns directed at JumpCloud, an essential zero-trust directory platform for identity and access management. The intrusion was linked to UNC4899, This incident mirrors a previous supply chain attack on the enterprise office phone company 3CX earlier in the year, both allegedly connected to North Korean state actors seeking cryptocurrency. This underscores North Korean actors' adaptability in finding innovative ways to infiltrate networks. The JumpCloud breach is a stark example of their preference for supply chain targeting, raising concerns about potential future breaches.

KIMSUKY A.K.A APT43: North Korean APT group Kimsuky adopted a deceptive strategy in their cyber operations. They circulated malicious batch files (*.bat) disguised as document program viewers (e.g., Word and HWP) via email. These files, when opened, simulated access to military or unification-related documents on Google Drive or Docs, creating a façade of document viewing. However, their real intent was malicious. These batch files cleverly detected various anti-malware processes and then downloaded and executed custom scripts tailored for each scenario.

For example, when confronted with Kaspersky, the batch file replaced Word's template file and ran a hidden cmd.exe. On the other hand, when dealing with Avast and Ahnlab processes, it downloaded scripts, altered browser and email shortcuts, and executed additional scripts. These covert tactics posed a significant risk, potentially resulting in malware infections and unauthorized manipulation of system files. Kimsuky's activities revealed an evolving approach.

In another instance, they combined Chrome Remote Desktop with their customized AppleSeed malware to take control of compromised systems. Spear phishing was their initial attack vector, with malware hidden within document files sent via email. After infecting a system, Kimsuky proceeded to install various malware, including Infostealers, RDP Patchers for enabling multiple remote desktop sessions, and Ngrok for remote access. Notably, they utilized Google's Chrome Remote Desktop to facilitate remote control through a host program. Users are strongly advised to exercise caution when managing suspicious email attachments and keep their software up to date to reduce the risk of infection.

CHINESE APT Groups

Chinese APT groups excel in sophisticated and persistent cyber espionage, often linked to state-sponsored hacking. They engage in high-profile cyberattacks targeting government entities, defense contractors, technology firms, and more, utilizing advanced methods such as zero-day exploits, custom malware, and social engineering. Their goals encompass stealing sensitive information, intellectual property theft, and securing strategic advantages in cyberspace.

Chinese APTs expand their reach to the Middle East, Asia, and critical infrastructure in the United States, including mobile platforms.In 2023, Double Dragon (APT 41) emerged as the notable and significant Chinese APT group.

The Android surveillance ware, WyrmSpy, and DragonEgg were linked to the Chinese espionage group APT41, also known as Double Dragon. APT41 has been active since 2012 and has targeted many organizations worldwide. This is the first time APT41 has been found using malware on mobile platforms. WyrmSpy and DragonEgg disguise themselves as system or third-party apps, trick users into granting extensive device permissions, and use additional modules to steal data. APT41 uses social engineering tactics to spread these malware instances, and none of these apps have been found on the Google Play Store yet.

RUSSIAN APT Groups

Russian APT groups are known for advanced cyber espionage, often tied to state-sponsored hacking. They conduct high-profile cyberattacks targeting governments, military, and critical infrastructure, utilizing sophisticated techniques like zero-day exploits and custom malware. Objectives include stealing sen sitive information and executing disruptive or destructive cyber operations.Russian APT activities are associated with the conflict in Ukraine, targeting NATO countries and Ukraine itself.

The two most active and prominent Russian APT groups for 2023 were COZY BEAR and TURLA.

APT29 A.K.A COZY BEAR: APT29, a Russian state-sponsored cyber espionage group, targeted NATO-aligned Ministries of Foreign Affairs using Duke malware. They cleverly used the open-source chat app Zulip to hide their activities. APT29 distributed tricky PDFs disguised as German embassy correspondence, with invitations to events like "Farewell to Ambassador of Germany" and "Day of German Unity," specifically designed to trap diplomatic entities. This campaign highlighted APT29's adaptability and sophistication in conducting targeted cyber espionage operations.

TURLA A.K.A VENOMOUS BEAR: Turla, a Russian state-sponsored hacking group, used a new malware backdoor called 'DeliveryCheck' to target the defense industry and Microsoft Exchange servers. They sent phishing emails with malicious Excel attachments that contained macros. Once activated, these macros created a fake Firefox updater task that downloaded and launched the DeliveryCheck backdoor. This allowed Turla to connect to their command-and-control server for further instructions. DeliveryCheck has a server-side component designed for Microsoft Exchange servers, turning them into command-and-control centers for attackers. The goal was to steal files containing Signal Desktop messages, providing access to private Signal conversations, documents, images, and archives on the compromised systems.

