radware

Why Bot Mitigation Could Be Crucial For GDPR Compliance

A report for organizations impacted by the GDPR

The GDPR in brief

The GDPR (General Data Protection Regulation) is a comprehensive and significant set of new laws that came into effect across the European Union on May 25, 2018, with the aim of harmonizing EU data privacy laws. The GDPR rules aim to compel businesses and other organizations to secure EU residents' Personally Identifiable Information (PII). At its core, it empowers EU residents by putting them in control of their personal data – and how that data can be obtained, stored, processed, and otherwise used. These wide-ranging regulations are applicable not only to organizations within Europe – any organization located anywhere in the world must comply if it collects personal information from EU residents.

A key aspect of the GDPR is a radical revision of what constitutes personal data and how businesses and other organizations obtain consent for its use. They will now be legally obligated to obtain verifiable consent from EU residents that is explicit, informed and freely given. Consent to use of personal data must be provided by individuals on an opt-in basis, rather than the currently widespread practice of opting out of providing consent to businesses that ask for personal data. In addition, residents can withdraw their consent, and even request that their personal data be deleted within a specified time frame. The regulation goes even further by requiring that organizations only use personal data for the sole purpose that was defined when the data was collected from the user.

Article 5 (f)[1] of the GDPR requires that "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

In the most extreme scenario, an organization is potentially liable for various legal sanctions and penalties of up to 4% of annual global revenue or €20 million (whichever is higher) – if found culpable for breach of one or more articles of the GDPR. The maximum fine can be imposed for the most serious infringements, such as not having sufficient customer consent to process data, or violating the core of 'privacy by design' concepts. This has put the legal onus on many organizations around the world to prepare for GDPR compliance by examining their systems and processes around personal data collection, storage, and usage thereof.

GDPR compliance requires data protection by design and by default

GDPR makes it mandatory to incorporate data protection by design and by default. 'Privacy by design' is a key legal requirement of the GDPR. It calls for personal data protection to be included right from the outset when developing and deploying systems that handle personal data, and not as an afterthought.

Article 25[1] of the GDPR requires that data controllers should "...implement appropriate technical and organisational measures... in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

If you handle any personal data of EU residents directly (or indirectly as a subcontractor) – such as users accessing your website or app from Europe – the GDPR compels you to stringently secure personal data handled across your technology infrastructure, as well as by your subcontractors and vendors (if they also handle or process personal data).

The GDPR requires data controllers and processors to implement appropriate technical and organizational measures, such as:

- Anonymizing and encrypting personal data
- Ensuring that data processing systems preserve the confidentiality, integrity, availability, and resilience of personal data
- Restricting access to personal data to authorized personnel for business-specific purposes only
- Ensuring that personal data is available and accessible in case of physical or technical issues
- Regular testing and evaluation of technical and organizational security measures

How bot threats can potentially lead to GDPR violations

We have observed that in preparation for GDPR compliance, the Security and Legal teams at many organizations often overlooked certain technical vulnerabilities in their data transmission, storage, and processing systems. These vulnerabilities allow malicious parties (including criminals, businesses, and even the governments of some nations) to deploy bots and malware to steal data from websites and mobile apps. The stolen data is often sold by criminals through 'darknet' marketplaces, or used in various illegal ways to commit theft, fraud, and espionage.

It would be legally and financially prudent for organizations that obtain or handle EU residents' personal data to examine some of the various attack vectors which could expose individual data owners' privacy to undue risks. While there exists a multitude of ways for nefarious parties in general to illegally obtain personal data, this report focuses on the compliance risks posed by malicious bots in particular.

As bot mitigation specialists, we are frequently approached by enterprises that are experiencing the negative business impact caused by bots. With the onset of the GDPR, businesses are increasingly concerned with the risks posed by bots that can steal personal data. Radware Bot Intelligence lists a growing number of threats that can potentially lead to personal data theft, including key threats such as:

Account Takeover: accomplished by bots using credential stuffing or brute-force techniques, which expose users' personal data to theft and other crimes.

Carding: a major risk factor through which personal information associated with credit and gift cards can be stolen by bots that attack websites with payment portals.

Content Scraping: escalating attacks on media and e-commerce sites, financial portals, classified directories, etc. are increasingly putting personal data at risk of being stolen for fraudulent purposes.

Digital Ad fraud: impacts advertisers and publishers, and potentially lets bots steal users' behavior-based cookies which can then be traced back to reveal identities. Unprotected session data can also make cookies vulnerable to malicious bots, hence this constitutes a critical path that leads to breach of PII.

Common vulnerabilities exploited to obtain personal data

Reverse engineering and encryption vulnerabilities

Fraudsters can potentially reverse-engineer your site URL structure using multiple scraping tools (such as Firebug, Wireshark, and Charles Proxy) to find vulnerable pages which may contain PII, even if the information therein is encrypted with advanced encryption methods such as MD5 (which can be broken). Scraping tools produce large volumes of automated traffic on web assets, but advanced bot detection solutions can help identify and block such automated attacks.

Credential stuffing tools

Attackers are increasingly deploying sophisticated cracking tools (such as Sentry MBA) that facilitate hacks on login pages. These malefactors exploit the propensity of internet users to reuse login credentials across websites that they use. A great deal of personal data is consequently exposed to fraudsters. Web Application Firewalls and conventional bot detection techniques cannot detect these 'low and slow' attacks from sophisticated bots and malware. A bot mitigation solution with device fingerprinting and advanced machine learning-based behavior analysis capabilities is essential to defend against such attacks.

Bot mitigation can help ensure GDPR compliance

While we have listed a few attack vectors often targeted by bots to obtain personal data, there are many other data sources which can be exploited by bad bots even if your enterprise follows the security formalities and procedures required by the GDPR regulations. Robust application security that respects 'privacy by design' – right from the design stage to post-deployment, is one of the first key steps that your organization can take to ensure the privacy of personal data. Being compliant with PCI-DSS, HIPAA, SOC-I & II (and other major security regulations on data in-transit and data at rest) should not lead to a sense of complacency when it comes to GDPR compliance.

Safeguarding personal data is good for businesses. Companies that protect personal data enjoy the continued trust and loyalty of their customers and users. Failure to mitigate bots may lead to situations where the personal data of individuals can be stolen. Under the GDPR mandates, such situations may potentially lead to regulatory scrutiny, litigation – and in the worst-case scenario – make your organization potentially liable for steep penalties, in addition to damage to your brand and reputation.

Recommendations

Radware Bot Manager recommends that every type of organization that obtains, stores, transmits, and uses EU residents' personal data carry out a holistic security review to ensure GDPR compliance.

- Confirm that users clearly provide consent to usage of their data, and collect only data that is required for business purposes.
- Enterprises that use third-party technology platforms (such as e-commerce platforms, payment processors, geo-location services, etc.) should ensure that every aspect of their interfacing systems that collect, store, and process personal data with and through such platforms is protected from bot attacks.
- Inspect for vulnerabilities that can be exploited by bots to steal personal data.
- Securing hardware and software systems from malware in general requires multiple layers of security protocols and processes, but advanced anti-bot solutions in particular can be implemented relatively easily using integration options such as JavaScript, APIs, and VMs.
- Bot threat mitigation to protect against breaches of personal data is one of the most crucial defenses for enterprises and other organizations to ensure that a Zero-Day attack doesn't lead to potential GDPR violations.

1) Full text of the GDPR Regulation:
data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

About Radware

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, acquired ShieldSquare in March 2019. ShieldSquare is now Radware Bot Manager.

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.