ЕСЛИ НЕ КОНТРОЛИРОВАТЬ СВОЙ ПЕРИМЕТР, ЕГО БУДУТ КОНТРОЛИРОВАТЬ ДРУГИЕ

ПИЛОТНЫЕ ПРОЕКТЫ РЕШЕНИЯ F6 ASM КАЖДЫЙ РАЗ ВЫЯВЛЯЮТ ПРОБЛЕМЫ НА ПЕРИМЕТРЕ, О НАЛИЧИИ КОТОРЫХ НИКТО НЕ ДОГАДЫВАЛСЯ

Николай СТЕПАНОВ
технический руководитель F6 Attack Surface Management

Владимир СОЛОВЬЕВ
руководитель группы внедрения систем защиты от атак АО «ДиалогНаука»

Бурный рост компаний, слияния-поглощения, текучка кадров, а иногда банальное безразличие к контролю своего внешнего периметра приводят к появлению множества «мёртвых», так называемых теневых активов. А поскольку любая хакерская атака начинается с разведки, киберпреступники в первую очередь ищут оставленное без присмотра сетевое оборудование — то, которое уже устарело, не контролируется, но всё же обладает доступом к корпоративной сети, или уязвимые сервисы, которые также не обновлялись длительное время, но всё ещё имеют принадлежность к корпоративной сети.

Довольно часто заказчики приходят с вопросом: как усилить свою кибербезопасность без значительных затрат времени и средств? Рекомендация одна — начать с внедрения системы управления поверхностью атаки (Attack Surface Management, ASM). В этой статье мы поговорим о том, что такое ASM, и на примере одного из лидеров отечественного рынка выясним, какие задачи решают системы класса ASM и куда вообще движется рынок решений данного класса.

ЗНАКОМСТВО С ASM

Понимание того, что именно надо защищать и какие элементы уязвимы, — первый шаг на пути к последовательной и эффективной стратегии защиты.

F6 Attack Surface Management (F6 ASM) — это комплексное информационно-аналитическое SaaS-решение, предназначенное для оценки поверхности атаки компании. Оно позволяет отслеживать незащищённые участки внешнего периметра, потенциальные уязвимости, теневые активы и некорректно настроенные элементы сети, которые потенциально могут быть использованы злоумышленниками в кибератаках (рис. 1).

Система позволяет выявить активы с высоким уровнем риска, выделить слабые места организации и соответствующим образом исправить ситуацию с целью предотвращения атак.

Достигается это путём применения множества различных сканеров (как с открытым кодом, так и самописных), которые позволяют обнаруживать забытые активы, устаревшее и уязвимое ПО, открытые порты и т.д. А глубокая интеграция с системой кибермразведки — F6 Threat Intelligence (F6 TI) — позволяет подсвечивать упоминания в дарквебе и активность ВПО, направленного на периметр компании.

F6 ASM — это полностью отечественная разработка. Хранение данных клиентов F6 осуществляется исключительно на территории России. Установка не требуется, система настраивается в несколько кликов.

Как появился данный продукт? Из «графа».

НАСЛЕДНИК ГРАФА

История F6 ASM уходит корнями к другой разработке компании — графу сетевой инфраструктуры. Это запатентованная технология системы кибермразведки — F6 TI, которая позволяет визуализировать связи между доменами, IP, сервер-сертификатами, злоумышленниками и сообщениями в дарквебе (рис. 2).

Изначально граф создавался для проведения расследований — это крайне полезный инструмент, чтобы распутать сложную атаку, деанонимизировать злоумышленника или найти инфраструктуру злоумышленников. Именно так он и использовался, пока не было замечено, что пользователи решения ищут не IP-адреса преступников, а заносят свои, чтобы найти связи.

Поэтому вопрос «если мы и так сканируем весь интернет и строим связи, почему бы нам не помочь клиентам держать их внешнюю инфраструктуру под контролем?» оказался для разработчиков F6 ASM абсолютно логичным.

