(https://clck.ru/h2cVD)

28 ноября 2016 - 14:47

Все об атаке "Человек посередине" (Man in the Middle, MitM)

Олег Иванов
Менеджер проектов Anti-Malware.ru

Проголосовало: 144

(/users/oleg-ivanov)

Аналитика (/analytics) Анализ угроз (/analytics/Threats_Analysis)

Домашние пользователи (/home_security) Малый и средний бизнес (/smb_security)

Перехват данных по сети (/threats/network-traffic-interception)

В этой статье мы попытаемся выяснить теорию атак посредника и некоторые практические моменты, которые помогут предотвратить эти типы атак. Это поможет нам понять тот риск, который несут подобные вторжения для нашей личной жизни, так как MitM-атаки позволяют вторгаться в коммуникации и прослушивать наши разговоры.

1. Обеспечение безопасности протокола связи

2. Атака посредника через HTTP-протокол

3. Атака посредника на плохо реализованный SSL

4. Понимание SSL

5. Проблемы центров сертификации

6. Криминалистика

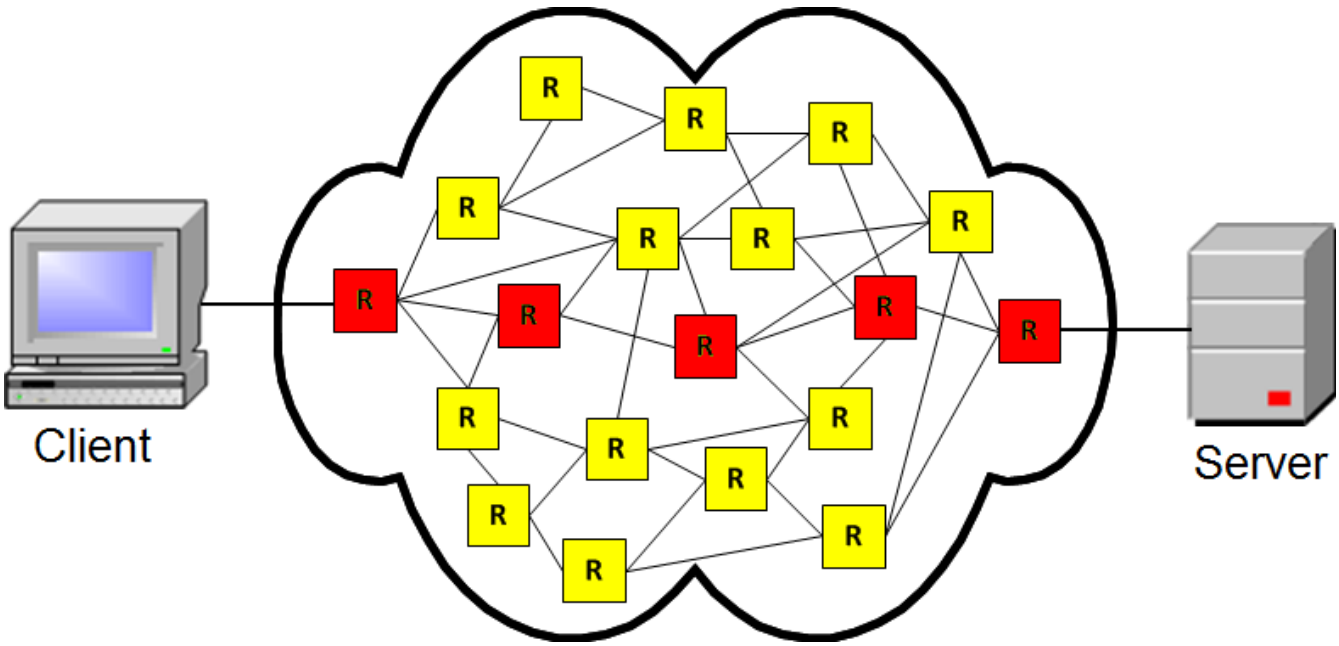
7. Вывод

Понимание того, как работает интернет

Чтобы понять принцип атаки посредника, стоит сначала разобраться с тем, как работает сам интернет. Основные точки взаимодействия: клиенты, маршрутизаторы, серверы. Наиболее распространенный протокол взаимодействия между клиентом и сервером — Hypertext Transfer Protocol (HTTP). Серфинг в интернете с помощью браузера, электронная почта, обмен мгновенными сообщениями — все это осуществляется через HTTP.

