ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки, доктор фізико-математичних наук,
доктор юридичних наук, професор

РАЧУК ВАЛЕРІЙ ОЛЕКСАНДРОВИЧ

Національний університет «Одеська юридична академія»,
асистент кафедри кібербезпеки

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО: ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА БЕЗПЕКА В ПРОЯВАХ НОВІТНІХ ТЕНДЕНЦІЙ

Широке використання інформаційно-телекомунікаційних технологій в усіх сферах суспільного життя породжує новітні технології, які потребують вирішення питань кібербезпеки. Це, в свою чергу, веде до розмежування і цієї галузі, де випереджаючі темпи мають інформаційні технології. При цьому інформаційна безпека відокремилася від телекомунікаційної в самостійну галузь зі своєю специфікою і своїм обладнанням, а забезпечення інформаційної безпеки стало одним з головних завдань сучасного суспільства, зокрема завдяки стрімкому розвитку саме інформаційних технологій і обладнанню, що використовується. Загрозу безпеці можуть представляти не лише технічні збої, але і неузгодженість даних в різних облікових системах, а також розподіл і швидкість передачі інформації та «людський» фактор. Тут, до речі, слід звернути увагу на новітній, поки ще маловідомий клас пристроїв, котрі стоять на межі телекомунікаційної та інформаційної безпеки, забезпечуючи її, а саме, на появу такого феномена як брокери мережевих пакетів (Network Packet Broker). Вони стали балансувальниками навантаження і виступають як спеціалізовані (моніторингові комутатори, агрегатори трафіку, Security Delivery Platform, Network Visibility). Брокери мережевих пакетів представляють собою спеціалізовані пристрої, які знайшли найбільше застосування в сучасних системах саме інформаційної безпеки. Такий клас пристроїв відносно новий і поки ще небагаточислений в загальноприйнятій мережевій інфраструктурі, в порівнянні з комутаторами, маршрутизаторами і т.д. Лідером в розробці даного типу пристроїв стала американська компанія Gigamon.

На теперішній час учасників, так званих «гравців», на цьому ринку, стало значно більше (в тому числі подібні рішення є у відомого виробника тестових комплексів – компанії IXIA), але про існування таких пристроїв, як і раніше, знає лише вузьке коло професіоналів. Слід зазначити, що навіть в питаннях термінології поки немає однозначної визначеності: назви варіюються від «системи забезпечення прозорості мережі» до простого – «балансери».

Під час розробки брокерів мережевих пакетів, виникли деякі особистості в тому, що окрім аналізу напрямків розвитку функціоналу та

випробувань в лабораторіях, в так званих тест-зонах, для потенційних споживачів, необхідно одночасно пояснювати про існування такого класу обладнання, оскільки, поки що, не всі знають про нього. Орієнтовно 15-20 років тому трафіку в мережі було ще мало, і це були переважно незначні дані. Безпосередньо закон Нільсена практично повторює закон Мура: швидкість інтернет – з'єднання збільшується щорічно приблизно на 50%. В свою чергу, промисловість відразу ж відгукнулася на це появою цілого спектру новітніх пристроїв для здійснення глибокого аналізу безпосередньо самого трафіку (DPI): починаючи з систем запобігання DDOS-атак, закінчуючи, включно, системами управління подіями інформаційної безпеки, такими, як: IDS, IPS, DLP, NBA, SIEM, Antimailware, тощо. Зазвичай, кожна з цих складових – це програмне забезпечення, яке встановлюється безпосередньо на серверну платформу. Причому кожна програма, так званий засіб аналізу, встановлюється на свою серверну платформу, а це означає, що: виробники програмного забезпечення різні, а значить обчислювальних ресурсів для аналізу на рівні L7 потрібно багато.

При побудові системи гарантованої інформаційної безпеки конче необхідно вирішити ряд проблемних задач, які автори сформулювали наступним чином: яким чином передавати сам трафік з мережевої інфраструктури на системи аналізу (в сучасній інфраструктурі розроблених для цього SPAN-портів поки що недостатньо ні за кількістю, ні за продуктивністю); яким чином розподіляти трафік між різними системами, котрі будуть здійснювати аналіз; яким чином здійснювати масштабування системи в разі, якщо буде недостатньо продуктивності одного комплекту аналізатора під час обробки всього обсягу трафіку, що надходить в нього; яким чином ефективно здійснювати моніторинг інтерфейсів 40G/100G, а в недалекому майбутньому вже 200G/400G, враховуючи той факт, що сам факт аналізу, на сьогоднішній час, підтримують тільки інтерфейси лише 1G/10G/25G. Виходячи з цього випливають ще такі супутні задачі: яким чином мінімізувати безпосередньо нецільовий трафік, що не потребує обробки, але потрапляє на засоби, які призначені для аналізу, цим самим витрачаючи їх ресурси; яким чином обробляти так звані інкапсульовані пакети та пакети, що містять службові мітки самого обладнання. Ці задачі пов'язана з тим, що брокери мережевих пакетів працюють на рівні пакетів, і саме через це, вони схожі на звичайні комутатори.

Головна відмінність брокерів мережевих пакетів від комутаторів полягає в тому, що правила розподілу і агрегації трафіку в брокерів мережевих пакетів повністю визначаються безпосередньо настройками.

У брокерів мережевих пакетів немає стандартів побудови таблиць пересилання (MAC-таблиць) і протоколів обміну з іншими комутаторами (типу STP), а саме тому діапазон можливих налаштувань в них набагато ширше.

Брокер може рівномірно розподілити трафік з одного або декількох вхідних портів на заданий діапазон вихідних портів, з функцією рівномірного навантаження по виходу.

