ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Attack Surface Management»

Описание функциональных характеристик

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Описание
ВПО	Вредоносное программное обеспечение
Заказчик	Лицо, заключающее договор на ПО
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ»; • Компанией-интегратором, по выбору Заказчика
ПО	Программное обеспечение «F6 Attack Surface Management»
Разработчик	АО «БУДУЩЕЕ»
СЗИ	Система Защиты Информации
Угроза или Киберугроза	Потенциально возможное происшествие, преднамеренное или нет, которое может оказать нежелательное воздействие на систему или хранящуюся информацию
API (Application Programming Interface)	Программный интерфейс, то есть описание способов взаимодействия одной компьютерной программы с другими
Brut	Метод взлома учетных записей и шифров путем перебора комбинаций паролей и ключей
Darkweb (даркweб)	«Темная сеть», скрытая анонимная сеть интернета, где действуют злоумышленники, а также форумы в открытом Интернете, посвященные хакерской тематике
DDoS-атака (Distributed Denial of Service)	Атака, целью которой является перегрузка сетевых ресурсов, делая их недоступными для их законных пользователей
DMARC (Domain-based Message Authentication, Reporting and Conformance)	Техническая спецификация, созданная группой организаций, предназначенная для снижения количества СПАМа и фишинговых электронных писем
DNS (Domain Name System)	Компьютерная распределенная система для получения информации о доменах
DNSSEC (Domain Name System Security Extensions)	Набор расширений IETF протокола DNS, позволяющих минимизировать атаки, связанные с подменой DNS-адреса при разрешении доменных имён
Exploit	Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему

Термин	Описание
Fuzzing	Метод тестирования программного обеспечения, который заключается в автоматической генерации и отправке случайных или данных в программу с целью выявления непредусмотренных ситуаций, таких как сбои, зависания или ошибки безопасности
JS-снифферы	Вредоносный код, внедряемый злоумышленниками для перехвата вводимых пользователем данных: номеров банковских карт, имен, адресов и т.д.
RDP (Remote Desktop Protocol)	Протокол, использующийся для обеспечения удалённой работы пользователя с сервером, на котором запущен сервис терминальных подключений
SaaS (Software as a Service)	Модель обслуживания, при которой программное обеспечение размещено в облачной инфраструктуре
SIEM (Security Information and Event Management)	Программные продукты для сбора и анализа информации о событиях безопасности. Используются для мониторинга событий и предотвращения инцидентов в режиме реального времени
SOAR (Security Orchestration, Automation and Response)	Продукты для оркестровки систем безопасности, то есть их координации и управления ими. Решения SOAR нужны для сбора данных о событиях безопасности, их обработки и автоматизации типовых сценариев реагирования
SPF (Sender Policy Framework)	Расширение для протокола отправки электронной почты через SMTP
SSH (Secure Shell)	Сетевой протокол, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL	Сертификат, поддерживающий старые алгоритмы с известными уязвимостями безопасности.
TLS	Сертификат, использующий современные алгоритмы шифрования
URI (Uniform Resource Identifier)	Последовательность символов, идентифицирующая абстрактный или физический ресурс
URL (Uniform Resource Locator)	Механизм, используемый браузерами для получения любого опубликованного во Всемирной сети ресурса
VPN (Virtual Private Network)	Обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети
WHOIS	Сервис для получения информации о регистрации доменов, например, дату регистрации и возраст домена, или узнать контакты, по которым можно связаться с организацией или человеком, чей домен вас заинтересовал

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Аннотация

Настоящий документ содержит описание функциональных характеристик программного обеспечения «F6 Attack Surface Management» (далее – ПО, Система, Attack Surface Management, ASM).

1.2 Назначение ПО

«F6 Attack Surface Management» (ASM) — это комплексная информационно-аналитическая система, предназначенная для всесторонней оценки поверхности атаки организации, включая ее цифровые активы, доступные в публичном пространстве.

Система обнаруживает активы в свободном доступе, оценивает уровень уязвимости таких активов и ранжирует их по уровню опасности, а также оповещает об активах с высоким уровнем риска для предотвращения потенциальной атаки. Для каждой найденной уязвимости Система предлагает рекомендации по исправлению.

1.3 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

Идентификация активов

– Выявление IP-адресов (IPv4, IPv6), связанных с активами компании;

– Сбор данных о развернутом оборудовании компании и сопоставление с данными об уязвимостях;

– Выявление фактов упоминания активов компании на теневых площадках сети Интернет;

– Сбор данных из форм ввода логина и пароля, связанных с активами Заказчика;

– Сбор данных, относящихся к опубликованным доменам, которые содержат преднамеренные орфографические неточности в доменном имени.

