**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**



**МОСКОВСКИЙ ПОЛИТЕХ**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

**ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ**

На тему:

«Изучение практических основ информационной безопасности»

**Выполнил**: ст. гр. 241-351 Зверев З.Д.

**Руководитель**: Кесель С. А., к.т.н., доцент кафедры «Информационная безопасность»

**Место проведения**: Московский Политех, лаборатория «Программно-аппаратных средств обеспечения информационной безопасности»

**Москва – 2025**

ОГЛАВЛЕНИЕ

[ИЗУЧЕНИЕ MITRE ATT&CK 3](#_Toc196249738)

[ИЗУЧЕНИЕ OWASP 5](#_Toc196249739)

[РАЗБОР ИНЦЕДЕНТА 8](#_Toc196249740)

# 

# ИЗУЧЕНИЕ MITRE ATT&CK

MITRE – некоммерческая американская организация, занимающаяся исследованиями в области регулирования и навигации в воздушном пространстве, систем глобального позиционирования (GPS), аэрокосмической промышленности, *кибербезопасности* и других.

Кроме разбираемой в этой работе матрицы MITRE ATT&CK, у этой компании есть и другие общедоступные проекты в области кибербезопасности, например каталоги CVE (Common Vulnerabilities and Exposures, общедоступный стандартизированный список уязвимостей) и CWE (Common Weakness Enumeration, список дефектов безопасности программного обеспечения).

«ATT&CK» расшифровывается как «Adversarial Tactics, Techniques and Common Knowledge».

Эта матрица представляет из себя общедоступную базу знаний, основанную на анализе реальных атак, поделённую на этапы. В ней содержится список тактик (заголовки столбцов), а также техник и подтехник (содержимое столбцов) для этой тактики. Нужна матрица MITRE ATT&CK для описания «паттернов поведения злоумышленников» и используется в качестве основы для разработки конкретных моделей угроз и методологий в сфере кибербезопасности.

Есть 3 матрицы MITRE ATT&CK – для корпоративных сетей и классических клиент-сервисных приложений (Enterprise ATT&CK), для мобильных приложений (Mobile ATT&CK) и для промышленных систем управления (ICS ATT&CK).