Можна створювати правила для копіювання, фільтрації, класифікації, де дуплікації і модифікації трафіку. Дані правила можна застосовувати до різних груп вхідних портів брокера мережевих пакетів, а також застосовувати послідовно один за одним безпосередньо в самому пристрої.

Слід відмітити, що важливою перевагою пакетного брокера стала можливість обробки трафіку на повній швидкості потоку зі збереженням цілісності сесій, навіть у разі балансування трафіку на кількох однотипних системах DPI.

Збереження цілісності сесій полягає в передачі всіх пакетів сесії транспортного рівня (TCP / UDP / SCTP) в один порт. Це важливо саме тому, що системи DPI (зазвичай це програмне забезпечення, яке працює на сервері, котрий підключений до вихідного порту пакетного брокера) аналізують вміст трафіку на рівні додатків, і всі пакети, що відправляються / приймаються одним додатком, повинні надходити на один і той же екземпляр аналізатора. Якщо пакети однієї сесії загубляться або розподіляться між різними пристроями DPI, то кожен окремий пристрій DPI, опиниться в ситуації, яка буде аналогічна читанню не суцільного тексту, а окремих слів з нього. Фактично, швидше за все, текст стане не зрозумілим.

Таким чином, брокери мережевих пакетів, будучи зорієнтованими на системи інформаційної безпеки, мають функціональні можливості, що допомагають підключити до високошвидкісних телекомунікаційних мереж програмні комплекси DPI, таким чином знизивши навантаження на них, що дозволить здійснити попередню фільтрацію, класифікацію та підготовку трафіку для спрощення подальшої обробки. Окрім того, оскільки брокери мережевих пакетів видають широкий перелік статистики і часто виявляються підключені до різних точок мережі, то під час діагностики проблем працездатності самої мережевої інфраструктури, вони також, так би мовити самостійно, знаходять своє місце, забезпечуючи сучасний рівень технологій, технічних засобів і послуг з безпеки.

Підсумовуючи зазначені переваги, підкреслимо прояви новітніх тенденцій і відзначимо, що вищезгадані брокери мережевих пакетів побудовані надзвичайно вдало за своїми базовими функціями. Сама назва «спеціалізовані/моніторингові комутатори» з'явилася згідно до основного (базового) призначення. При цьому відбувається збір трафіку з даної інфраструктури, що здійснюється за допомогою пасивних оптичних відгалужувачів TAP і/або SPAN-портів та наступний його розподіл поміж засобами, які призначені для проведення аналізу. В разі логіка достатньо проста. Між різнотипними системами трафік дублюється (віддзеркалюється), а в разі наявності однотипних систем – відповідно балансується. Таким чином, до базових функцій входять: фільтрація по полях до L4 (MAC, IP, TCP / UDP-порт і т.д., поєднання в один декількох слабонавантажених каналів (наприклад, для обробки в одній системі DPI). Даний функціонал дозволяє забезпечити можливість рішення базового завдання тобто підключення систем DPI до інфраструктури мережі. Брокери мережевих пакетів активно розвиваються в частині надання принципово нових можливостей,

починаючи з балансування по вкладених заголовкам тунелів до дешифрування трафіку, досягають цього шляхом додавання інтерфейсів 40/100G. Обмеження, у різних виробників, базовим функціоналом брокерів, які забезпечують обробку до 32 інтерфейсів 100G на 1U, не дозволяє фізично розмістити більше інтерфейсів 1U на передній панелі. Саме тому, виникає проблема зниження навантаження на засоби аналізу, а для складної інфраструктури неможливо забезпечити навіть вимоги до базової функції. Це призводить до того, що сесія, яка розподілена по кількох тунелях, або забезпечена MPLS-маркерами, може бути розбалансована на різні екземпляри аналізатора, в результаті чого повністю випаде з аналізу. Такі моделі, на жаль, не можуть бути використані з високою Терабітною продуктивністю, але ж на їх основі існує можливість побудувати реально якісну та сучасну систему для інформаційної безпеки. В такій системі, насамперед, кожен засіб, що здійснює аналіз, гарантовано отримає інформацію, яка тільки в такій формі, яка необхідна для виконання завдань з аналізу в найбільш доступному вигляді.

Отже, прогрес в безпеці інформаційних технологій відкриває нові горизонти саме в кібербезпеці з її багатогранними можливостями.

Ключові слова: інформаційно-телекомунікаційні технології, інформаційні технології, безпека, брокери мережевих пакетів, трафік, управління, агрегатори трафіку.

Ключевые слова: информационно-телекоммуникационные технологии, информационные технологии, безопасность, брокеры сетевых пакетов, трафик, управления, агрегаторы трафика.

Key words: information and telecommunication technologies, information technologies, security, network packet brokers, traffic, management, traffic aggregators.

ЗАДЕРЕЙКО ОЛЕКСАНДР ВЛАДИСЛАВОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

ЗАХИСТ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ГРОМАДЯН

Сучасна людина не може повністю вимкнутися з інформаційного обміну. Це приводить до обмеження її когнітивних можливостей і як наслідок, до втрати її особистого інформаційного суверенітету. Перебуваючи під впливом інформаційних потоків, вона піддається різним погрозам: синдрому інформаційної втоми, інформаційної поразки, відкритості до маніпуляції свідомістю.

Цей беззаперечний факт обумовлює два найбільш актуальних завдання, які стоять перед кожною людиною – вибирати з інформаційного мейнстріму тільки ту інформацію, яка дозволить протидіяти інформаційному ураженню і як наслідок – маніпуляції свідомістю через інформаційну дію [1, с. 74].