**Grey Wizard - новий гравець на ринку ІБ, що пропонує інноваційний захист**

**Захист веб-ресурсів: нові технології та рішення**

За даними досліджень, кіберзлочини входять в ТОП-3 корпоративних ризиків. Вони ж позиціонуються і як найбільш значний ризик для підприємств в довгостроковій перспективі.

В інтернет-епоху захист веб-сайтів від кібератак повинен бути головним пріоритетом для будь-якого онлайн-бізнесу, а також для всіх компаній, що обробляють конфіденційні дані або проводять фінансові операції. Надійна система безпеки веде до більшої довірі з боку клієнтів та економії коштів у разі фактичної атаки.

Для побудови надійної системи захисту веб-додатків потрібні як установка і налаштування складного устаткування великої вартості, так і участь кваліфікованих фахівців, які в свою чергу коштують досить недешево. Web Application Firewal (WAF) дозволяє запобігти крадіжці персональних даних, фінансовим махінаціям та промисловому шпигунству, надаючи інструменти для моніторингу та приведення корпоративної політики безпеки у відповідність до вимог регуляторів. Разом з тим, WAF не захищає від DDoS-атак, і тому компаніям доведеться купувати додаткове обладнання для усунення цієї проблеми. В таких умовах значний інтерес представляє комплексне і просте у використанні рішення від компанії Grey Wizard.

**Чому Grey Wizard?**

Компанія Grey Wizard з'явилася на ринку відносно недавно. Вона була створена у відповідь на реальні проблеми, пов'язані зі збільшенням рівня складності кіберзагроз та чисельності кіберзлочинців. Команда Grey Wizard складається з професіоналів польського інтернету, в тому числі менеджерів з повним розумінням бізнес-процесів електронної комерції, та інженерів, що спеціалізуються на найсучасніших технологіях. Деякі з них брали участь в розробці і захисті Allegro Group, однієї з найбільших європейських гравців електронної комерції і рекламних послуг OLX Group. Це справжні ентузіасти і експерти, що володіють глибокими знаннями в області кібербезпеки. Не випадково основний пріоритет компанії - забезпечення першокласного захисту від кібератак.

Незважаючи на досить молодий вік, компанія відмінно зарекомендувала себе на світовому ринку ІБ, випустивши кілька унікальних продуктів для захисту від кібератак. У цій статті ми розглянемо тільки один з модулів рішення Grey Wizard Shield - систему захисту від спеціалізованих атак на веб-додатки. Продукт забезпечує ефективний захист від багатьох видів кібератак, включаючи волюметричні атаки. Технологія, заснована на машинному навчанні, забезпечує високу ефективність і допомагає швидко виявляти будь-які потенційні загрози. У другій статті ми торкнемося тематики захисту від DDoS-атак за допомогою продукту Grey Wizard.

**Машинне навчання в кібербезпеці**

Сьогодні захист від кібератак вимагає технологічно просунутих рішень, здатних не тільки відбивати атаки в реальному часі, але перш за все детектувати погрози і ефективно захищати веб-сайти та додатки. Для надійного захисту від кібератак розробники Grey Wizard використовують алгоритми, засновані на технології машинного навчання (МН). МН тісно пов'язане з штучним інтелектом і використовує дуже просунуті алгоритми, здатні поліпшити систему захисту, використовуючи аналітику зібраних даних.

Ефективність Grey Wizard Shield в значній мірі обумовлена інтелектуальними алгоритмами МО. Синергія знань експертів в області кіберзахисту світового рівня і механізмів машинного навчання дозволяє продукту детектувати всі можливі аномалії через всебічний моніторинг веб-додатків і виявлення небезпечних запитів з мережі.

Алгоритми МО дозволяють завжди бути на крок попереду кіберзлочинців, адже вони виявляють навіть ті методи атаки, які ще не були ідентифіковані. Крім того, вони здатні розпізнавати атаки, що не виявляються традиційними системами на основі правил.