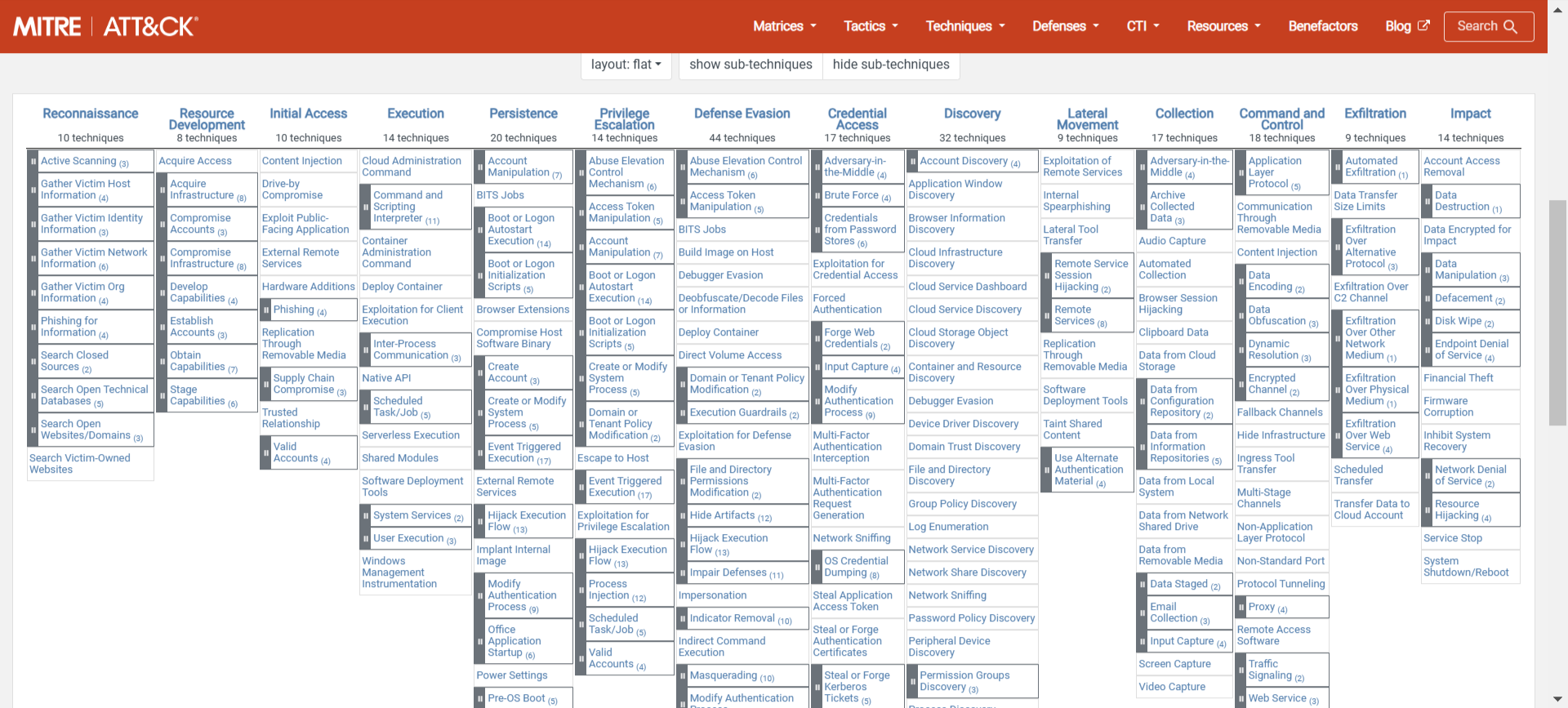


Рис. 1, неполная матрица MITRE ATT&CK

Также, на сайте MITRE ATT&CK, кроме матриц и информации о тактиках, техниках и подтехниках, можно найти информацию о «группировках» («кластерах активности с общими названиями») злоумышленников, а также информацию об их «типичном поведении» (рис. 2 и рис. 3).

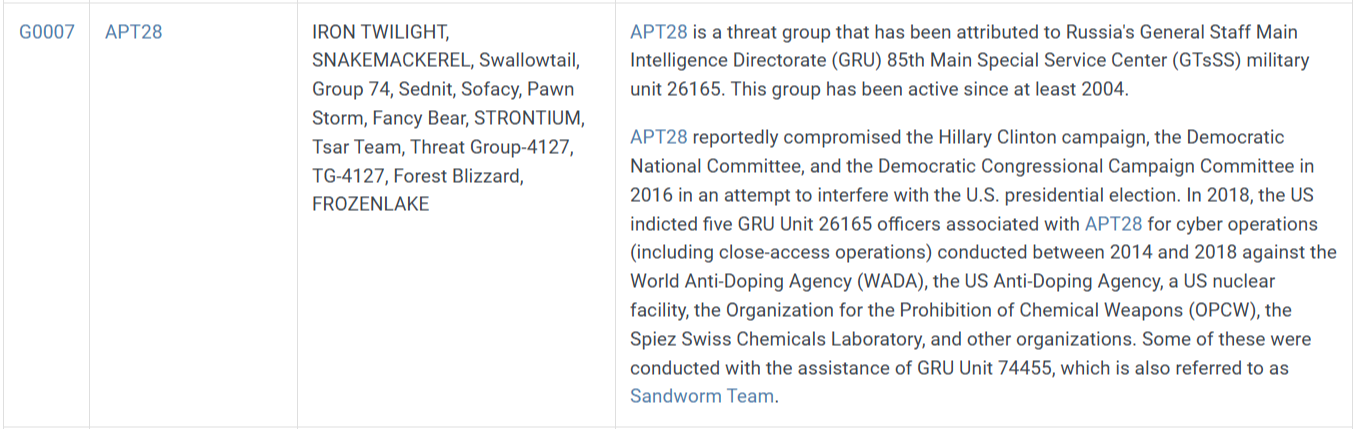


Рис. 2, информация об APT28 в разделе «Groups»

