The Latest Cybersecurity Threats

and How to Detect and Mitigate Them

by Edgio

Organisations globally are engaged in digital transformation, a cyber-industrial revolution promising digital automation and operational agility. The pandemic was just cause for our digital stampede but organisations quickly chose the latest offering incorporating machine learning, artificial intelligence and blockchain without understanding the attack surface. The rapid, unbridled digital transformation adds cybersecurity risks that must be addressed.

$9.4M is the average cost of a data breach in the US.

83% of customers stop business with an org after a breach.

75% of web apps have a high severity vulnerability.

According to a 2022 IBM study by the Ponemon Institute, 83% of U.S. companies have experienced a data breach more than once, costing them over $9.44 million, more than double the global average of $4.35 million. To add fuel to the fire, the Cybersecurity and Infrastructure Security Agency recently added 66 new vulnerabilities to its Known Exploited Vulnerabilities Catalog. Additionally, new common vulnerabilities and exposures (CVEs) grew by over 24% year-over-year in 2022. At this point, it's not if a cyberattack is going to occur, but when.

What these numbers don't include is the potential damage to your brand's reputation and to your customers. According to research from PCI Pal, 83% of consumers will stop spending with an organisation immediately after a security breach - and over 21% of those consumers will never return.

In this article, we'll look at some of the most significant cybersecurity threats organisations are currently facing and how to detect and mitigate them in order to protect your customers, your brand and your bottom line. Here are some highlights:

- 24% of all breaches involve ransomware
- DDoS attacks grew a whopping 57% year-on-year from 2022-2023
- 34% of all login attempts are done by bots
- $4.5 milion is the average cost of credential stuffing

Ransomware

According to Verizon's 2023 Data Breach Investigations Report (DBIR), ransomware continues its reign in 24% of all security breaches.

What is ransomware? A type of malware delivered by attackers that encrypts a victim's data on their devices or servers compromising the availability of their data and demanding payment in exchange for the decryption key.

Ransomware is ubiquitous among organisations of all sizes and in all industries. In fact, over 90% of industries have

ransomware as one of their top three threats, including finance, retail, healthcare and education - and the overall costs of recovering from a ransomware incident are increasing. The most common ways ransomware spreads is through email, desktop sharing software and applications.

1. Educate employees. Phishing and other social engineering techniques are by far the biggest vector or entry point for ransomware attacks, making it critical to implement a comprehensive cybersecurity awareness program to educate employees about the risks, teach them to recognise suspicious emails and links and encourage them to report potential threats.
2. Have regular backups of important data and to keep all software and systems up to date with the latest security patches.
3. Run security tests regularly to validate system and network health of your systems.
4. Maintain up-to-date anti-virus software and scan all software downloaded from the internet prior to executing.
5. Restrict users' ability (permissions) to install and run unapproved software, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
6. Segment your network to isolate critical systems and data from less secure areas.
7. Secure assets behind a proxy-based service, which masks internet-facing applications. If the application cannot be discovered, there's no attack surface to exploit.

Implement advanced web application and API protection services (CWAAP) for all your web-facing applications to mitigate any application vulnerability that can be used by the attackers as a backdoor into your critical systems and data via direct compromise or lateral movements.

Phishing

If you ever received an email containing a suspicious attachment or a harmful link that prompts you to update your password, you've experienced a phishing attempt. These attacks make up 44% of all social engineering security incidents.

What is phishing? Phishing is a type of social engineering attack that aims to trick victims into providing sensitive information or installing malware via nefarious links usually delivered in the form of spam emails.

These attack types are becoming increasingly sophisticated and harder to detect. Breaches caused by longest mean time to identify and contain at 295 days according to IBM's 2022. Recently popular are phishing attempts on employees asking them to provide ID comes from the company's CEO.

Advancements in generative AI are only enhancing messaging authenticity, making it more likely that employees will fall for such scams. increasingly read on mobile devices, bad actors have taken advantage of the fact these small-screen devices have limited functionality to examine email headers or links, raising the of employees clicking on bogus links.

To protect against phishing:

1. Educate employees about the dangers of phishing, including how to spot a phishing email, avoiding clicking on unknown links and reporting any unusual activity promptly.
2. Run internal phishing campaigns to identify weak points in any part of your organisation.
3. Run external email scans to tag emails from external entities properly along with advanced email filtering and spam detection systems to identify and block phishing attempts.
4. Invest in remote browser isolation (RBI) and micro-segmentation to prevent access to the rest of the system if malware is downloaded from a phishing email.
5. Implement Multi-Factor Authentication (MFA) and enforce regular password updates to prevent an attacker from gaining unlimited access.