INCIDENCE RESPONSE USED CASES

BlackCat Bites Back: A Ransomware Tale of Woe and Wise Words

Imagine a dark Friday night, the clock ticking past midnight. The air crackles with anticipation, not for a party, but for a digital heist. A shadowy figure, codenamed BlackCat, prowls the network of a seemingly secure company. Armed with a malicious file, BlackCat slips past the defenses, a silent predator in the cyber jungle.

Dawn breaks, and the first scream echoes through the network. Files, once vibrant with data, are now frozen in a digital wasteland, renamed with the chilling extension ".nheukwq." Panic sets in. BlackCat, the notorious ransomware gang, has struck, leaving behind a ransom note like a mocking trophy.


RECOVER-nheukwq-FILES.txt - Notepad

File Edit Format View Help

```
>> What happened?

Important files on your network was ENCRYPTED and now they have "nheukwq" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

Samples are available on your User Panel.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and Install Tor Browser from: https://torproject.org/
2) Navigate to User Panel: http://qcypkuyv62li77jp6xkdde5hpvub75ryaktqdu3vozxan5izkvshcfqd.onion/?access-
key=X0PqSTCm8IljQGw2SI2JCFhSeZc82PyX2BgUaOS8bfrmx68YT1H5SEdAn7yKHvo2AspEcTTEfvRNiPlAzfbhs1U832%2B
```

The Ransomware note

The investigation begins, a digital detective story. Forensic tools are wielded like magnifying glasses, dissecting the attack, each step revealing BlackCat's cunning tactics. From reconnaissance to privilege escalation, the story unfolds, a chilling testament to the sophistication of modern cybercrime.

But fear not! from this digital darkness, wisdom emerges. Like battle-hardened veterans, we share the scars of BlackCat's attack, not to scare, but to fortify your defenses.

Here are the weapons in your digital arsenal:

- **The EDR shield:** A watchful guardian, this tool scans your systems for threats, ready to repel any BlackCat incursion.
- **The hunter's instinct:** Don't wait for the attack. Be the predator, proactively searching for vulnerabilities before they become footholds for the enemy.
- **The SIEM eye:** This all-seeing oracle gathers and analyzes security data, painting a clear picture of your network's health, revealing even the faintest BlackCat shadow.
- **The email fortress:** Don't let phishing emails be your downfall. Build an impenetrable barrier, filtering out the poison before it reaches your inbox.
- **The employee army:** Train your team, equip them with the knowledge to spot danger and the courage to fight back. Multi-factor authentication is their armor, strong passwords their swords.
- **The backup fortress:** Should the worst happen, have a secure haven for your data. Regular backups are your escape route, ensuring your valuable information survives any digital siege.