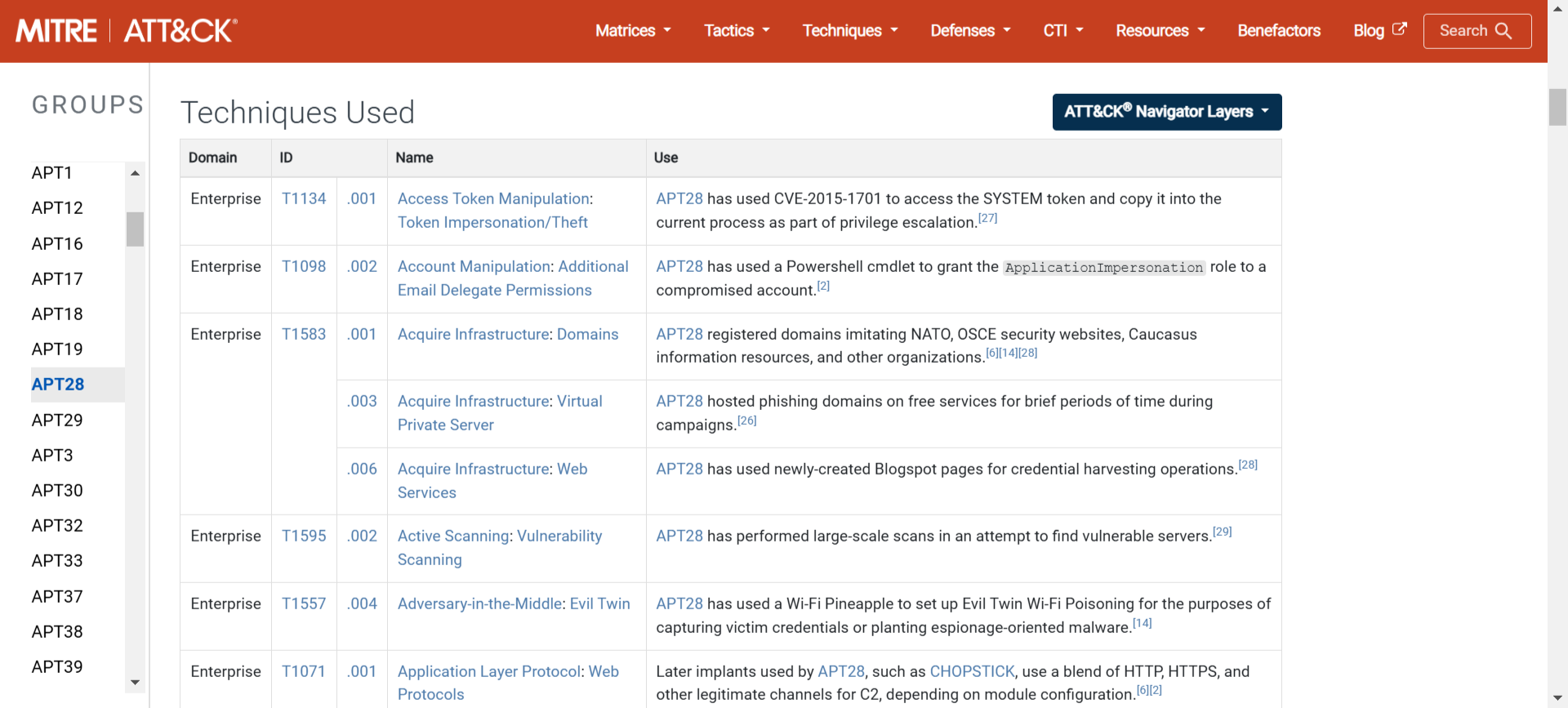


Рис. 3, неполный список используемых APT28 техник

# ИЗУЧЕНИЕ OWASP

OWASP или «Open Worldwide Application Security Project» – это международная некоммерческая организация, ставящая своей целью улучшение безопасности веб-приложений и другого программного обеспечения. Один из основных принципов OWASP заключается в том, что все их материалы являются общедоступными, и их можно найти на их веб-сайте.