Когда вы вводите http://www.anti-malware.ru (http://www.anti-malware.ru) в адресной строке вашего браузера, то клиент (вы) отправляет запрос на отображение веб-страницы серверу. Пакет (HTTP GET-запрос) передается через несколько маршрутизаторов на сервер. После этого сервер отвечает веб-страницей, которая отправляется клиенту и отображается на его мониторе. HTTP-сообщения должны передаваться в безопасном режиме, чтобы обеспечить конфиденциальность и анонимность.

Рисунок 1. Взаимодействие клиент—сервер



Обеспечение безопасности протокола связи

Безопасный протокол связи должен иметь каждое из следующих свойств:

1. **Приватность** — только предполагаемый получатель может прочитать сообщение.
2. **Аутентичность** — личность взаимодействующих сторон доказана.
3. **Целостность** — подтверждение того, что сообщение не было изменено в пути.

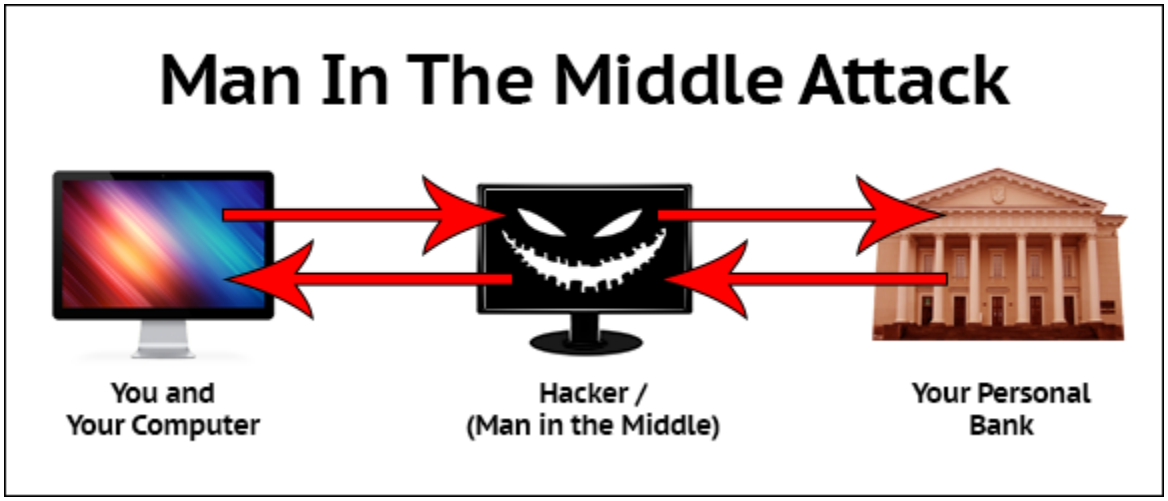
Если хоть одно из этих правил не соблюдено, весь протокол скомпрометирован.

Атака посредника через HTTP-протокол

Злоумышленник может легко осуществить атаку посредника, используя технику, называемую ARP-спуфинг. Любой в вашей сети Wi-Fi может послать вам поддельный ARP-пакет, из-за него вы неосознанно будете посылать весь ваш трафик через злоумышленника вместо маршрутизатора.

После этого злоумышленник получает полный контроль над трафиком и может отслеживать запросы, посылаемые в обе стороны.