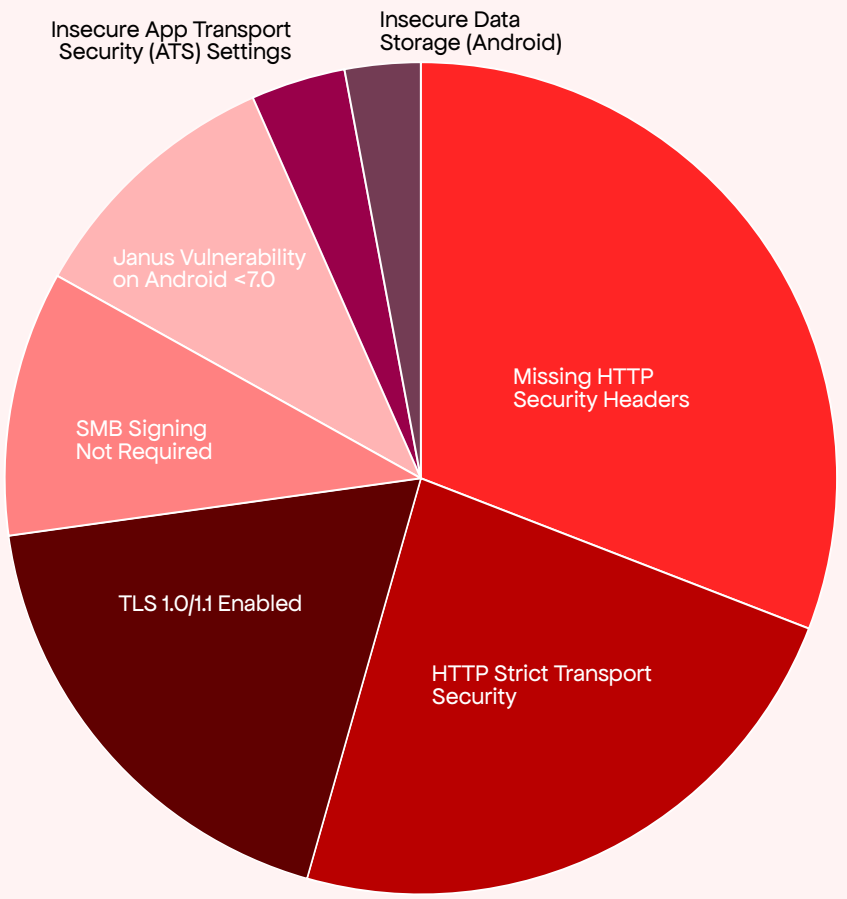
Name	BLACKCAT Ransomware
Type	Ransomware, Crypto Virus, Files locker
Cyber Criminal Contact	Website on Tor network
Encrypted Files Extension	Depends on the variant
Distribution methods	Infected email attachments (macros), torrent websites, malicious ads., Unpatched Vulnerable Applications.
Damage	All files are encrypted and cannot be opened without paying a ransom. Additional password-stealing trojans and malware infections can be installed together with a ransomware infection.
Free decryptor available	No
Ransom note	GET IT BACK-[file_extension]-FILES.txt
Ransom demand	$2 million - $5 million or more in Bitcoin
Detection names	Ransom:Win32/BlackCat.A (Microsoft), Ransom.Win32.BLACKCAT.SMYPCC5 (TrendMicro), HEUR:Trojan-Ransom.Win32.Generic (Kaspersky), Mal/Blackcat-A (Sophos), See all detection name variations on VirusTotal
Removal	Remove ransomware and related malware from your PC using trustworthy software. To repair malware damaged on Windows OS.

Intel Drop: Top Cyber Threats from the Front Lines

Attention, all operatives! This intel report brings you intel straight from the trenches, compiled by our elite offensive team. We've spent Q1-Q3 2023 knee-deep in client assessments, battling web vulnerabilities like seasoned veterans. Now, we're sharing the enemy's playbook, exposing their most frequent dirty tricks. Consider this your pre-mission briefing, troops.

HOSTILE TARGETS: WEBSITES AND WEB APPLICATIONS.

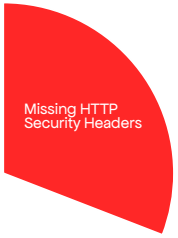
Enemy Maneuvers:



Vulnerabilities

Missing HTTP Security Headers (42%)

These are like barbed wire fences around your data, and the enemy loves to find gaps. This top vulnerability exposes the web applications or websites to various attacks, such as clickjacking, cross-site scripting, and information disclosure.



Global Statistics

Our analysis reveal alarming vulnerabilities across the web. Enemy forces exploit a crucial weakness: the under-adoption of vital HTTP security headers. Only 6.7% of top websites wield the Content-Security-Policy shield (XSS defense), and a mere 19.4% deploy the Strict-Transport-Security barricade (HTTPS enforcer).

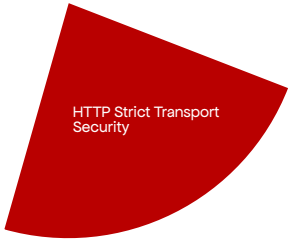
Prepare for Engagement!- Recommendation

- **Deploy the Strict-Transport-Security shield:** Force HTTPS connections, severing enemy communication lines. (Recommended value: max-age=31536000; includeSubDomains)
- **Equip the Content-Security-Policy armor:** Whitelist trusted sources, blocking malicious content infiltration.
- **Fortify with X-Frame-Options:** Control website embedding, preventing enemy framing maneuvers. (Recommended value: SAMEORIGIN)
- **Neutralize X-Content-Type-Options sniffers:** Prevent content type guessing, thwarting enemy reconnaissance. (Only valid value: nosniff)
- **Control Referrer-Policy intel:** Limit information sent with navigation, cloaking your movements from enemy eyes.
- **Deploy Permissions-Policy restrictions:** Limit browser features and APIs, denying enemy access to vital resources.

