УДК 004.056.5:004.75

МЕТОД РОЗШИФРОВКИ ТРАФІКУ TLS ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ ЗАГРОЗ

Радівілова Т.А., Тавалбех М.Х.
Харківський національний університет радіоелектроніки
E-mail: tamara.radivilova@gmail.com, tavalbeh@icloud.com

DECRYPTING TLS TRAFFIC METHOD FOR HIDDEN THREATS DETECTION

The analysis of the basic methods of decrypting the TLS traffic was conducted on this work. The methods and technologies for detecting malicious activity in encrypted traffic used by leading companies are presented. Also developed, tested and offered a method of interception and decryption of traffic transmitted through TLS. The developed method was automated and can be used for remote listening to the network, which will allow decoding data transmitted in real-time mode.

В даний час існує тренд збільшення частки шифрованого трафіку. За оцінками Cisco, 60% трафіку в інтернет зашифровано, а за прогнозами Gartner до 2019-го вже 80% трафіку буде таким. Шифрування потрібне для забезпечення приватності громадян, для збереження таємниці в секреті, для виконання вимог законодавства. Але зловмисники також використовують шифрування для обходу механізмів детектування їх несанкціонованої активності, приховуючи взаємодію з командними серверами шкідливих програм і для інших завдань [1].

Існує багато ситуацій, коли адміністратори IT повинні використовувати перевірку пакетів, наприклад за допомогою Wireshark. Однак, коли дані зашифровуються, це стає більш складним завданням. Зазвичай найпростішим способом дешифрування даних є використання закритого ключа для відповідного відкритого ключа. Wireshark надає ще один засіб для дешифрування даних, а також з використанням пре-мастер ключа. Ponemon Institute попросив респондентів оцінити ймовірність виникнення атак і здатність протистояти цим атакам, які показано в таблиці 1 [2].

Пропонований в даній роботі підхід представляє собою метод розшифровки TLS-трафіку, який передбачає наявність у зловмисника доступу до комп'ютера або мережі, або ж зловмисник міг занести на комп'ютер жертви закладки, які можуть збирати дані про сесії. Такі умови потрібні для формування файлів сесійних ключів, які будуть використовуватися разом з відповідним перехопленим трафіком. Перехопити трафік жертви можна, перебуваючи в будь-якій ділянці мережі між сервером і об'єктом нападу.

Нижче наведено опис реалізації запропонованого методу розшифровки TLS-трафіку. В реалізації використовувався аналізатор трафіку Wireshark, який допомагає провести аналіз роботи мережі, діагностувати проблеми, а також має

багато інших корисних можливостей.

Таблиця 1. Напади та ймовірність протистояння ним.

	Ймовірність	
	нападу	***Протистояння нападу***
1. Зловмисник робить фішингові загрози ще більш законними, і навіть інформовані одержувачі вважають, що використання TLS гарантує їм безпеку. Однак, натиснувши на посилання, зловмисник надсилає користувачів до сервера SSL, завантаженого зловмисним програмним забезпеченням, яке заражає клієнта, оскільки трафік зловмисного програмного забезпечення зашифрований і не розпізнається системами виявлення вторгнень.	79%	17%
2. Зловмисник надсилає зашифрований потік захищених, чутливих та інших критичних даних, що надходять через брандмауер через "звичайні" порти (443,80 та ін.), які брандмауер налаштований прийняти, оскільки вони є затвердженими портами.	78%	30%
3. Ряд зловмисників використовує шифрування, щоб приховати інформацію про мережу, включаючи паролі та конфіденційні дані, які вони надсилають на сервери SSL. Шифрування засліпило системи моніторингу/інспектування для цієї внутрішньої мережі.	74%	16%
4. Зловмисник заважає комунікаціям із шкідливим програмним забезпеченням, коли хробак, вірус або ботнет «телефонує додому», щоб відправити вкрадені дані до головного комп'ютера або завантажити інструкції або більше шкідливих кодів.	66%	26%
5. За допомогою міжсайтового скриптингу зловмисники викрадають файли cookie, які можуть використовуватися для захоплення облікового запису або сеансу, зміни налаштувань користувача, отруєння cookie і/або неправдивої реклами. Все це можна виконати, ховаючись в SSL/TLS трафіку.	62%	19%

Нижче наведено опис реалізації запропонованого методу розшифровки TLS-трафіку. В реалізації використовувався аналізатор трафіку Wireshark, який допомагає провести аналіз роботи мережі, діагностувати проблеми, а також має багато інших корисних можливостей.

1. Робимо закладку на комп’ютер жертви (вірус, e-mail, та ін.). Використовуємо

лог-файли сесійних ключів для отримання ключів, які використовуються для шифрування та дешифрування трафіку. Отримання таких лог-файлів за допомогою закладок не є трудомістким (браузери, бібліотеки NSS, java-додатки, відладні записи Java Virtual Machines).

2. Аналізуючи отримані варіанти ключ записів ключей, складаємо NSS-файл з відповідним форматом. Цей формат використовується Wireshark'ом, щоб розшифрувати TLS-записи, зашифровані відповідними ключами. Для цього потрібно мати лог-файл із записами сесійних ключів в NSS-форматі і аналізатором трафіку Wireshark. Wireshark дуже чутливий до формату NSS-файлу, тому краще ретельно перевірити, чи збігається кількість байт у кожному елементі рядка, відсутність зайвих пропусків та інше.

3. Захоплюємо трафік аналізатором трафіку після того, як буде розпочато запис ключів до лог-файлу, так як в іншому випадку нам не вдасться мати сесійні ключі, які відповідають захопленим TLS-записам. Треба пам’ятати, що ключі є дійсними тільки для однієї TLS-сесії і не підходять для дешифрування трафіку іншого сеансу.

4. Відкидаємо непотрібні пакети, що проходять через інтерфейс, що прослуховується, для чого використовуємо відстеження обміну трафіком з визначеним хостом і фільтрації за потрібним протоколом.

5. Після того, як вдалося сформувати файл із сесійними ключами, прив'язуємо файл до Wireshark'у.

6. Тепер у вмісті пакету з'явилася вкладка «Розшифровані дані SSL/TLS» і можна побачити текст запиту. Також можна обрати будь-який пакет протоколу TLS і в його контекстному меню обрати функцію «Follow SSL/TLS Stream» і, незважаючи на зашифровану передачу HTTPS, ми бачимо трафік, що передається, і можемо його експортувати для подальшого аналізу.

Особливістю описаного методу є те, що не обов'язково захоплювати трафік на комп'ютер, який генерує TLS-трафік, його можна перехватити просто будучи в мережі і прослухавши її. А добити файл із сесійними ключами можна, встановивши на комп'ютер жертви закладку або просто скопіювати його, маючи доступ до комп'ютера.

ВИСНОВОК. В процесі роботи розроблено метод дешифрування трафіку TLS, який можна застосувати навіть при віддаленому прослуховуванні мережі. Даний метод автоматизовано і дозволяє розшифровувати дані практично в режимі онлайн.

Література

1. White paper. Cisco public. Encrypted Traffic Analytics. 2018 Cisco.
2. Hidden Threats in Encrypted Traffic: A Study of North America & EMEA. Independently conducted by Ponemon Institute LLC. 2016.