Рисунок 2. Схема атаки посредника



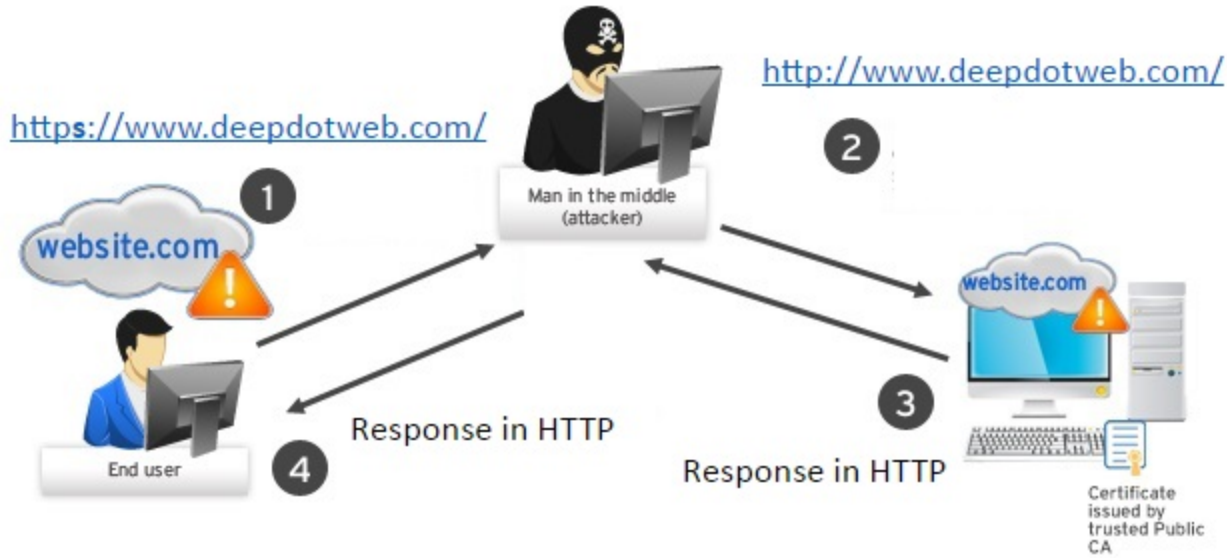
Для предотвращения таких атак была создана защищенная версия протокола HTTP. Transport Layer Security (TLS) и его предшественник, Secure Socket Layer (SSL), являются криптографическими протоколами, которые обеспечивают безопасность передачи данных по сети. Следовательно, защищенный протокол будет называться HTTPS. Можно посмотреть, как работает защищенный протокол, набрав в адресной строке браузера https://www.anti-malware.ru (https://www.anti-malware.ru) (обратите внимание на наличие S в https).

Атака посредника на плохо реализованный SSL

Современный SSL использует хороший алгоритм шифрования, но это не имеет значения, если он реализован неправильно. Если хакер может перехватить запрос, он может его изменить, удалив из запрашиваемого URL «S», тем самым обойдя SSL.

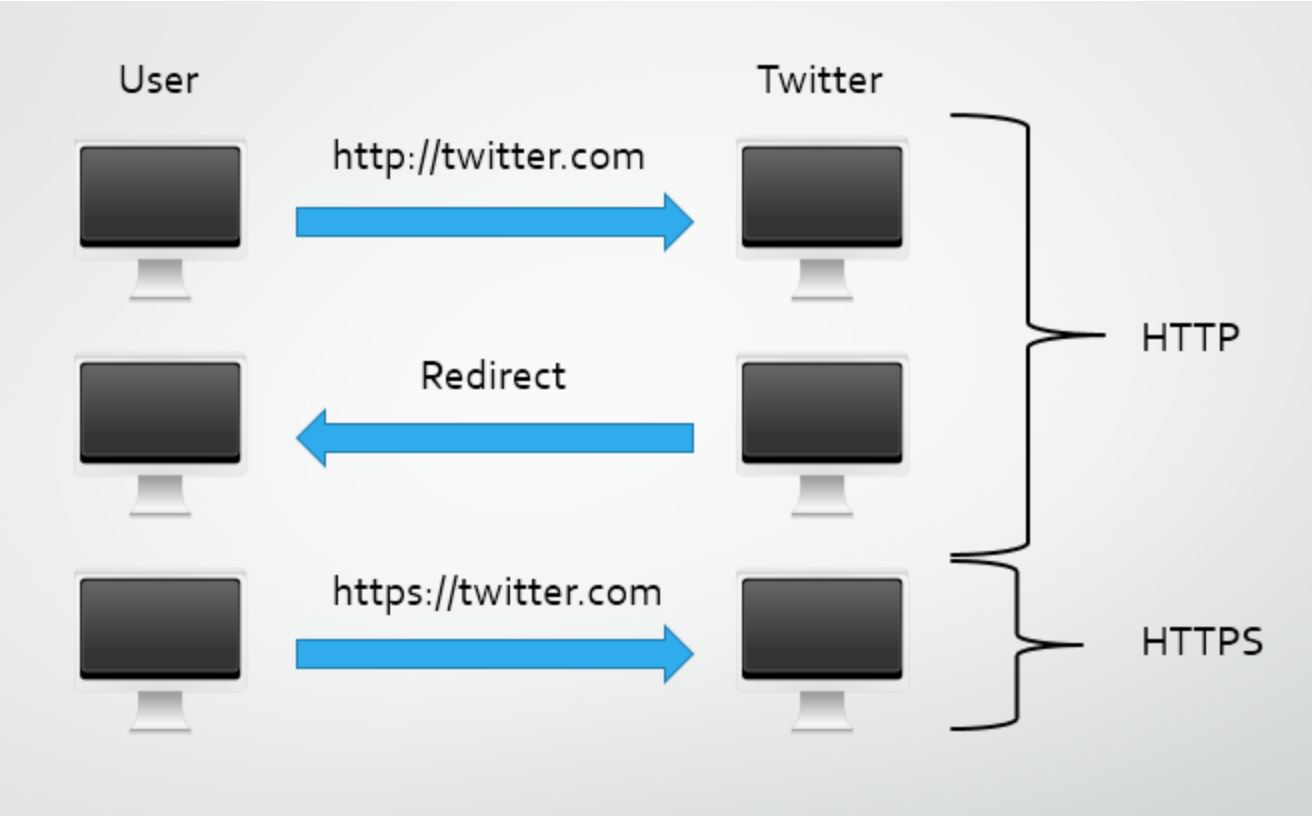
Такой перехват и модификацию запроса можно заметить. Например, если вы запрашиваете https://login.yahoo.com/ (https://login.yahoo.com/) а в ответ приходит http://login.yahoo.com/ (http://login.yahoo.com/), это должно вызвать подозрения. На момент написания статьи такая атака действительно работает на сервисе электронной почты Yahoo.