Remember, soldiers, security is your mission! Every implemented header strengthens your defenses, every website secured weakens the enemy.

HTTP Strict Transport Security (HSTS) Not Implemented (32%):

This encryption flag is your armored convoy escort. Without it, your data marches exposed, vulnerable to ambush.



Global Statistics

Only 26.6% of top websites utilize this vital encryption shield, leaving the remaining 73.4% exposed to man-in-the-middle attacks.

Enemy Tactic:

- **SSL Stripping/Downgrading:** Ambush initial HTTP requests, hijacking traffic to malicious doppelganger sites. Users, oblivious to the unencrypted connection, unwittingly surrender sensitive data.

Impact:

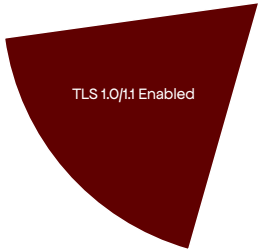
- **Compromised Credentials:** Passwords, credit card numbers, and personal information laid bare to the enemy.
- **Data Exfiltration:** Sensitive intel siphoned off, leaving organizations vulnerable and exposed.

Countermeasures:

- **Deploy HSTS Fortification:** Configure web servers to send the appropriate HSTS header with each response.
- **Max-Age Directive:** Specify how long browsers remember the HTTPS-only access requirement (e.g., max-age=31536000).
- **IncludeSubDomains Directive:** Extend protection to all subdomains, sealing off potential infiltration routes.

TLS 1.0/1.1 Enabled (25%)

These outdated protocols are like creaky bunkers – full of security holes. These protocols are riddled with vulnerabilities like SSL stripping, channel downgrade, and protocol downgrade. Enemy forces exploit these weaknesses, intercepting communications, and pilfering sensitive data.



Enemy Tactic:

- **Exploiting Outdated Encryption:** Like cracking a rusty lock, attackers breach TLS 1.0 and 1.1 with ease, siphoning off intel and disrupting operations.
- **Unencrypted Communication:** Imagine sending intel in plain text – over 61% of network traffic lacks encryption, leaving data exposed for all to see.

Intel Flash:

- 80% of network traffic analyzed has encryption flaws.
- TLS 1.0 and SSL v3 still linger, despite deprecation by internet standards and PCI DSS.

Countermeasures:

- **Fortify the Network:** Disable TLS 1.1 and lower versions, erecting a modern, secure barrier against enemy attacks.
- **Upgrade Defenses:** Update websites, applications, and libraries to support TLS 1.2 or higher, ensuring robust encryption across the board.
- **Test and Verify:** Conduct compatibility checks across operating systems and browsers to guarantee seamless operation with upgraded protocols.

SMB Signing Not Required (14%)

Our analysis and investigation reveals a critical network vulnerability: widespread use of the default "public" community name in SNMP agents. This open door allows enemy forces to waltz in, steal sensitive network intel, or even rewrite the battle plan!

Enemy Maneuver:

- **Leveraging Default Code:** The ubiquitous "public" name acts as a universal password, granting access to anyone who stumbles upon it. Imagine leaving your HQ vault unlocked – that's how vulnerable your networks are!

Impact:

- **Intel Siphon:** Enemy agents can download network maps, device configurations, and user privileges, painting a clear picture of your defenses.
- **Configuration Hijack:** With access, the enemy can rewrite firewall rules, redirect traffic, and sow chaos within your network, rendering it useless.

Severity Rising:

- **CVE Surge:** The number of vulnerabilities linked to this open door has skyrocketed, from 16 in 2019 to 23 in 2023!
- **CVSS Score Soars:** The threat level has escalated, with a 2023 score of 10.0, indicating a high-impact, critical breach.

Enemy Targets:

- Top Nations: China, India, and the US are prime targets, with countless networks vulnerable to this simple exploit.

Countermeasures:

- **Fortify the Code:** Replace "public" with a robust community name, a complex cipher at least 12 characters long, mixing upper and lowercase, numbers, and symbols.
- **Deploy Access Control Lists:** Create digital gatekeepers – ACLs restrict access to authorized personnel and devices, keeping the enemy out.
- **Encrypt Network Traffic:** Cloak your data in an impenetrable shield – SNMP encryption scrambles sensitive information, making it unreadable to prying eyes.
- **Secure Unneeded Devices:** Don't leave unnecessary equipment online – disable SNMP on devices that don't require network management.