Генерация оповещений

– Сопоставление информации из образов ВПО с данными об инфраструктуре компании и оповещение в случаях, если ВПО имеет файл настроек, где затрагиваются IP-адреса, домены и другие активы компании, или же ВПО делает запрос к активам Заказчика;

– Интеграция системы оповещений через SIEM и SOAR;

Валидация активов

– Сканирование подсетей компании для определения открытых портов, служб и используемых веб-приложений;

– Отображение полной инфраструктуры компании с технической оценкой активов и уровня защищенности инфраструктуры в режиме реального времени;

– Обнаружение и анализ уязвимостей конфигураций сервисов, приложений, программного и аппаратного обеспечения, в том числе программных библиотек в активах компании;

– Поиск неточностей в конфигурации активов компании, таких как: общедоступные базы данных, файловые хранилища или списки директорий сервисов;

– Обнаружение фактов взаимодействия ВПО, проанализированных в общедоступных решениях типа “песочница”, а также проанализированных в платформах детонации, с активами компании;

– Предоставление информации о принадлежности активов компании к бот-сетям.

Отслеживание изменений

– Пассивное сканирование пространства IPv4 на предмет выявления активов инфраструктуры компании в режиме реального времени;

– Обнаружение неточностей в конфигурации DNSSEC, SPF и DMARC в активах компании;

– Выявление наличия работающего ВПО в выявленных активах компании.

– Обнаружение и анализ самоподписанных сертификатов, актуальных версий SSL/TLS и алгоритмов шифрования в активах;

– Предоставление актуальной информации о событиях фишинга, затрагивающих инфраструктуру компании;

– Выявление использования вредоносного кода типа JS-снифферы на доменах и страницах вебсайтов компании;

– Отслеживание изменений и повторные проверки уровня защищенности.

Активное сканирование

– Обнаружение уязвимостей, которые могут быть использованы злоумышленниками для несанкционированного доступа к системам;

– Применение метода Brut — нахождение слабых паролей и ключей к учетным записям клиента, работающим по протоколам SSH, FTP, HTTP, OAuth и др.;

– Применение метода Fuzzing — тестирование ПО на наличие уязвимостей и ошибок в приложениях, а также выявление скрытых файлов и каталогов;

– Применение метода Exploit — проверка безопасности ПО или сети при помощи специально созданного программного кода (эксплойта), цель которого получить контроль над системой, выявив бреши для их последующего устранения;

– Применение метода Сканирование портов — поиск открытых портов на устройствах, подключенных к сети, а также на серверах.

1.4 Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

– Internet Explorer версии 8.0 и выше;

– Google Chrome версии 4.0 и выше;

– Mozilla Firefox версии 3.5 и выше;

– Apple Safari версии 4.0 и выше;

– Opera версии 10.5 и выше;

– iOS Safari версии 3.2 и выше;

– Opera Mobile версии 11.0 и выше;

– Google Chrome for Android версии 11.0 и выше;

– Mozilla Firefox for Android версии 26.0 и выше;