Самый известный проект OWASP – это OWASP Top-10. Это обновляющийся раз в несколько лет отчёт с 10 самыми частыми проблемами безопасности (уязвимостями) веб-приложений. На данный момент актуальна версия 2021 года, но в первой половине 2025 года планируется публикация нового отчёта.



Рис. 4, сравнение и изменение OWASP Top-10 2017 и 2021

OWASP ASVS (Application Security Verification Standard) – это проект OWASP, представляющий из себя стандарт для проведения проверок уровня безопасности приложений. Основная цель этого проекта – «нормализовать диапазон охвата и уровень строгости, когда речь идёт о проверке безопасности веб-приложений».

Предполагается ссылка на требования ASVS в установленном формате. Делается это для разных целей: как указание для разработчиков или сторонних лиц, обеспечивающих безопасность приложений.  
Формат ссылки: <chapter>.<section>.<requirement>; на каждой из 3 позиций ставится число.  
Также может указываться версия ASVS, тогда формат будет выглядеть иначе: v<version>-<chapter>.<section>.<requirement>; если версия не указывается, ссылка считается ссылающей на требование в новейшей версии.

OWASP Gen AI – проект по обеспечению безопасности генеративного ИИ. Этот проект включает в себя «OWASP Top-10 LLM and Gen AI» – список 10 основных уязвимостей для языковых моделей и генеративного ИИ. На сайте этого проекта есть документ на русском языке с «Топ-10 OWASP для приложений LLM 2025» от 11 марта 2025 г., с наиболее частыми уязвимостями, объяснением их причин и методами устранения (документ доступен не только на русском).

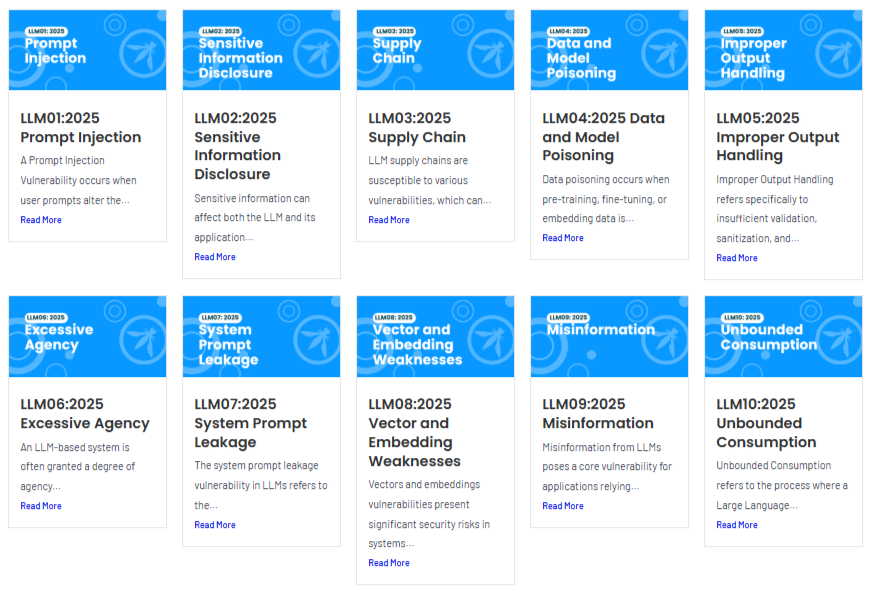


Рис. 5, OWASP Top-10 LLM and Gen AI 2025

OWASP Juice Shop – это «намеренно-небезопасное» веб-приложение. Оно создано для тренингов по безопасности, демонстраций уязвимостей, командных турниров и в качестве «подопытного кролика» для тестирования инструментов безопасности. OWASP Juice Shop содержит уязвимости из OWASP Top-10 и другие. Во время выполнения лабораторных работ на дисциплине «проектная деятельность» я запускал это приложение в контейнере Docker и тестировал на нём инструменты проверки безопасности.

