ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «Group-IB AssetZero»

Версия 1.0

ОПИСАНИЕ РЕАЛИЗАЦИИ

СОДЕРЖАНИЕ

1. Аннотация

Настоящий документ содержит описание реализации программного обеспечения «Group-IB AssetZero» версии 1.0 (далее – ПО).

2. Краткое описание и назначение ПО

Group-IB AssetZero – комплексное и основанное на данных киберразведки решение по модели ПО, позволяющее организациям оценивать поверхность атаки и управлять ею. Решение обеспечивает полную видимость доступных извне активов, выявляя из них те, которые могут быть использованы в качестве вектора атаки, а также оптимизирует мероприятия по снижению рисков и ликвидации последствий с помощью интеграции, управления задачами и легкого в использовании пользовательского интерфейса.

Основными целями создания Системы являются:

- предоставление интерфейса с отображением результатов мониторинга сети Интернет;
- создание возможности взаимодействия в режиме реального времени;
- повышение качества и количества обнаруживаемых уязвимостей;
- предоставление прозрачной статистической и аналитической информации.

3. Функциональные требования к ПО

Функционал ПО должен предусматривать выполнение следующих критериев:

- Пассивное сканирование пространства IPv4 на предмет выявления активов инфраструктуры компании в режиме реального времени.
- Выявление адресов IPv6, связанных с активами компании.
- Обнаружение связей между SSL/TLS-инфраструктурой компании.
- Многоуровневый подход к построению связей между доменами, IP-адресами и активами инфраструктуры компании на основе исторических данных WHOIS, DNS и запущенных сервисов.
- Сбор данных о развернутом оборудовании компании и сопоставление с данными об уязвимостях.
- Отображение полной инфраструктуры компании с технической оценкой активов и уровня защищенности инфраструктуры в режиме реального времени.
- Обнаружение и анализ уязвимостей конфигураций операционных систем, 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 неточностей в конфигурации DNSSEC, SPF и DMARC в активах компании.
- Уведомление о предстоящих изменениях состояния TLS инфраструктуры активов (окончание действия SSL-сертификатов).
- Обнаружение и анализ самоподписанных сертификатов, актуальных версий SSL/TLS и алгоритмов шифрования в активах.
- Сканирование подсетей компании, чтобы определять открытые порты, службы и используемые веб-приложения. Сканирование не должно предполагать использование уязвимостей или загрузки какого-либо контента. Сканирование должно проводиться в “скрытом режиме”, подразумевающем отсутствие обнаружения факта сканирования со стороны СЗИ компании. Сканирование должно выявлять открытые порты служб удаленного администрирования (RDP,

SSH, VPN и т.п.), порты баз данных, небезопасные заголовки служб, открытые прокси-серверы, запущенные узлы Tor, а также то, был ли актив целью DDoS-атаки.

- Выявление фактов похищения аутентификационных данных, связанных с обнаруженными активами компании с помощью ВПО или фишинга.
- Выявление наличие аутентификационных данных компании в опубликованных в общем доступе или на теневых площадках, взломанных базах данных сторонних сервисов, имеющих возможное отношение к обнаруженным активам компании.
- Обнаружение фактов взаимодействия ВПО, проанализированных в общедоступных решениях типа “песочница”, а также проанализированных в платформах детонации, с активами компании.
- Выявление наличия работающего ВПО в выявленных активах компании.
- Выявление фактов упоминания активов компании в теневых площадках сети Интернет.
- Сопоставление информации об образцах ВПО с инфраструктурой компании и оповещение в случае, если ВПО имеет файл настроек, где затрагиваются IP-адреса, домены и другие активы компании.
- Предоставление актуальной информации о событиях фишинга, затрагивающих инфраструктуру компании.
- Выявление использования вредоносного кода типа JS-снифферы на доменах и страницах веб-сайтов компании.
- Предоставление информации о принадлежности активов компании к бот-сетям.
- Интеграция системы оповещений через API с системами тикетов, SIEM и SOAR;
- Отслеживание изменений и повторные проверки уровня защищенности.

4. Эксплуатационные требования к ПО

В ходе эксплуатации решения должны выполняться следующие требования:

- Совместимость — решение должно быть совместимо с наиболее популярными программно-аппаратными средами (указаны в п.5 «Программно-аппаратные среды функционирования ПО);
- Универсальность — возможность использования поисковых и ключевых слов и выражений для осуществления настроек поиска на различных типах площадок сети Интернет, указанных в п.3 «Функциональные требования к ПО»;
- Обеспечение точности полученных результатов — осуществление многоэтапных проверок наличия текстовых/графических данных на страницах площадок сети Интернет.
- Надежность — обеспечение бесперебойной работоспособности ПО не ниже 95% времени на протяжении года.

5. Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

- Windows Internet Explorer версии 11.0 и выше
- Google Chrome версии 8.6.395 и выше
- Mozilla Firefox версии 82.0.1 и выше
- Apple Safari версии 14.0 и выше
- Opera версии 10.5 и выше
- iOS Safari версии 14.0 и выше
- Opera Mobile версии 10.0 и выше
- Google Chrome for Android версии 11.0 и выше
- Mozilla Firefox for Android версии 82.0 и выше
- Windows Internet Explorer Mobile версии 10.0 и выше

6. Общие принципы функционирования ПО

Система осуществляет непрерывный поиск и выявление активов компании, производит их анализ и категоризацию, оповещает об угрозах и нарушениях и выполняет оценку рисков. Результатом анализа являются следующие параметры, доступные в теле объекта (актива):

- текстовое и графическое превью;
- графические виджеты, отображающие обобщенную оценку текущих проблем, нарушений, угроз и активов, прошедших проверку безопасности;
- детализированная информация об обнаруженных активах, проблемах, нарушениях и угрозах;
- обнаруженные проблемы;
- обнаруженные активы — доменные имена, сертификаты SSL/TLS, IP-адреса, подсети, общедоступное ПО, формы ввода учетных данных;
- кнопки для скачивания csv файла;
- блок графа с детализированной информацией об активах компании и связях между ними;
- блок компаний (для управления отображением инфраструктуры компании и отдельных дочерних предприятий).

После обнаружения рисков, связанных с выявленными активами, в системе генерируется тикет на устранение этих рисков. Возможно ведение тикета, присвоение различных рабочих ему статусов. Переоценка защищенности инфраструктуры внешних активов осуществляется не реже, чем 1 раз в сутки.

7. Реализация ПО

Система состоит из следующих модулей:

- модуль идентификации активов в сети Интернет;
- модуль валидации активов;
- модуль уведомлений и оценки рисков.

В рамках предоставляемого интерфейса операторы системы имеют возможность выгружать базовую отчетность об актуальном состоянии объектов (активов).

7.1. Модуль идентификации активов в сети Интернет

В разделах «Dashboard», «Assets» и «Graph» представлена возможность просматривать результаты поиска активов компании в сети. В разделе «Dashboard» результаты поиска разделены на подразделы и представлены в виде виджетов «SSL», «Domain» и «IP», соответствующие источникам получаемых данных: «SSL» — сертификаты SSL/TLS, «Domain» — доменные имена, «IP» — IP-адреса; в разделе «Assets» — на подразделы «Domains», «SSL», «IP-addresses», «IP subnets», «Software» и «Login forms», представленные в виде вкладок; в разделе «Graph» — все обнаруженные активы компании представлены в виде связного графа.

7.2. Модуль валидации активов

Система тестирует каждый обнаруженный в сети актив для определения его в одну из следующих категорий: уязвимости, сетевая безопасность, утечки учетных данных, защищенность от вредоносного ПО, упоминания на теневых площадках, защита SSL/TLS, безопасность электронной почты, а также DNS и домены. Тестирование предполагает три типа результата:

- ошибка — критическая проблема, требующая срочных действий;

- предупреждение — вероятная проблема, требующая дальнейших действий;
- тест пройден — проблем не найдено.

7.3. Модуль уведомлений и оценки рисков

Система обогащает обнаруженные активы и потенциальные проблемы контекстом из Group-IB Threat Intelligence & Attribution, что позволяет приоритизировать риски и определить, используется ли выявленная уязвимость или техника атаки в реальных условиях.

8. Устранение неисправностей ПО

Устранение неисправностей ПО происходит в 2 этапа:

- Устранение критичных неисправностей. Производится непосредственно при обнаружении неисправности, выпуск исправляющего обновления производится незамедлительно.
- Устранение неисправностей не являющихся критическими. Производится в равно запланированные промежутки времени (раз в 2 недели) одновременно с выпуском других обновлений.

Среднее временной интервал доступности продукта за год – 95%.

Для обеспечения бесперебойной работы ПО необходима команда технической поддержки, состоящая не менее чем из двух специалистов разработки, а также не менее чем из одного dev-ops инженера.

Сообщить об обнаруженной неисправности можно при помощи отправки уведомления на электронный ящик AssetZero@group-ib.ru.

9. Совершенствование ПО

ПО находится в состоянии постоянного совершенствования. План совершенствования утверждается на год, впоследствии становится доступен для конечных пользователей.

Выпуск готовых обновлений производится не реже 1 раза в месяц.

10. Фактическое размещение инфраструктуры и команды разработки

Команда, а также инфраструктура разработки размещены по адресу – г.Москва, ул. Шарикоподшипниковская д.1