АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ПРЕДОТВРАЩАЮЩЕЕ ФИШИНГОВЫЕ АТАКИ

ANTIVIRUS SOFTWARE THAT PREVENTS PHISHING ATTACKS

УДК 004.424

Прокопайло Александр Александрович, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Prokopailo A.A. aka2h@yandex.ru

Аннотация

Многие современные антивирусные решения предлагают уровень защиты, предназначенный для предотвращения фишинговых атак. Эти продукты обычно не мешают фишинговым письмам попадать в почтовый ящик; вместо этого они выявляют фишинговые веб-сайты и блокируют загрузку страницы, прежде будет получен к ней доступ.

Annotation

Many antivirus solutions today provide a layer of protection designed to prevent phishing attacks. These usually do not prevent phishing emails from reaching your inbox; instead, they identify phishing websites and block page loading.

Ключевые слова: фишинг, целевой фишинг, атака, информационная безопасность, мошенничество, антивирусное программное обеспечение.

Keywords: phishing, spear phishing, attack, cyber security, fraud, antivirus software.

HTTPS - это протокол связи, используемый для передачи данных между браузером и веб-сервером, к которому происходит подключение. Буква «S» в HTTPS означает «Безопасный» и указывает на то, что данные, передаваемые на данном веб-сайте, зашифрованы. Можно узнать, что веб-сайт использует HTTPS, проверив URL-адрес или посмотрев значок замка в адресной строке.

Внедрение HTTPS резко возросло за последние годы. Согласно отчету Google о прозрачности, сегодня около 86 процентов всех веб-сайтов, открытых в Chrome , загружаются по протоколу HTTPS . Всего два года назад эта цифра составляла около 60 процентов. Широкое распространение HTTPS помогло сделать Интернет более безопасным местом.

Это означает, что у антивирусных компаний остается три основных варианта предотвращения фишинговых атак, у каждого из которых есть свои плюсы и минусы:

1. Фильтрация сетевого трафика.

Как упоминалось выше, шифрование HTTPS не позволяет антивирусному программному обеспечению знать, какие веб-сайты посещаются, а это означает, что программное обеспечение не может проверить безопасность URL-адреса HTTPS.

Чтобы обойти это, существует несколько различных способов фильтрации сетевого трафика, загружаемого через HTTPS:

Перехват HTTPS

Большинство антивирусных продуктов используют перехват HTTPS, который включает установку локального прокси-сервера, который эффективно подделывает все сертификаты SSL (фрагменты кода, обеспечивающие безопасность связи между пользователем и веб-сайтом) для создания атаки типа «человек посередине». Когда пользователь посещает веб-сайт HTTPS, исходящее соединение перенаправляется на локальный прокси-сервер, который генерирует новый сертификат SSL, известный как подстановочный сертификат, для олицетворения запрошенного веб-сайта перед проверкой его безопасности. Если веб-сайт считается безопасным, он передается в браузер, и он отображается

на экране. Если веб-сайт окажется небезопасным, прокси отправит браузеру предупреждение.

Проблема в том, что браузер не может проверить сертификат безопасности реального веб-сайта, поскольку он может видеть только поддельный сертификат SSL, созданный прокси-сервером.

Хотя этот подход может обеспечить высокую частоту блокировки, он действительно представляет некоторые значительные риски для безопасности. Во-первых, это потенциально может сделать более уязвимыми для злонамеренных эксплойтов «злоумышленник посередине». Во-вторых, повторное шифрование данных с помощью поддельного сертификата безопасности означает, что пользователь не сможете определить, действительно ли соединение с веб-сайтом является безопасным или нет, что потенциально может привести к отправке конфиденциальной информации через незащищенное соединение.

Перехват HTTPS также вызывает некоторые вопросы о конфиденциальности. Черный список всех известных фишинговых URL-адресов будет иметь размер в сотни мегабайт и должен постоянно обновляться, что делает непрактичным хранить черный список локально на компьютере. Вместо этого антивирусные продукты, использующие фильтрацию на основе URL-адресов, хранят черный список на своих серверах и запрашивают URL-адрес каждый раз, когда пользователь посещаете веб-сайт. Тот факт, что каждый URL-адрес, который пользователь посещает, запрашивается на стороне сервера, означает, что антивирусная компания потенциально может собирать информацию обо всех посещаемых веб-сайтах, если они захотят.