**Моніторинг веб-додатків і відображення атак**

Алгоритми, що використовуються в Grey Wizard Shield, виконують детальний аналіз мережевого трафіку, яким обмінюються клієнтський пристрій і веб-додаток. Взявши за основу перелік з кількох параметрів, Grey

Wizard визначає тип трафіку і його динаміку, що дозволяє виявляти будь-які аномалії і в той же час мінімізувати ризик помилкових попереджень.

Таким чином, моніторинг додатків в реальному часі дозволяє команді Grey Wizard негайно реагувати на будь-які загрози, пов'язані з атаками на додатки клієнтів.

Grey Wizard WAF аналізує всі HTTP-запити в реальному часі, перевіряючи їх на відповідність декільком правилам безпеки. Якщо виявлена підозріла спроба маніпулювання даними, запит блокується і не досягає цільового сервера. Тому клієнти, які використовують WAF, захищені від можливих негативних наслідків спроб вторгнення. Той же метод застосовується для захисту клієнтів з використанням програмного забезпечення з відкритим кодом (Wordpress, Joomla, osCommerce), яке особливо схильне до вразливостей нульового дня, які часто з’являються в різних додатках або плагінах.

Особливо слід відзначити функції ідентифікації небезпечних запитів. Grey Wizard Shield використовує інтелектуальні алгоритми для аналізу запитів, що генеруються користувачами, забезпечуючи тим самим високий рівень захисту від таких атак, як SQL-ін'єкції, міжсайтовий скриптинг (XSS) або включення локального файлу (Local file include, LFI).

Крім того, продукт захищає від неправильної конфігурації, неадекватного захисту конфіденційних даних та контролю над дозволами користувачів і т.д.

Підводячи підсумки, слід сказати, що Grey Wizard аналізує вхідний трафік, використовуючи безліч методів одночасно. Завдяки цьому він може успішно виявляти і блокувати будь-який нерегулярний трафік, що створюється ботами і скриптами, тим самим захищаючи як веб-сайт, так і його користувачів. Важливо відзначити, що правила розробляються селективно, щоб мінімізувати помилкові спрацьовування.

**Простота підключення**

Щоб активувати захист від кібератак, не потрібні спеціальні навички програмування. Інтеграція і розгортання служб займає всього 15 хвилин. Цей час, присвячений активації Grey Wizard Shield, є важливим етапом щодо забезпечення безпеки вашої компанії.

**Додаткові переваги - CDN для всіх клієнтів**

Мережа доставки контенту (CDN) - це масштабна розподілена система для передачі інформації між багатьма дата-центрами і точками обміну трафіком в Інтернеті. Її кінцева мета - зробити вміст сторінки доступним в найкоротший час для кінцевого користувача.

CDN, що входить до складу Grey Wizard, надає цілий набір переваг для замовника. По-перше, трафік на захищені веб-сайти проходить через інтелектуальну розподілену мережу. Ця служба заснована на механізмі Anycast, який направляє кінцевих користувачів на найближчий сайт, на якому доступні запитані ресурси.

По-друге, передача контенту для відвідувачів сторінки може бути автоматично оптимізована. На практиці це означає, що користувачі будуть отримувати статичні дані, з кешу на серверах Grey Wizard. Таке кешування особливо важливо для графіки, таблиць стилів CSS і файлів Javascript, що використовуються на сторінках.

По-третє, дані, передані відвідувачам веб-сайту, додатково стискаються і позначаються так, що браузер зберігає їх локально в кеш-пам'яті замість повторного завантаження (якщо дані не були змінені).

Крім того, служба CDN активує захист веб-сторінки від мережевих і орієнтованих на додатки атак, блокуючи доступ шкідливих ботів, які споживають пропускну здатність і обчислювальні ресурси облікового запису хостингу.

Отже, Grey Wizard Shield є сучасним і технологічно просунутим рішенням для захисту веб-ресурсів від різного роду атак. Серед переваг рішення - високий рівень виявлення загроз, простота підключення і налаштування. Є також додаткові приємні бонуси - мережа доставки контенту, доступна для всіх замовників рішення. Крім того, в Grey Wizard Shield присутній хмарний захист від DDoS-атак. Більш докладно про цей інструмент ми поговоримо в наступній статті.