DDoS Attacks

Distributed Denial-of-Service (DDoS) attacks continue to be ubiquitous and have remained in the top spot of incidents for several years now.

What is a DDoS attack? A malicious attempt to disrupt the availability of networks and systems by overwhelming the target or its surrounding infrastructure with a flood of traffic, rendering it unavailable to legitimate users.

DDoS attacks can be launched from a large number of compromised devices, also known as botnets, by malware. The distributed nature of the botnet makes it difficult to trace the source of the attack.

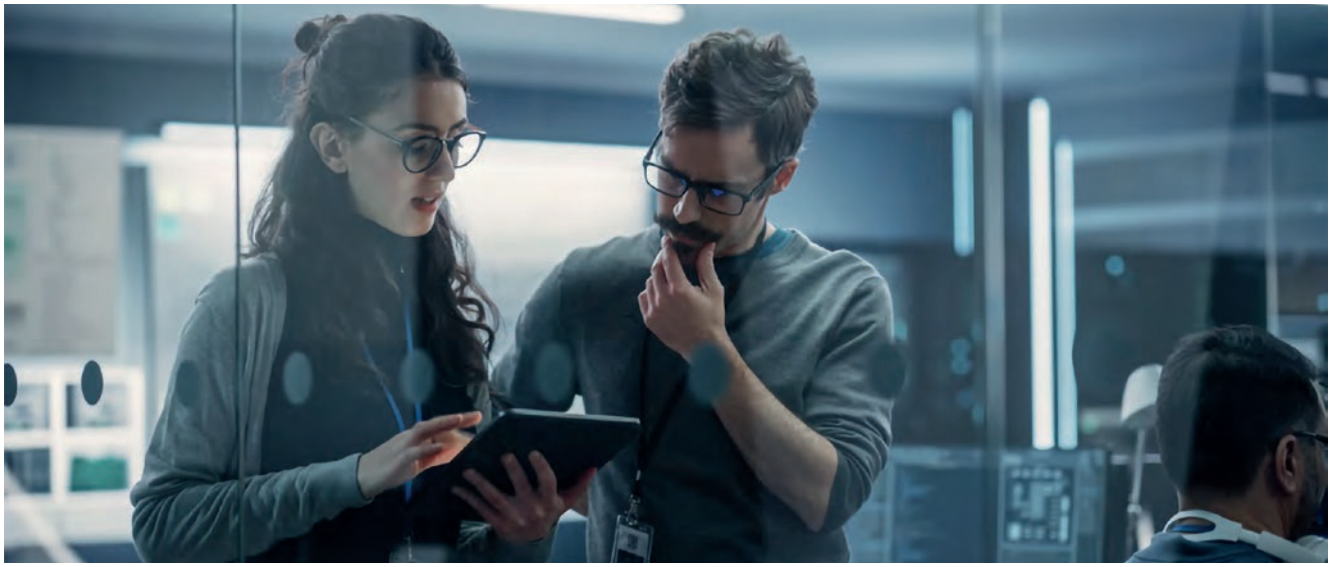
DDoS attacks are commonly achieved via exploiting network or transport layer protocol (i.e. ICMP DP flood, or TCP flood) where massive volumes of packets are being sent to saturate a network. Application DDoS, in the form of carefully crafted HTTP flood, is designed to surgically overload a sensitive application or backend system that has been on the rise. In fact, the 2023 DBIR found the median DDoS attack grew a whopping 57% from 1.4 gigabytes per second (Gbps) last year to 2.2 Gbps now, and the 97.5 percentile grew 25% from 99 Gbps to 124 Gbps. This is why it's critical to have holistic protection from the full spectrum of DDoS attacks.

On June 14th 2022, Edgio prevented one of the largest recorded DDoS attacks measuring 176 million packets per second (Mpps) which targeted a multinational e-commerce client based in Asia. Our proprietary software-based DDoS detection and mitigation system, called 'Stonefish' internally, was able to protect our clients from the attack. Despite its massive size, our client which saw no impact on its origin as Edgio's network absorbed 100% of the attack traffic. Our 24X7 SOC notified the client, even though there was no action required from them. On June 27th, 2022, Edgio prevented yet another, even larger, DDoS attack for an important customer. This attack was 355.14 Mpps, which places it at 44% of the largest publicly disclosed DDoS attack ever. Once again, Edgio's network absorbed the attack traffic.