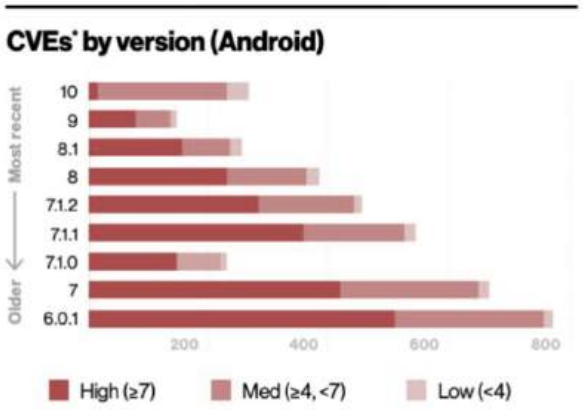
Every hardened SNMP agent strengthens our defenses, every encrypted connection severs enemy intel pipelines!

Janus Vulnerability on Android <7.0 (14%)

This old Android bug is like a hidden tunnel into your network. Our reconnaissance reveals a critical Android vulnerability; Janus, allowing enemy forces to modify app code and APK files without compromising signatures, bypassing verification like a cloaked spy. This opens the door for malware, spyware, and ransomware to infiltrate devices and wreak havoc!

Enemy Tactic:

- **Code Tampering:** Like a forged document passing inspection, the enemy alters app code, injecting malicious functionality while maintaining a seemingly legitimate facade.



Impact:

- **System Integrity Compromised:** Enemy code can manipulate core functions, steal data, and disrupt operations, turning your Android device into a Trojan horse.
- **Millions Exposed:** 7.5% of Android devices remain vulnerable, a vast target pool for enemy exploitation.

Affected Regions:

- China, India, and Brazil: Enemy intel indicates these regions are prime targets for Janus attacks.

Countermeasures:

- **Upgrade to Android 7.0+:** Patch the vulnerability and strengthen defenses with the latest code.
- **Prioritize Security Updates:** Install updates religiously, sealing cracks in your digital armor.
- **Activate Google Play Protect:** Deploy this real-time shield to scan for and neutralize threats.
- **Download Wisely:** Stick to trusted sources like Google Play, scrutinize permissions and reviews.
- **Fortify with Mobile Security:** Implement reputable solutions for proactive threat detection and protection.
- **Conduct Security Audits:** Regularly scan devices for vulnerabilities and plug any gaps before the enemy can exploit them.

Take action, secure your Android devices, and repel the digital invaders!

Insecure App Transport Security (ATS) Settings (5%)

Think of ATS as your air defense system, filtering out unauthorized missiles. Weak settings leave your data vulnerable to aerial bombardment. Widespread insecure App Transport Security (ATS) settings leave iOS and iPadOS apps vulnerable, exposing sensitive data like an open comms channel.

Over 25% of apps analyzed by lack proper encryption, allowing the enemy to eavesdrop and steal vital intel.

Enemy Tactic:

- **Exploiting Insecure Connections:** Unencrypted communications act like unarmored soldiers, easily intercepted and compromised. Enemy forces can steal data, manipulate transmissions, and disrupt operations.

Impact:

- **Data Breach:** Sensitive information like passwords, financial details, and user data are laid bare, leaving users vulnerable to identity theft and other attacks.
- **App Hijacking:** Enemy forces can hijack app functionality, spreading misinformation, disrupting operations, and even launching attacks from compromised devices.

Vulnerability History:

This critical weakness has lurked since iOS 9 and OS X v10.11, a ticking time bomb exploited by the enemy for years.

Countermeasures:

- **Fortify App Defenses:** Ensure all network connections use HTTPS, the digital equivalent of armored communication lines.
- **Deploy TLS 1.2 or Higher:** Equip apps with the latest encryption protocols, like soldiers wielding advanced weaponry.
- **Activate Google Play Protect:** Deploy this real-time shield to scan for and neutralize threats.
- **Eliminate Insecure Exceptions:** Don't create backdoors for the enemy! Avoid exceptions for specific domains, closing any potential infiltration routes.