Рисунок 3. Перехват и модификация запроса



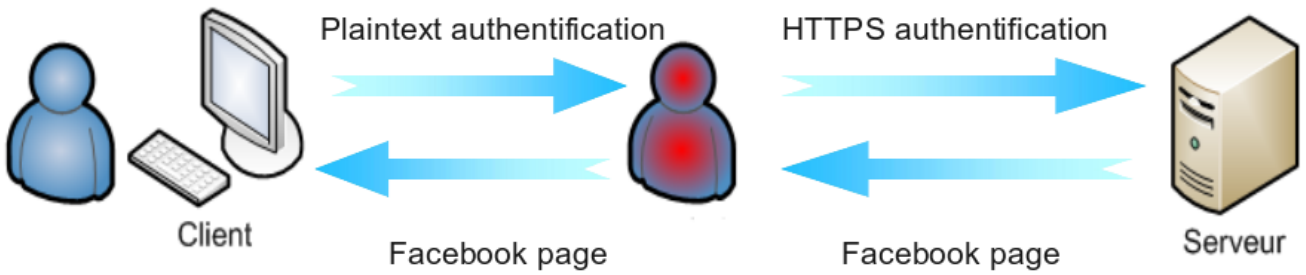
Чтобы предотвратить такую атаку, серверы могут реализовать HTTP Strict Transport Security (HSTS) — механизм, активирующий форсированное защищенное соединение через протокол HTTPS. В этом случае, если злоумышленник модифицирует запрос, убрав из URL «S», сервер все равно перенаправит пользователя 302-редиректом на страницу с защищенным протоколом.

Рисунок 4. Схема работы HSTS



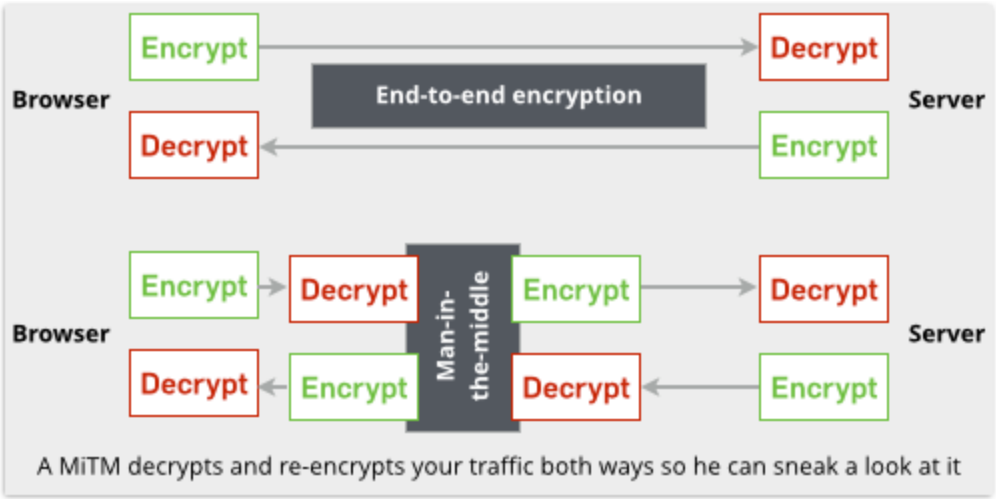
Такой способ реализации SSL является уязвимым для другого вида атаки — злоумышленник создает SSL-соединение с сервером, но различными уловками заставляет пользователя использовать HTTP.