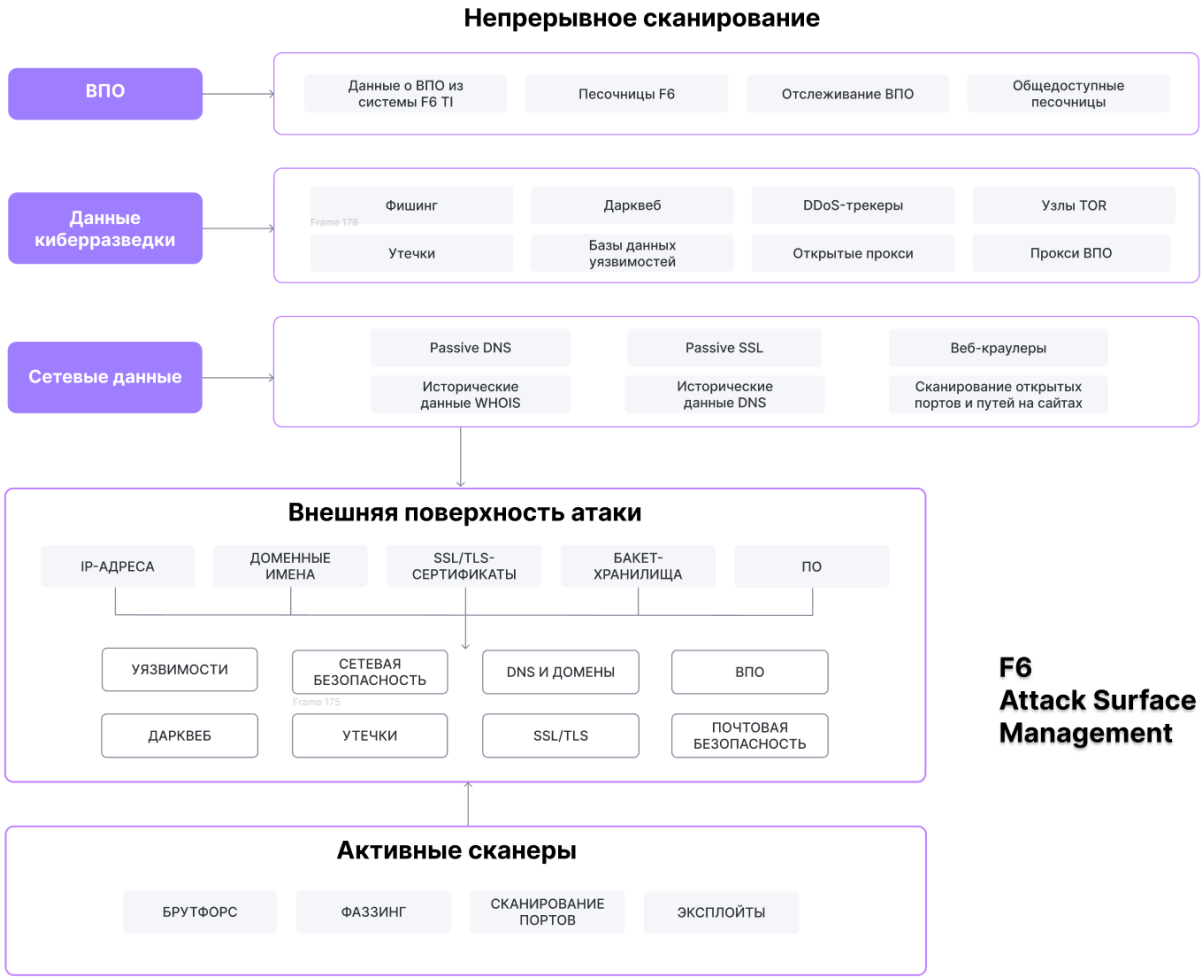
– Internet Explorer Mobile версии 10.0 и выше;

– Яндекс.Браузер версии 20 и выше;

– Microsoft Edge версии 105 и выше.

2 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

Общие принципы функционирования ПО:



Система осуществляет непрерывное сканирование открытых источников в сети Интернет с помощью различных инструментов и выявляет цифровые активы компании. При сканировании Система ищет:

- IP-адреса, связанные с компанией Заказчика;
- Данные о сетевой инфраструктуре Заказчика, используемых ПО, хранилищах и т.п.;
- Вредоносное ПО (ВПО), которое обращается к активам компании Заказчика или имеет упоминание активов компании в конфигурационных файлах;
- Упоминания компании в теневых сегментах сети Интернет (дарквеб-форумы и торговые площадки злоумышленников);
- Ресурсы с доменными именами, похожими на доменные имена компании, но имеющие преднамеренные ошибки в написании.

На основе полученных при сканировании данных Система составляет внешнюю поверхность атаки инфраструктуры Заказчика, состоящую из следующих активов:

- IP-адреса;
- Доменные имена;
- SSL/TLS-сертификаты;

- Файловые хранилища, в т.ч. облачные сервисы;
- Используемое ПО, версии используемого ПО.

Затем Система производит анализ активов, оценивает их уязвимости и потенциальный риск, а также ранжирует по уровню опасности.

Система предлагает рекомендации по устранению уязвимостей для каждого актива с проблемой. В результате анализа Система присваивает каждому активу следующие параметры:

- Текстовое и графическое превью;
- Обобщенная оценка текущих проблем, нарушений, угроз и активов, прошедших проверку безопасности;
- Детализированная информация об обнаруженном активе;
- Детальная информация об обнаруженных проблемах, нарушениях и угрозах;
- Рекомендации по устранению проблемы.

После обнаружения рисков, связанных с выявленными активами, в системе генерируется запрос к Разработчику на устранение этих рисков. Переоценка защищенности инфраструктуры внешних активов осуществляется не реже, чем 1 раз в сутки.

3 РЕАЛИЗАЦИЯ ПО

ПО «F6 Attack Surface Management» представляет из себя комплексную систему, состоящую из нескольких модулей. ПО реализовано на следующих языках программирования:

– JavaScript;

– Typescript (версия 5.1);

– Python (версия 3.9);

– Golang (версия 1.21).

Система состоит из следующих модулей:

– Модуль идентификации активов в сети Интернет;

– Модуль валидации активов;

– Модуль ручной проверки уязвимостей;

– Модуль актуализации проблем;

– Модуль уведомлений и оценки рисков;

– Модуль активного сканирования.