To protect your business from DDoS attacks:

1. Utilise a content delivery network (CDN) service to distribute your web content across multiple servers and data centres. Highly distributed, edge-based CON solutions that have built-in DDoS protection can absorb and mitigate layer 3, 4 and 7 attacks across massive edge networks.
2. Deploy anomaly detection and Intrusion Detection Systems (IDS) to monitor network traffic and identify unusual patterns or behaviours. These systems can detect and raise alerts for potential DDoS attacks in real-time.
3. Implement DDoS mitigation services that employ massive scrubbing centres to stop direct-to-origin attacks which may side-step a CON or proxy layer and target your internet-facing applications in the data centres.
4. Deploy multiple solutions such as rate-limiting, network redundancy and bandwidth scaling to reduce the disruption of your applications while engaging CON and DDoS mitigation services to increase resiliency.
5. Develop an incident response plan specifically tailored to DDoS attacks. This plan should outline the steps to be taken during an attack, including contact information for relevant personnel, communication protocols, and procedures for diverting traffic or activating DDoS mitigation services.
6. Conduct regular DDoS assessments and testing to identify any weaknesses in your infrastructure. This helps identify areas that require improvement and ensures that your protection measures are effective.
7. Consider a 24/7 Security Operating Centre (SOC) to improve your business' security responsiveness.

Learn more about how you can reduce vulnerabilities and defend your brand against DDoS attacks from the Edgio biog.



Zero-Day Exploits

Some of the highest-profile security incidents of the last couple of years were attributed to zero-day vulnerabilities found in open-source software and popular SaaS used in many enterprises (i.e. Apache, WordPRess, Drupal, Confluence, etc).

What are zero-days? Zero-day is a term that describes a situation when software developers and security teams are unaware of a software vulnerability and they've had "O" days to work on a security patch or an update to fix the issue. A zero-day exploit is the technique a malicious actor uses to cause damage to or steal data from a system affected by a vulnerability.

Businesses should:

1. Follow secure coding practices and frameworks, such as OWASP (Open Web Application Security Project) guidelines during the development of your website. This reduces the likelyhood of introducing vulnerabilities that could be exploited in zero-day attacks.
2. Implement a highly capable Web Application and API Proection (WAAP) that detects not only the most common vulnerablities but also provides the ability to create virtual patches to mitigate zero-day exploits quickly.
3. Utilise multiple security measures such as firewalls, intrusion detection and prevention systems and web content filtering. These can help block access to malicious websites and known command and control servers associated with zero-day exploits.
4. Leverage artificial intelligence and machine learning (AI/ML) solutions to quickly detect patterns in data that may indicate suspicious behaviour or malicious activity.
5. Keep your software up to date and patched. Although zero-day vulnerabilities are unknown, software vendors often release patches and updates to address known vulnerabilities.
6. Stay informed on the latest security news, vulnerabilities, and patches. Subscribe to security bulletins or follow reputable sources to stay up-to-date.
7. Develop and regularly update an incident response plan specific to zero-day attacks. This plan should outline the steps to be taken when a zero-day vulnerability is discovered or when an attack is suspected, including communication protocols, containment measures and recovery procedures.

Edgio built its own intelligent rules engine that integrates open source, proprietary and application-specific rules to protect against known and zero-day threats.

Advanced Persistent Threats

Requiring more resources than a standard web application attack, Advanced Persistent Threats (APT) are highly complex, manually executed attacks which pose a large threat to large enterprises or governmental networks.

What are APTs? APTs are methods used by attackers to infiltrate a network and establish a long term presence to gather highly sensitive info or to compromise the integrity of the system.

APTs are often targeted and sophisticated attacks launched by nation-state actors or other highly skilled attackers. These attacks can be perpetrated by breaching the weakest part of an organisation's system that's least well-maintained (e.g. non-revenue generating or an informational website). These weak points from seemingly less valuable targets allow the attacker to potentially gain backdoor access to other critical services.

To protect against APTs, it is crucial to:

1. Have robust network segmentation in place and implement strong perimeter defence such as firewalls, intrusion detection/prevention systems and secure gateways to monitor and control inbound and outbound network traffic.
2. Use advanced threat intelligence and behaviour-based analytics to identify and block suspicious activities.
3. Utilise robust endpoint security solutions that include antivirus, anti-malware and host-based intrusion detection/prevention systems. Regularly update and patch endpoint software to address vulnerabilities and ensure the latest threat definitions are in place.
4. Patch software and OS vulnerabilities as quickly as possible.
5. Implement holistic security solutions and ensure all internet-facing applications, regardless of how "valuable" they are, are protected to prevent lateral movements.
6. Enforce strong access controls and authentication mechanisms. Use complex passwords, implement two-factor authentication (2FA) or multi-factor authentication (MFA) and regularly review and revoke unnecessary user privileges.