Рисунок 5. Схема атаки при HSTS



Для предотвращения таких атак современные браузеры вроде Chrome, Firefox и Tor отслеживают сайты, использующие HSTS и устанавливают с ними соединение со стороны клиента по SSL в принудительном порядке. В этом случае злоумышленнику, проводящему атаку посредника, придется создавать SSL-соединение с жертвой.

Рисунок 6. Схема атаки, где злоумышленник устанавливает SSL-соединение с жертвой



Для того чтобы обеспечить SLL-соединение с пользователем, злоумышленник должен знать, как действовать в качестве сервера. Давайте разберемся в технических аспектах SSL.

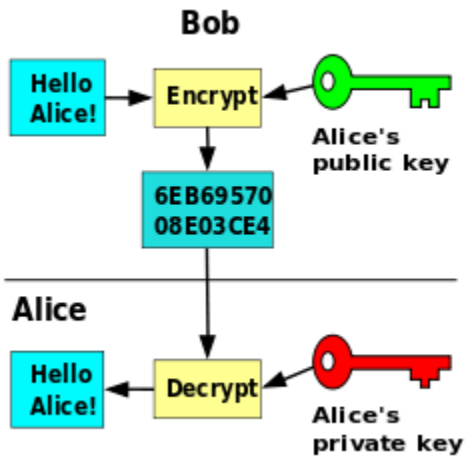
Понимание SSL

С точки зрения хакера, компрометирование любого протокола связи сводится к тому, чтобы найти слабое звено среди перечисленных выше компонентов (приватность, аутентичность и целостность).

SSL использует асимметричный алгоритм шифрования. В симметричном шифровании проблема заключается в том, что для шифрования и дешифрования данных используется один и тот же ключ, такой подход недопустим для интернет-протоколов, поскольку злоумышленник может проследить этот ключ.

Асимметричное же шифрование включает в себя 2 ключа для каждой стороны: открытый ключ, используемый для шифрования, и конфиденциальный ключ, используемый для дешифрования данных.

Рисунок 7. Работа публичного и конфиденциального ключей



Как SSL обеспечивает три свойства, необходимые для безопасной связи?

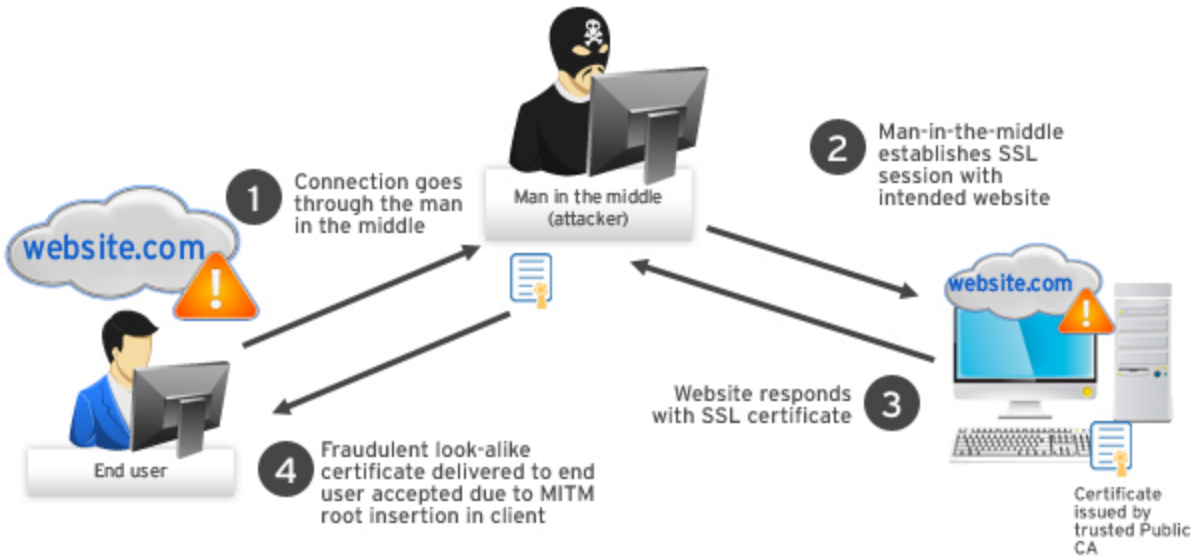
1. Поскольку для шифрования данных используется асимметричная криптография, SSL обеспечивает приватное соединение. Это шифрование не так уж легко взломать и остаться незамеченным.

