6. Новый массив точек записывается в файл.

Алгоритм извлечения информации:

1. Выделение массива со всеми точками из файла-контейнера.

2. Удаление из массива n точек, которые содержат целые числа.

3. Перемешивание точек на основе seed.

4. Формирование сообщения с предпоследнего бита каждой координаты.

5. Обрезать часть данных по длине, равной полученному значению.

Таким образом, на основании проведенного анализа можно сделать вывод, что для реализации стеганографического внедрения в STEP-файлы наиболее оптимальным подходом является комбинация адаптированного метода LSB для работы с цифровыми координатами CARTESIAN_POINT и дополнительных криптографических механизмов для повышения общей стойкости системы. Выбор именно данных координат основан их высокой точностью, широким распространением, а также минимальным визуальным влиянием на модель при манипуляции с младшими битами.

ЛИТЕРАТУРА

1. Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации: учебно-метод. пос. для студ. вузов / П. П. Урбанович. – Минск: БГТУ, 2016. – 219 с.

2. Блинова, Е. А. Стеганографический метод на основе встраивания скрытых сообщений в кривые Безье изображений формата SVG (Steganographic method based on hidden messages embedding into Bezier curves of SVG images) (на англ. языке) / Е. А. Блинова, П. П. Урбанович // Журнал Белорусского государственного университета. Математика. Информатика – 2022. – № 3. – С. 68–83.

УДК 003.26

А.Н. Николайчук, ассист.;
(БГТУ, г. Минск)

ОБНАРУЖЕНИЕ СТЕГАНОГРАФИЧЕСКИХ УГРОЗ НА ОСНОВЕ АНАЛИЗА АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ С ИСПОЛЬЗОВАНИЕМ IDS/IPS

В современной сфере информационной безопасности защита данных традиционно фокусируется на криптографии (шифровании) и противодействии вредоносному ПО. Однако существует класс угроз, связанных со скрытием самого факта передачи информации – сетевая стеганография [1]. Стеганографические методы не нарушают целост-

ность системы, а используют избыточность сетевых протоколов для организации скрытых каналов связи. Актуальность данной темы обусловлена тем, что стеганографический трафик полностью соответствует спецификациям протоколов.

Сетевая коммуникация строится на базе модели TCP/IP, состоящей из четырех уровней. Стеганография может быть реализована на любом из них путем использования служебных полей заголовков:

– прикладной уровень (данные могут скрываться в текстовых полях, заголовках запросов или в структуре имен хостов);

– транспортный уровень (для передачи скрытых бит часто используются начальные номера последовательностей (ISN) или зарезервированные флаги);

– сетевой уровень (используются поля идентификации пакетов (IP ID), флаги фрагментации или поле «время жизни» (TTL);

– канальный уровень (работа ведется со служебными полями кадров внутри локальной сети).

Скрытый канал создается путем «инкапсуляции» (вложения) секретных данных в эти поля. Поскольку поля являются легитимными, пакет проходит через сетевое оборудование без препятствий [2].

Методы скрытой передачи данных принято разделять на три основные группы [3-6]:

– модификация содержимого пакетов (изменение значений в заголовках или полезной нагрузке, например, данные записываются в неиспользуемые биты IP-заголовка);

– модификация структуры передачи (не меняет сами пакеты, а управляет процессом их отправки);

– гибридные методы (сочетают в себе обе вышеуказанные техники).

Обнаружение таких угроз традиционными средствами (межсетевые экраны, антивирусы) крайне затруднительно, так как трафик выглядит легитимным, поэтому в данном докладе предлагается рассмотреть использование для этих целей системы обнаружения и предотвращения вторжений (IDS/IPS). IDS (Intrusion Detection System) – система, которая мониторит сетевой трафик или активность на хостах на предмет признаков атак или политик безопасности и генерирует оповещения, а IPS (Intrusion Prevention System) – активная система, которая не только обнаруживает, но и может автоматически блокировать подозрительную активность (например, разрывать соединение, отбрасывать пакеты).

Чтобы обнаружить стеганографию, IDS/IPS должна перейти от простого поиска известных вирусов (сигнатур) к анализу аномалий.