7. Encrypt sensitive data in transit and at rest to protect against unauthorised access.
8. Implement data loss prevention (DLP) measures to detect and prevent the exfiltration of sensitive information.
9. Develop a robust incident response plan specific to APTs. This plan should include procedures for detecting, containing and eradicating APTs. Regularly test and update the plan to align with the evolving threat landscape.

Bot Attacks

Finally, one of the biggest threats to business is bot attacks. A large part of the internet traffic today is from automated clients, aka bots.

What are bot attacks? A bot attack is a type of cyber attack that uses automated scripts to disrupt a site, steal data, make fraudulent purchases or perform other malicious actions.

Some bots are essential to the functioning of an online business (i.e. SEO bots, monitoring bots, chatbots and social media bots), however, there are also large numbers of bad bots that could cause severe damage to an organisation.

Some of the most common attacks performed by bad bots include credential stuffing, application DDoS attacks, data scraping, inventory exhaustion and gift card fraud.

According to IBM, the average cost of credential stuffing to an organisation was $4.55 million in 2022. In fact, over 10 billion credential stuffing log-in attempts were recorded in 2022, making up 34% of all login attempts. Another study shows that one in four organisations have lost $500k from a single bot attack.

Due to the prevalence of bot attacks, every business should have an advanced bot management solution in its cybersecurity arsenal.

Look out for an advanced bot management solution that:

1. Uses signature fingerprinting and behavioural inputs to separate “good” bots (e.g. Google) from bad bots.
2. Utilise a machine learning model that combines both signature and behavioural models to detect and identify bad bots.
3. Configures advanced rules and set actions based on bot score based on risk tolerance.
4. Provides real-time analytics with drill-down and advanced filtering.
5. Customises allowlists via API (programmatically) or via the console based on URL, UA, JA3, cookie and more.

How can businesses detect and mitigate cyber-attacks?

Even though the threat landscape continues to evolve, there are still several things you can do, as mentioned throughout this article, to protect your business from cyber-attacks:

- Adopt holistic security protection by utilising edge-enabled security solutions that are massively scalable and improve both the security and observability of the network and application traffic, as well as the performance and reliability of your applications.
- Keep all software and systems up to date with the latest security patches and implement advanced web application and API protection services (WAAP) for all your web-facing applications to mitigate any application vulnerability that can be used by the attackers as a backdoor into your critical systems and data.
- Protect your network, applications, and origin using an edge-based DDoS protection solution.
- Thwart direct-to-origin attacks with a dedicated high-capacity DDoS scrubbing solution.
- Implement an advanced bot management solution to detect and monitor bot traffic and mitigate malicious bots.
- Educate and train employees to help protect against attacks like phishing scams.
- Consider a 24 x 7 SOC to supplement your security operations and improve your business' security responsiveness.

Key Edgio security advantages

Edgio is one of the very few players in the market providing edge-enabled, holistic, multi-layer security solutions. Our customers know Edgio's WAAP defends their business' infrastructure, applications, and brand 24 x 7. Edgio's holistic, edge security platform provides comprehensive protection across the network and infrastructure, web applications and APIs, including bot management. In addition, Edgio's managed security services (threat analysis and managed SOC) and analytics (analytic dashboard, real-time logs and SIEM integration) enable businesses to identify threats and act faster than ever.

- Edgio's 250 Tbps of bandwidth capacity is one of the largest global edge networks.
- Edgio is one of few edge platforms to provide a fully comprehensive network and application protection via our Web Application and API protection (WAAP). Our multi-layered solution provides holistic protection.
- Edgio's unique Dual WAAP mode allows customers to perform security AB testing via production traffic, providing predictive data, cutting down the security update cycle and improving response time against new vulnerabilities.
- Edgio's advanced bot management solution utilises a patent-pending machine learning model to detect bots via signature and behavioural fingerprinting on the server side without requiring JS injection or modification of SDKs.
- Edgio's automated DDoS Mitigation works 24 x 7 x 365 protecting thousands of web applications daily. Edgio's proprietary Stonefish DDoS mitigation system analyses samples of all packets traversing our network, scoring them for threats and taking action when necessary.
- Edgio's managed security team and 24 x 7 SOC proactively mitigate threats and offload customer security operations.
- Edgio is API-first, and supports security automation and Terraform integration. All security updates can be deployed on the entire Edgio network in under 60 seconds.

For more infomration, see https://edg.io