OWASP MAS (Mobile Application Security) – стандарт безопасности для мобильных приложений (MASVS, Mobile ASVS) и подробное руководство по тестированию мобильных приложений (MASTG). В них описываются процессы, методы и инструменты, используемые при тестировании безопасности мобильных приложений, а также исчерпывающий набор тестовых сценариев, позволяющий тестировщикам получать согласованные и полные результаты. Текущая версия MASVS – 2.1.0, MASTG – 1.7.0.

OWASP WSTG (Web Security Testing Guide) - подробное руководство по тестированию безопасности веб-приложений и веб-сервисов. WSTG создан специалистами по кибербезопасности. OWASP называет его «свод лучших практик, используемых тестировщиками на проникновение и организациями по всему миру». Форма ссылки на WSTG: WSTG-<category>-<number>. Форма с указанием версии документа: WSTG-<version>-<category>-<number>.

OWASP ZAP – бесплатный open-source сканер уязвимостей вроде Burp Suite. Позволяет проводить ручное и автоматическое сканирование веб-приложений. OWASP ZAP я также использовал при выполнении лабораторных работ на «проектной деятельности».

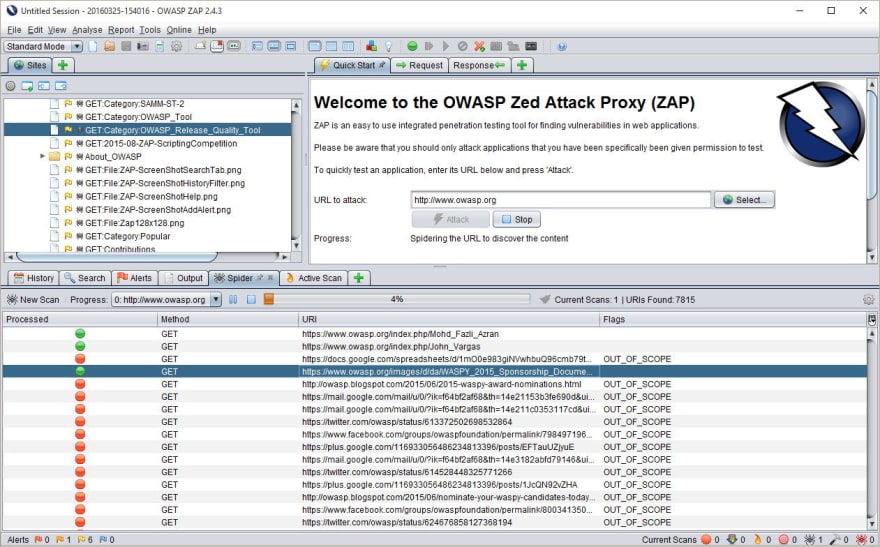


Рис. 6, пример интерфейса OWASP ZAP

OWASP Dependency-Check – это инструмент определения компонентов программного обеспечения (SCA), который пытается обнаружить известные уязвимости зависимостей проекта. Оно было создано после попадания уязвимости «использование компонентов и библиотек с известными уязвимостями» в список OWASP Top-10 2013.

Это далеко не все проекты OWASP – в их GitHub более 1300 репозиториев, а предложить проект может любой. Но перечисленные и описанные выше проекты являются основными и наиболее используемыми.

# РАЗБОР ИНЦЕДЕНТА

В 2024 году было значительное количество атак APT-группы SideWinder в Джибути. Позже злоумышленники переключились на другие организации в Азии, а также проявляли особое внимание к целям в Египте. Кроме того, был зафиксирован ряд атак, которые свидетельствуют об особом интересе группы к атомным электростанциям и ядерной энергетике в Южной Азии, а также о постепенном расширении ее деятельности на новые страны, особенно в Африке.