То есть, она должна знать «нормальный» профиль трафика и выбрасывать предупреждение при любых статистических отклонениях: неожиданный объем DNS-запросов, странные временные задержки, нетипичная длина пакетов.

Один из самых известных инструментов в этой области – Snort. Это мощный движок для анализа пакетов с гибкой системой правил. Основная логика будет такой: «Если в трафике есть такие-то характеристики (источник, порт, содержимое, частота), то выполни такое-то действие (залогируй, предупреди, останови)».

Для стеганографии ключевыми становятся правила, основанные на аномалиях, а не на конкретном коде. Они анализируют поведение, статистику, структуру.

В качестве примера был использован метод DNS-туннелирования [2]. Его суть заключается в передаче данных внутри DNS-запросов (запросов на поиск имени хоста). Вместо реального имени узла клиент отправляет серверу закодированную информацию в виде поддомена.

Был запущен клиент, написанный на языке python, использующий библиотеку scapy, передающий данные через DNS-туннель. На первом этапе Snort работал с базовым набором правил. Весь трафик был пропущен системой, так как он выглядел как стандартная активность по разрешению доменных имен.

На втором этапе были добавлены правила, направленные на поиск аномалий (рис. 1). В частности, анализировалась длина строки запроса в UDP-пакетах (порт 53). Был установлен порог срабатывания, если длина отдельной метки (части доменного имени) в запросе превышает 63 символа, что является нарушением стандарта и характерно для некоторых методов туннелировании.

После настройки правил система Snort зафиксировала попытку передачи данных и сгенерировала оповещения, в лог-файлах сохранена подробная информация: время инцидента, IP-адреса отправителя и получателя, а также структура аномального пакета. Таким образом, угроза была успешно идентифицирована на основе поведенческого анализа. Системы IDS/IPS, в частности Snort с адаптированным набором правил, являются практически применимым инструментом для выявления статистических и поведенческих аномалий, для которых нужно подбирать индивидуальный подход. Как показал пример с DNS-туннелированием, корректно настроенная система способна детектировать факт скрытой передачи данных на основе отклонений от нормальных сетевых профилей – таких как аномальная длина полей, частотные или временные характеристики трафика.

```
alert udp any any -> 192.168.0.7 53 (
    msg:"DNS STEGANOGRAPHY: Long subdomain detected"
    dsize:>12;
    content:"|00 00|";
    content:"|01 00|";
    byte_test:1, >, 63, 12, relative;
    sid:1000001;
    rev:1;
    metadata:service dns;
  )
```

Рисунок 1 – Правило для поиска аномалии

Таким образом, для комплексного противодействия стеганографии можно внедрять и совершенствовать методы анализа аномалий в существующие системы мониторинга безопасности. Перспективным направлением является развитие гибридных систем, сочетающих правила, основанные на экспертных знаниях о конкретных методах, с адаптивными алгоритмами машинного обучения для выявления неизвестных стеганографических каналов.

ЛИТЕРАТУРА

1. Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации. – Минск: БГТУ, 2016. – 220 с.

2. Zander, S. A Servey of Convert Channels and Countermeasures in Computer Network Protocol / S. Zander, G. Armitage, P. Branch // IEEE Communications Surveys & Tutorials – 2007. – V.9. – № 3. – P. 44–57.

3. Николайчук А.Н., Урбанович П.П. Использование полей заголовка протокола IP для создания скрытого канала передачи данных // Информационные технологии. Физика и математика: Материалы 89-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием): Белорусский государственный технологический университет. – Минск, 2025. – С. 43–46.

4. Николайчук А.Н. Сравнительный анализ методов сетевой стеганографии // VIII Междунар. науч.-техн. конф. «Минские научные чтения – 2025», Минск, 3 – 5 декабря 2025 г. : в 3 т. Т. 1. – Минск: БГТУ, 2025. – С. 441–444.

5. Применения сетевой стеганографии для скрытия данных, передаваемых по каналам связи / О.Ю. Пескова, Ю. Г. Халабурда // Известия ЮФУ. Технические науки – 2012.

6. Handel, T., Sandford, M. Hiding data in the OSI network model / T. Handel, M. Sandford // In Proceedings of The First International Workshop on Information Hiding – 1996. – P. 23–38.