2. Сервер подтверждает свою легитимность, посылая клиенту SSL-сертификат, выданный центром сертификации — доверенной третьей стороной.

Если злоумышленнику каким-либо образом удастся заполучить сертификат, он может создать условия для атаки посредника. Таким образом, он создаст 2 соединения — с сервером и с жертвой. Сервер в этом случае думает, что злоумышленник — это обычный клиент, а у жертвы нет возможности идентифицировать злоумышленника, поскольку тот предоставил сертификат, доказывающий, что он сервер.

Ваши сообщения доходят и приходят в зашифрованном виде, однако проходят по цепочке через компьютер киберпреступника, где у него есть полный контроль.

Рисунок 8. Схема атаки при наличии у злоумышленника сертификата



Сертификат не обязательно должен быть подделан, если у злоумышленника есть возможность скомпрометировать браузер жертвы. В этом случае он может вставить самостоятельно подписанный сертификат, который будет доверенным по умолчанию. Так и реализовываются большинство атак посредника. В более сложных случаях хакер должен пойти другим путем — подделать сертификат.

Проблемы центров сертификации

Отправляемый сервером сертификат выдан и подписан центром сертификации. В каждом браузере есть список доверенных центров сертификации, и вы можете добавлять или удалять их. Проблема здесь заключается в том, что если вы решите удалить крупные центры, вы не сможете посещать сайты, использующие подписанные этими центрами сертификаты.

Сертификаты и центры сертификации всегда были самым слабым звеном HTTPS-соединения. Даже если все было реализовано правильно и каждый центр сертификации имеет солидный авторитет, все равно сложно смириться с фактом, что приходится доверять множеству третьих сторон.

На сегодняшний день существует более 650 организаций, способных выдавать сертификаты. Если злоумышленник взломает любую из них, он заполучит любые сертификаты, которые пожелает.

Даже когда существовал всего один центр сертификации, VeriSign, бытовала проблема — люди, которые должны были предотвращать атаки посредника, продавали услуги перехвата.