В рамках пользовательского интерфейса возможно выгружать отчетность об актуальном состоянии активов.

3.1 Модуль идентификации активов в сети Интернет

Модуль предназначен для поиска цифровых активов компании в сети Интернет. Модуль использует информацию об основном доменном имени компании для идентификации связанных IP-адресов, доменов и поддоменов, SSL/TLS-сертификатов, а также используемого программного обеспечения, облачных сервисов и файловых хранилищ.

Кроме того, модуль позволяет выявить теневые активы, которые наиболее подвержены риску кибератак. ПО осуществляет следующие виды сканирования (обнаружения активов):

1. Пассивное обнаружение. При пассивном обнаружении анализируются все выявляемые внешне характеристики активов (запущенное программное обеспечение, версия, открытые порты, формы входа пользователей в систему и другая базовая информация).
2. Логическое обнаружение. В рамках данного типа обнаружения объединяются разные источники информации. На основе полученных данных можно сделать предположения о возможных уязвимостях, затрагивающих активы компании. Если во время сканирования Система обнаружила не только название ПО, но и его версию, операторы Системы могут сопоставить эту информацию со списком известных уязвимостей и найти те, которым подвержен актив компании. В этом случае система создаст проблему с уровнем опасности, который зависит от CVSS уязвимости.
3. Активное обнаружение. При активном обнаружении (по умолчанию выключено, но может быть включено Пользователем) используется полезная нагрузка для сканирования на предмет наличия уязвимостей. Если в активе будет обнаружена проблема, ПО уведомит об этом в пользовательском интерфейсе.

3.2 Модуль валидации активов

Модуль проводит проверки (тесты) каждого актива для определения уровня их опасности и дальнейшей оценки уровня риска. Тесты проводятся в следующих категориях:

- Уязвимости;
- Сетевая безопасность;
- Вредоносные программы;
- Упоминания в даркбеве;
- Безопасность SSL/TLS сертификатов;
- Почтовая безопасность;
- DNS и домены.

В результате тестирования активу присваивается категория проблемы, степень (уровень) опасности, описание проблемы и причина возникновения, а также потенциальные последствия по матрице MITRE ATT&CK. Актив может получить следующий уровень опасности:

- Критическая опасность – критическая проблема, требующая срочных действий;
- Высокая опасность – проблемы могут нанести потенциально серьезный ущерб и требуют повышенного внимания;
- Средняя опасность - вероятная проблема, требующая дальнейших действий;
- Низкая опасность – незначительная ошибка;
- Успешная проверка – проблем не найдено.

3.3 Модуль ручной проверки уязвимостей

Модуль предназначен для проведения ручной проверки со стороны Пользователя найденных Системой проблем. Ручная проверка необходима, чтобы убедиться, что проблема действительно решена и актив не содержит уязвимости.

Модуль создает команду для терминала персонального компьютера Пользователя, адаптированную для каждой отдельной проблемы. Команда отображается в пользовательском интерфейсе ПО. Обратите внимание, что команды создаются только для ОС на базе Unix.

3.4 Модуль актуализации проблем

Модуль предназначен для постоянной проверки уже обнаруженных Системой активов, отслеживает изменения в цифровом отпечатке и проводит переоценку защищенности внешней поверхности атаки. Модуль ежедневно отслеживает изменения и актуализирует информацию о каждом активе. При обнаружении каких-либо изменений модуль передает данные в Систему для дальнейшей обработки. Если проблема, связанная с активом, была устранена, то при следующей проверке модуль актуализации присвоит проблеме новый статус – Решенный.

3.5 Модуль уведомлений и оценки рисков

Модуль оповещает Пользователей о выявленных событиях кибербезопасности, в которых были упомянуты активы компании. Система интегрирована с ПО «F6 Threat Intelligence».

Данные из ПО «F6 Threat Intelligence» позволяют обогатить контекстом данные Системы об активах и связанных с ними возможных угрозах и уязвимостях. Под контекстом

подразумеваются данные об IP-адресах, доменных именах, SSL/TLS-сертификатах, бакет-хранилищах и публично доступном программном обеспечении.

Дополненные контекстом данные используются Системой для оценки и приоритизации рисков.

3.6 Модуль активных сканеров

Модуль предназначен для поиска и сбора информации о цифровых активах и киберугрозах с целью их обнаружения и анализа. Это комплексный подход к информационной безопасности, который включает в себя мониторинг веб-приложений, автоматический подбор паролей к сервисам, поиск открытых портов на хостах, а также поиск уязвимостей в программном обеспечении.