Insecure Data Storage (Android) (4%)

Leaving sensitive intel lying around is like broadcasting your location on an open channel. Confidential data lies unprotected, like classified documents left on an open battlefield, vulnerable to exploitation by malware, network interception, or even physical device capture.

Enemy Tactic:

- **Data Breaches:** Enemy forces exploit insecure storage like unlocked vaults, siphoning off passwords, financial information, and user data – vital intel for their operations.

Impact:

- **User Privacy Compromised:** Personal and financial data exposed, leaving users vulnerable to identity theft, financial fraud, and other attacks.
- **App Reputation Destroyed:** Data breaches erode trust, damaging app developers' and organizations' reputations.

Widespread Threat:

- **76% of mobile apps affected:** This critical vulnerability is not an isolated incident, but a rampant enemy infiltration tactic.
- **OWASP Top 10 Risk:** Ranked second on the OWASP's list, the threat is clear and present.
- **Data Breaches Soar:** 31 million accounts leaked in just three months, with major nations like the US, Russia, and France at risk.

Countermeasures:

- **Encrypt Data:** Shield sensitive information with impenetrable encryption, both at rest and in transit.
- **Secure Storage:** Lock down data in secure locations, like fortified vaults for your digital intel.
- **Review and Update Policies:** Regularly audit data storage practices, plugging any gaps before the enemy can exploit them.
- **Incident Response Plan:** Have a robust plan in place to swiftly respond to and mitigate breaches, minimizing damage and protecting your data.

Key trends and developments should we anticipate in the year 2024

Next-Level Phishing Attacks

Social engineering attacks involving tricking users into giving attackers access to systems will also increase in sophistication. Generative AI (such as ChatGPT) tools enable more attackers to make smarter, more personalized approaches, and deepfake attacks will become increasingly prevalent.

IoT Cyber Attacks

More devices talking to each other and accessing the internet means more potential "ins" for cyber attackers to take advantage of. With the work-from-home revolution continuing, the risks posed by workers connecting or sharing data over improperly secured devices will continue to be a threat.

Generative AI: a new frontier in cyber threats

As AI increases in sophistication at a frankly alarming rate, we will continue to see more sophisticated and smart AI-powered attacks. This will range from deepfake social engineering attempts to automated malware that intelligently adapts in order to evade detection. At the same time, it will help us detect, evade or neutralize threats thanks to real-time anomaly detection, smart authentication and automated incident response. If cyber attack and defense in 2024 is a game of chess, then AI is the queen – with the ability to create powerful strategic advantages for whoever plays it best.

Social engineering and user privacy: the human factor

The human element is a significant factor in cybersecurity incidents, with 95% of breaches attributed to human error. This makes it not only a common issue but also a costly and serious one. Educating users about these attacks and implementing strong security measures are vital.

5G Security

The rollout of 5G networks introduces faster speeds and lower latency, but it also brings new security risks. Ensuring the security of 5G networks and devices is essential to protect critical infrastructure and sensitive data.

Insider Threats

Insider threats pose a significant risk as they come from within an organization. Implementing strong access controls, monitoring user activities, and conducting regular security audits are essential to mitigate insider threats.

The Rise of Quantum Computing and Its Impact on Cybersecurity

Quantum computing, a rapidly advancing field in 2024, is revolutionizing how we think about data processing and problem-solving. Unlike classical computing, which uses bits represented as 0s or 1s, quantum computing utilizes qubits. Qubits can exist in multiple states simultaneously, thanks to quantum superposition. This allows quantum computers to process vast amounts of data at unprecedented speeds, solving complex problems much faster than traditional computers.

Cybersecurity Skills Gap and Education

In 2024, the cybersecurity sector continues to grapple with a significant challenge: the skills gap. As cyber threats become more sophisticated, the demand for skilled cybersecurity professionals surges. However, there is a noticeable shortage of individuals equipped with the necessary skills and knowledge to effectively combat these evolving threats. This gap poses a risk not only to individual organizations but also to global cyber infrastructure.

Multi-Factor Authentication

Multi-factor authentication (MFA) is a security measure that requires users to provide more than one form of authentication before they can access an account. This additional layer of security helps to protect against cyberattacks, as attackers must have access to multiple pieces of information in order to gain access. Organizations should ensure that all accounts are secured with MFA to reduce the risk of unauthorized access.

Contact us

info@cybervergeent.com
+234-1-2900808

www.cybervergent.com
212/214 Herbert Macaulay Way, Yaba, Lagos.