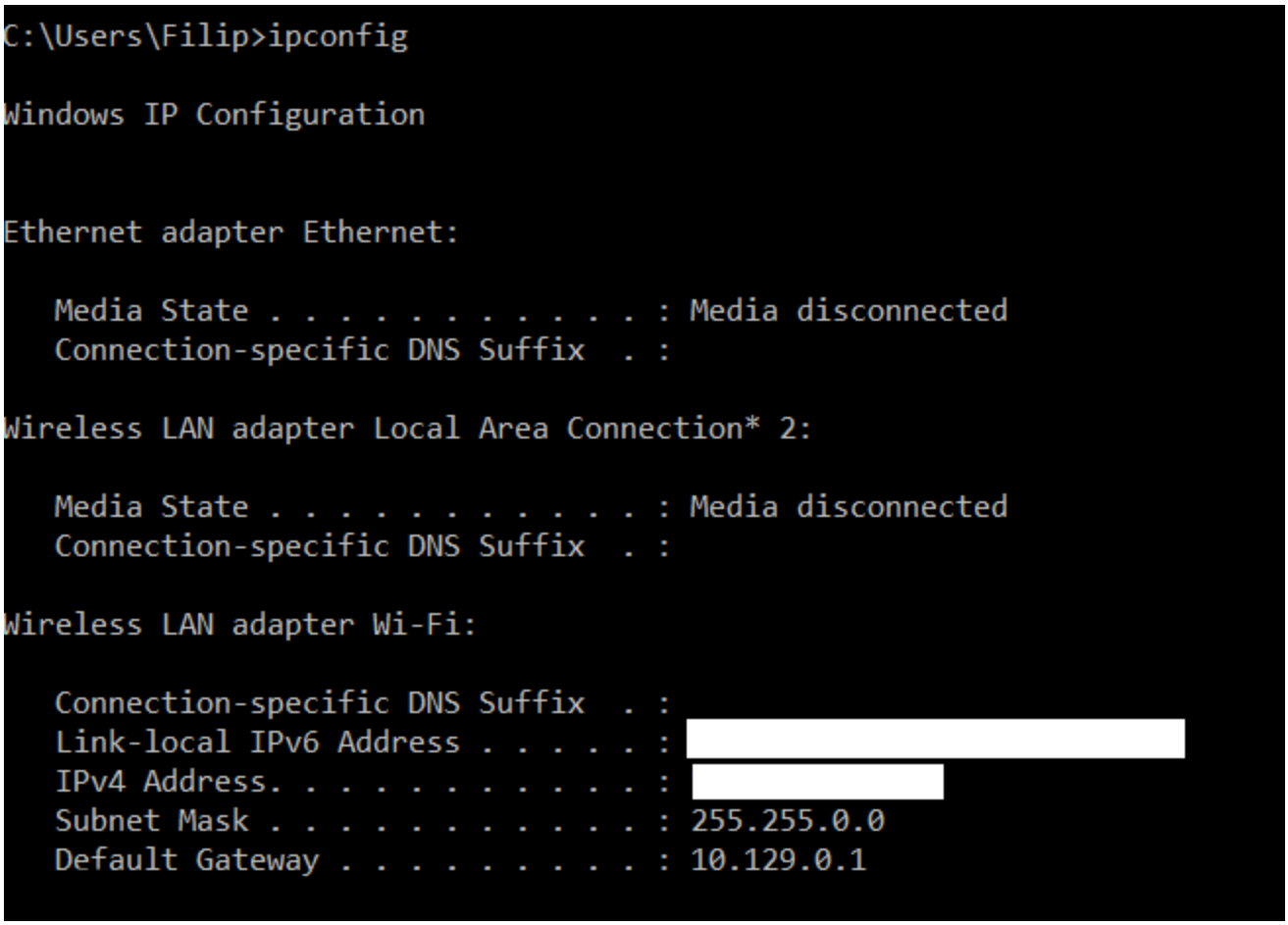
Также многие сертификаты были созданы благодаря взлому центров сертификации. Различные приемы и трюки использовались, чтобы заставить атакуемого пользователя доверять мошенническим сертификатам.

Криминалистика

Поскольку злоумышленник отправляет поддельные пакеты ARP, нельзя увидеть его IP-адрес. Вместо этого нужно обращать внимание на MAC-адрес, который является специфическим для каждого устройства в сети. Если вы знаете MAC-адрес вашего маршрутизатора, вы можете сравнить его с MAC-адресом шлюза по умолчанию, чтобы выяснить, действительно ли это ваш маршрутизатор или злоумышленник.

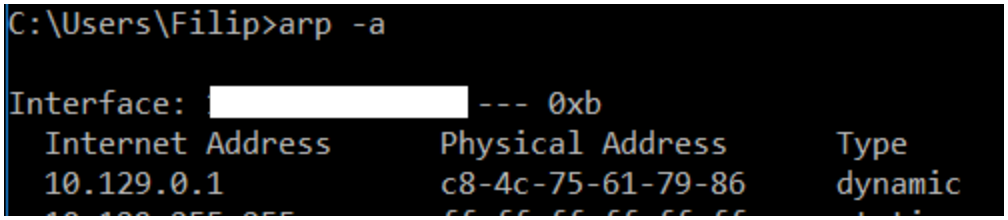
Например, на ОС Windows вы можете воспользоваться командой ipconfig в командной строке (CMD), чтобы увидеть IP-адрес вашего шлюза по умолчанию (последняя строка):

Рисунок 9. Использование команды ipconfig



Затем используйте команду arp –a для того, чтобы узнать MAC-адрес этого шлюза:

Рисунок 10. Использование команды arp –a



Но есть и другой способ заметить атаку — если вы отслеживали сетевую активность в то время, когда она началась, и наблюдали за пакетами ARP. Например, можно использовать Wireshark для этих целей, эта программа будет уведомлять, если MAC-адрес шлюза по умолчанию изменился.