SideWinder постоянно совершенствует свой инструментарий, чтобы обходить механизмы детектирования защитного ПО, лучше закрепляться в скомпрометированных сетях и скрывать свое присутствие в зараженных системах. На основе наблюдений «Лаборатории Касперского» за деятельностью группы есть предположение, что она постоянно отслеживает случаи детектирования своего инструментария. Сразу после того, как средства безопасности обнаруживают инструменты SideWinder, злоумышленники оперативно – иногда за считаные часы – создают новую или модифицированную версию вредоносного ПО. Если обнаружение произошло на основе поведенческого анализа, APT-группа SideWinder обычно меняет методы закрепления в системе и загрузки компонентов.

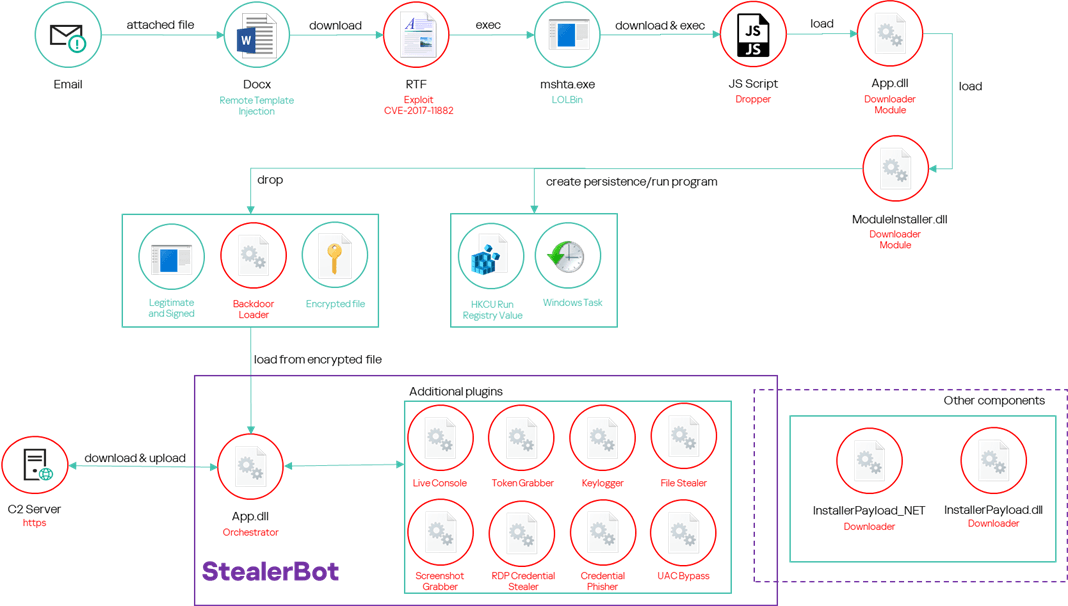


Рис. 7, схема заражения устройств

Злоумышленники рассылают целевые фишинговые письма с прикрепленным файлом DOCX. В этом документе применяется техника инъекции удаленного шаблона для загрузки RTF-файла с удаленного сервера, находящегося под контролем злоумышленников. В файле эксплуатируется известная уязвимость CVE-2017-11882 «Microsoft Office Memory Corruption Vulnerability» для выполнения вредоносного шелл-кода и запуска многоэтапного процесса заражения, в результате которого устанавливается ВПО, названный в «Лаборатории Касперского» Backdoor Loader. Он служит загрузчиком для StealerBot – набора посткомпрометационных инструментов, который используется исключительно группой SideWinder.

В последней волне атак целями группы SideWinder также были дипломатические учреждения в Афганистане, Алжире, Болгарии, Китае, Индии, Руанде, Саудовской Аравии, Турции и Уганде, а также на Мальдивах.