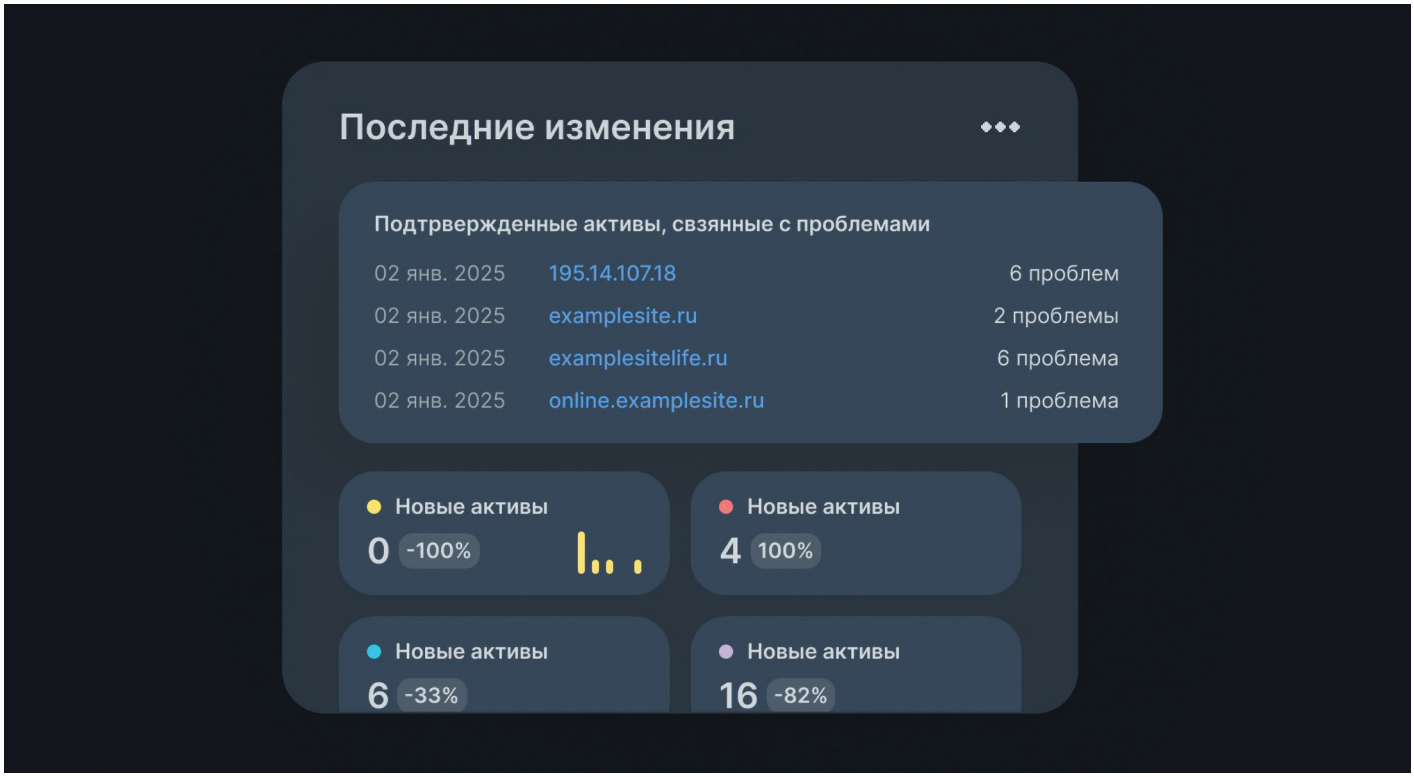

Рисунок 1. Обнаружение используемых и забытых теневых активов

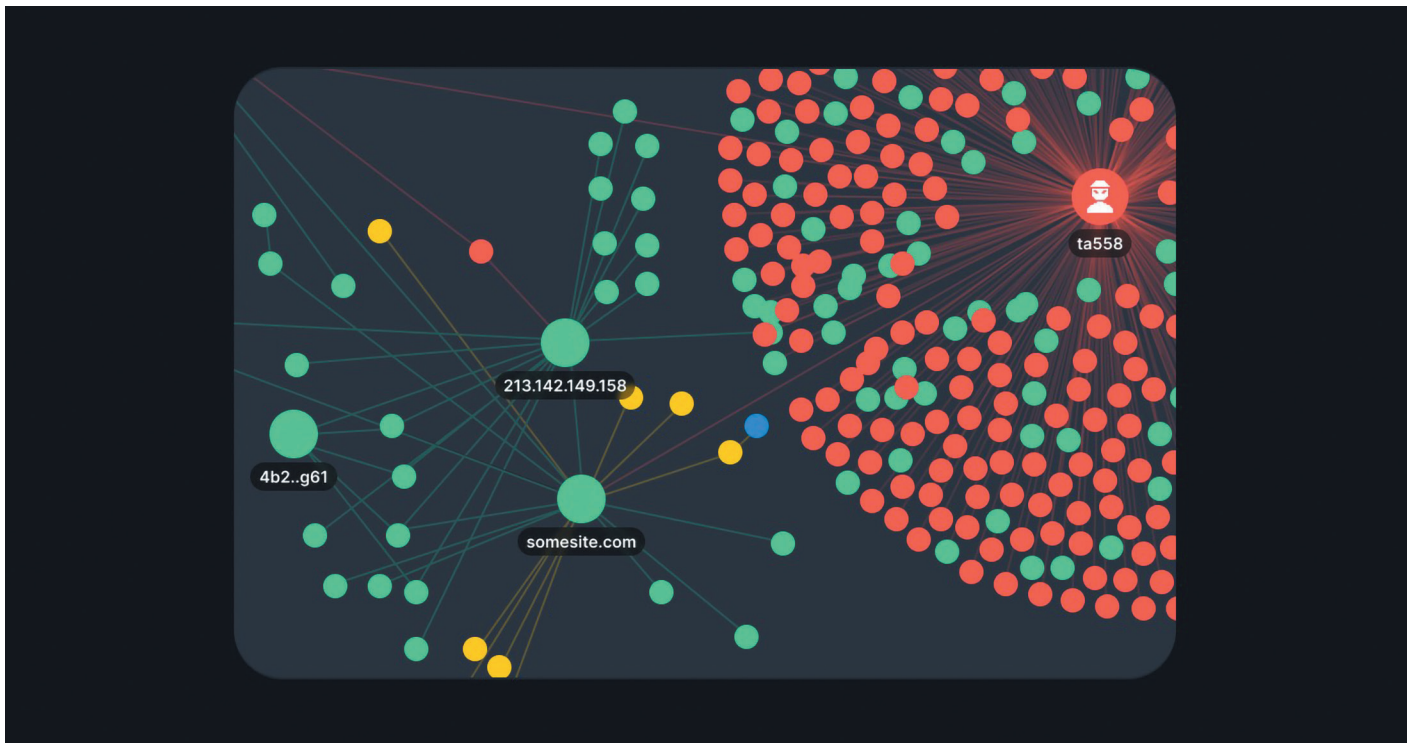

Рисунок 2. Графовый анализ сетевой инфраструктуры

АВТОМАТИЗАЦИЯ ЗАЩИТЫ ПЕРИМЕТРА

Со временем продукт технически развивался, но его суть оставалась неизменной. F6 ASM имеет восемь категорий, по которым проводит ежедневные проверки. Каждый день эксперты F6 сканируют всю сеть Интернет и находят домены, IP-адреса, SSL-сертификаты, которые могут быть связаны с клиентом. После этого происходит проверка всех доменов и IP-адресов на предмет уязвимого ПО, сопоставляя версии ПО и известные уязвимости, открытые порты, небезопасные заголовки на сайтах и почтовые записи (Dmarc, SPF). Также происходит обогащение данными киберразведки от системы F6 TI, чтобы найти упо-