Фильтрация индикации имени сервера

Другой способ предотвращения фишинговых атак - фильтрация сетевого трафика на основе незашифрованных битов HTTPS-соединения, таких как указание имени сервера (SNI). SNI - это расширение протокола TLS, на котором основан HTTPS. Когда используется SNI, клиент отправляет имя хоста, к которому он хочет подключиться, во время первоначального рукопожатия TLS .

SNI не зашифрован, поэтому антивирусное программное обеспечение может видеть хост, к которому пользователь хочет получить доступ, и тем самым определять, является ли он вредоносным. Если программное обеспечение считает хост вредоносным, оно вмешивается и предотвращает загрузку страницы.

Сетевая фильтрация также может включать блокировку трафика на IP-адреса, на которых размещены фишинговые веб-сайты, или даже блокирование диапазонов IP-адресов.

2. Расширения браузера

Расширения браузера - еще один распространенный способ борьбы с фишингом. Браузеры позволяют расширениям перехватывать попытки подключения и получать доступ к содержимому веб-страниц, независимо от того, зашифровано соединение или веб-страница. Расширения браузера несколько ограничены тем фактом, что - в отличие от других методов в этом списке, которые будут работать со всеми приложениями, работающими в вашей системе, - они совместимы только с конкретными браузерами, для которых они были разработаны.

3. Перехватить разрешение имени хоста

Каждое подключенное к Интернету устройство имеет IP-адрес, который представляет собой набор чисел, которые другие машины могут использовать для поиска устройства. Система доменных имен (DNS) помогает преобразовать IP-адрес устройства во что-то более удобное для чтения людьми. Например, google.com запомнить намного проще, чем IP-адрес 173.194.32.195.

Разрешение имени хоста — это процесс, в котором имя хоста (например, google.com) преобразуется в его IP-адрес (73.194.32.195). Некоторые антивирусные программы предотвращают фишинг, прерывая этот процесс, чтобы предотвратить загрузку вредоносных веб-сайтов. Это может быть достигнуто либо путем перехвата пакетов DNS, либо путем настройки DNS-сервера с соответствующими черными списками.

Литература

1. Морозов, М. Атакуют "шнельботы". Германские торпедные катера Второй Мировой / М. Морозов, С. Патянин. - М.: Яуза, 2007. - 110 с.
2. Сорокин, З. Идем в атаку / З. Сорокин. - М.: ДОСААФ, 2016. - 200 с.
3. Стайн, Р.Л. Атака мутанта / Р.Л. Стайн. - М.: Росмэн, 2016. - 107 с.
4. Фостер, Дж.С. Защита от взлома: сокеты, эксплойты, shell-код: выявление уязвимостей операционных систем и прикладных программ к атакам хакеров / Дж.С. Фостер. - М.: ДМК, 2009. - 784 с.
5. Чирилло, Д. Обнаружение хакерских атак / Д. Чирилло. - М.: СПб: Питер, 2010. - 864 с.
6. Якименко, А. В атаке - "Меч" / А. Якименко. - М.: ДОСААФ, 2010. - 240 с.

Literature

1. Morozov, M. Attack "snail boats". German torpedo boats of the Second World War / M. Morozov, S. Patyanin. - M .: Yauza, 2007 .-- 110 p.
2. Sorokin, Z. We go to the attack / Z. Sorokin. - M .: DOSAAF, 2016 .-- 200 p.
3. Stein, R.L. Attack of the mutant / R.L. Stein. - M .: Rosmen, 2016 .-- 107 p.
4. Foster, J.S. Protection against hacking: sockets, exploits, shell-code: identifying vulnerabilities of operating systems and applications to hacker attacks / J.S. Foster. - M .: DMK, 2009 .-- 784 p.
5. Cirillo, D. Detection of hacker attacks / D. Cirillo. - M .: SPb: Peter, 2010 .-- 864 p.
6. Yakimenko, A. In the attack - "Sword" / A. Yakimenko. - M .: DOSAAF, 2010.- 240 p.