Примечание: если атакующий будет правильно подменять MAC-адреса, отследить его станет большой проблемой.

Вывод

SSL — протокол, заставляющий злоумышленника проделать огромную работу для совершения атаки. Но он не защитит вас от атак, спонсируемых государством или от квалифицированных хакерских организаций.

Задача пользователя заключается в том, чтобы защитить свой браузер и компьютер, чтобы предотвратить вставку поддельного сертификата (очень распространенная техника). Также стоит обратить внимание на список доверенных сертификатов и удалить те, кому вы не доверяете.

(https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19)
Подписывайтесь на канал "Anti-Malware" (https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19) в Яндекс Дзен, чтобы первыми узнавать о новостях и наших эксклюзивных материалах по информационной безопасности.

(/analytics/Threats_Analysis/5G-and-routing-attacks)

(/analytics/Threats_Analysis/protection-corporate-wi-fi)

ПРАКТИКА

Защита сетей SD-WAN с помощью решений Fortinet (/practice/methods/SD-WAN-Fortinet)

(/practice/methods/SD-WAN-Fortinet)

(/stories/feed)

Читайте также

- Аналитика (/analytics)
- Практика (/practice)
- Интервью (/interviews)
- Сравнения (/compare)
- Обзоры (/reviews)

Сертифицированные продукты (/certified)

Корпоративные продукты (/certified/corporate)

Персональные продукты (/certified/home)

Сводный реестр ФСТЭК и AM Test Lab (/certified/information_security_russia)

Прислать свою статью (/send_article)

ОБЗОР НЕДЕЛИ

Обзор InfoWatch Traffic Monitor 7.3, системы защиты от утечек конфиденциальной... (/reviews/InfoWatch-Traffic-Monitor-73)

(/reviews/InfoWatch-Traffic-Monitor-73)

Обзоры и сравнения

Обзор InfoWatch Traffic Monitor 7.3, системы защиты от утечек конфиденциальной информации (/reviews/InfoWatch-Traffic-Monitor-73)

(/reviews/InfoWatch-Traffic-Monitor-73)

Обзор Ideco UTM 12.0, российского универсального шлюза сетевой

безопасности (/reviews/Ideco-UTM-12)
(/reviews/Ideco-UTM-12)

Обзор СёрчИнформ КИБ 5.2, российской DLP-системы (/reviews/SearchInform-Kib-52)
(/reviews/SearchInform-Kib-52)

(/interviews/2022-05-23/38729)

Рамиль Хантимиров:

«Для снижения бизнес-рисков требуется специализированная защита от DDoS, а не провайдер или CDN» (/interviews/2022-05-23/38729)

Статьи

(/analytics/Technology_Analysis/Who-benefits-from-blocking-Proton-VPN-in-Russia)

Кому выгодна блокировка Proton VPN в России (/analytics/Technology_Analysis/Who-benefits-from-blocking-Proton-VPN-in-Russia)

(/analytics/Technology_Analysis/Russian-PAM-evolution)

Эволюция PAM-систем в России (/analytics/Technology_Analysis/Russian-PAM-evolution)

(/analytics/Threats_Analysis/DDoS-in-the-first-quarter-of-2022)

Развенчиваем мифы: DDoS-атаки в первом квартале 2022 г. были аномально сильными (/analytics/Threats_Analysis/DDoS-in-the-first-quarter-of-2022)

КАТАЛОГ СЗИ

Средства защиты (/security)

Угрозы (/threats/information-security-threats)

Сертифицированные СЗИ (/certified/information_security_russia)

Реестр Anti-Malware.ru (/certified)

УСЛУГИ

Реклама (/advertisment)

Сертификация (/services/certification)

Индивидуальные тесты (/services/tests)

О НАС

Редакция (/team)

Контакты (/contact)

Авторы (/best-authors)

Прислать материал (/send_article)

Политика конфиденциальности (/privacy-policy)

Свидетельство о регистрации СМИ ЭЛ № ФС 77 - 68398, выдано федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) 27.01.2017