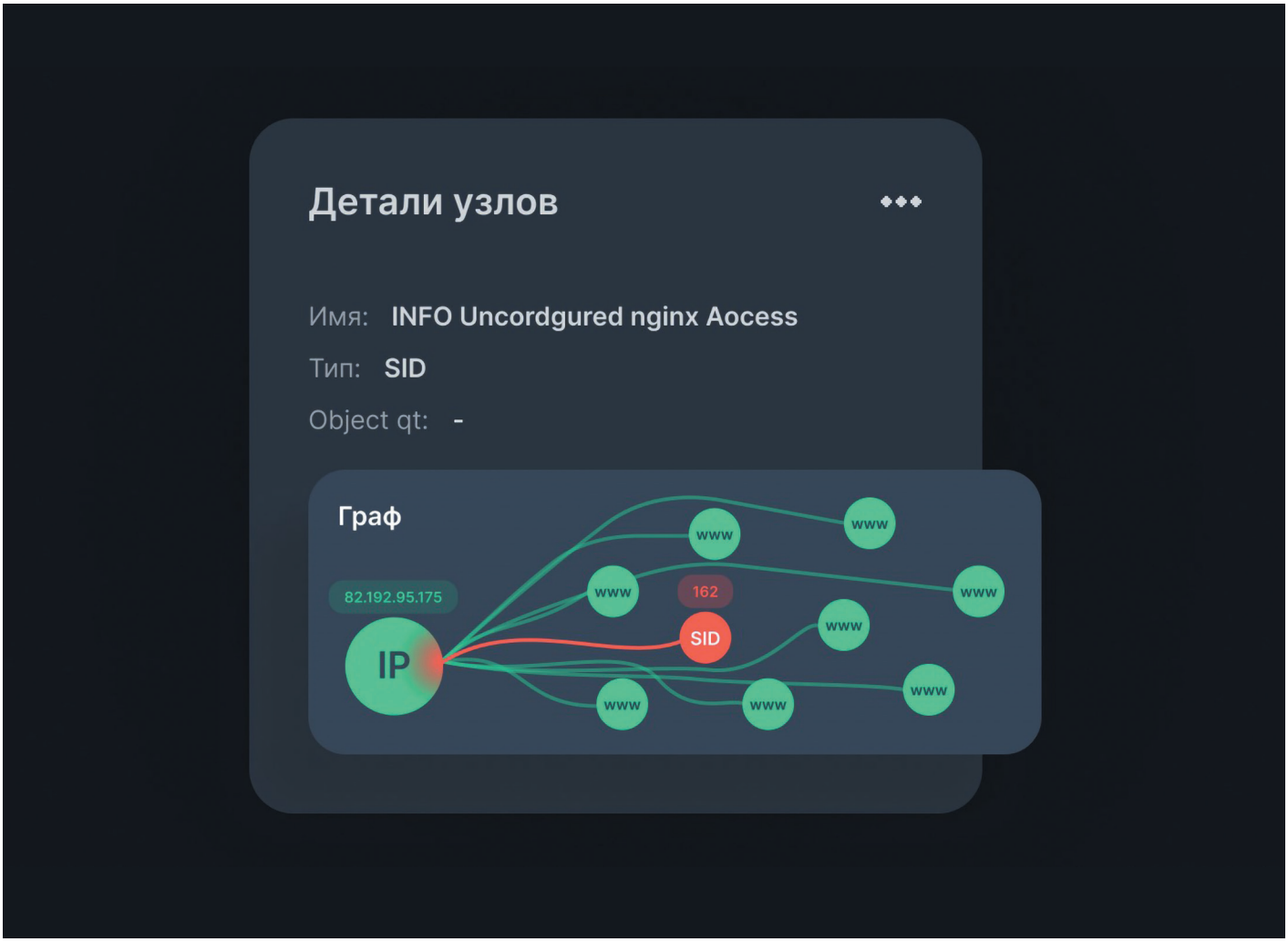

Рисунок 3. Непрерывный мониторинг всех изменений во внешней поверхности атаки

минание доменов или IP на хакерских форумах или внутри конфигов ВПО (рис. 3).

Улучшая стабильность и скорость работы, эксперты F6 не переставали учитывать пожелания клиентов. Многие использовали F6 ASM для того, чтобы автоматизировать свою защиту периметра. Исходя из этого, к системе стали привлекаться аналитики Центра кибербезопасности (CDC), чтобы оперативно помогать клиентам устранять проблемы на периметре. Для тех, кто не хочет, чтобы кто-то, кроме их сотрудников, изучал проблемные точки компании, F6 выпустили обучающие курсы.

Наша основная цель — автоматизация защиты периметра. Когда от клиента требуется провести только определённую работу, а он уже знает, где проблема, что это за проблема, что нужно сделать, чтобы её решить.

ПЕРСПЕКТИВЫ ASM

Исходя из текущих запросов рынка, F6 начали готовиться к релизу активного сканирования. Сейчас F6 ASM работает таким образом, чтобы не «нагружать систему». Эксперты заметили высокий спрос на «активное сканирование», когда система автоматически пытается эксплуатировать известную CVE. Данную потребность доработали, и тем самым в системе появится возможность вносить собственный код, который будет автоматически отрабатывать по всем активам клиента.

Также на текущий момент имеется огромный спрос на on-prem-решения. Для этого решение F6 ASM пересобрали таким образом, чтобы оно могло быть запущено на серверах клиента и только клиент мог получить доступ к своим просканированным данным. Это позволяет обезопасить клиента от передачи внутренней информации за пределы компании.

Подводя итоги, суммируем: решения класса Attack Surface Management, в частности решение F6 ASM, обеспечивают полный мониторинг всех известных и неизвестных активов клиента, доступных извне, и позволяют эффективно реагировать на новые уязвимости и атаки до того, как они приведут к серьёзным последствиям. Для запуска от пользователя системы требуется лишь указать цели сканирования и далее только ожидать результата.

Пилотные проекты решения F6 ASM у наших заказчиков каждый раз выявляют проблемы на периметре, о наличии которых никто не догадывался. Поэтому необходимо постоянно контролировать внешний периметр и эффективно его защищать перед современными киберугрозами.