АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Вредоносная программа Retefe используется для компрометации пользователей онлайн-банкинга

12 ноября 2016 года

Вредоносная программа под названием Retefe специализируется на компрометации пользователей различных банков, включая Tesco Bank. Его клиенты недавно подверглись массовой компрометации аккаунтов. Retefe используется злоумышленниками для кражи данных онлайн-банкинга, которые затем могут быть использованы с целью осуществления мошеннических операций.

Согласно новостному порталу BBC, за выходные было зафиксировано около 40 тыс. подозрительных банковских транзакций, причем половина из них приходилась на незаконное списание денежных средств. Позже представители Tesco Bank подтвердили, что в результате компрометации пострадало около 9 тыс. клиентов банка.

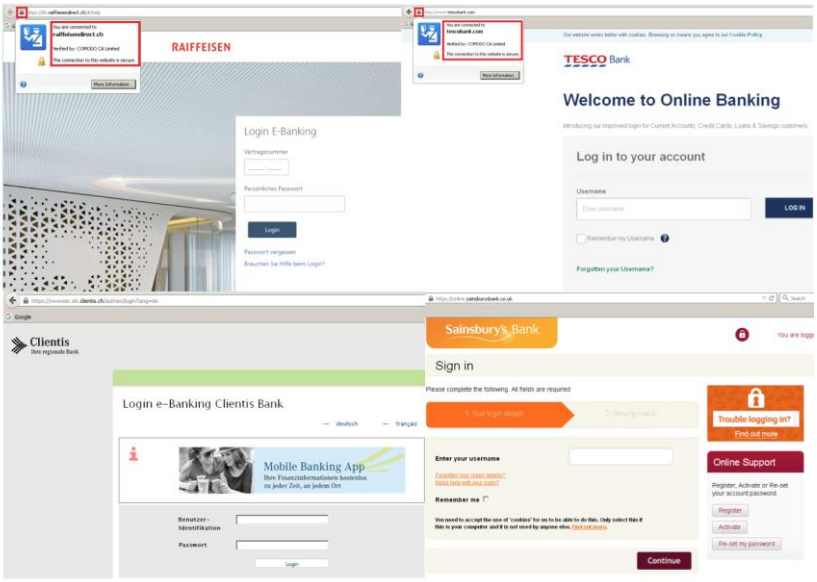
Специалисты по безопасности Tesco Bank решили временно заблокировать возможность проведения транзакций с использованием онлайн-банкинга. В то же время, активными остались такие функции клиентов банка как снятие наличных, платежи с использованием чипа карты и ее PIN-кода, а также прочие операции, связанные с оплатой счетов.

Анализ экземпляров вредоносной программы аналитиками ESET показывает, что она нацелена на компрометацию банков из довольно длинного списка разных стран мира. Отметим, что вредоносная кампания началась, по крайней мере еще в феврале 2016 г. Обратите внимание, что вредоносное ПО Retefe уже активно использовалось злоумышленниками и до этой кампании, но при этом злоумышленники использовали другие методы ее распространения.

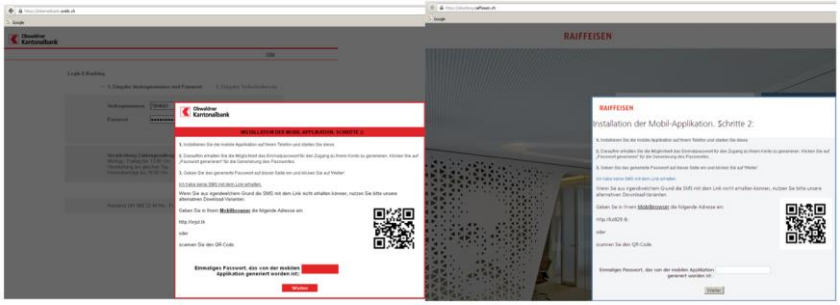
В случае попытки подключения пользователя к системе онлайн-банкинга из списка вредоносной программы на скомпрометированной системе, Retefe модифицирует веб-страницу сайта онлайн-банкинга и пытается украсть конфиденциальные данные для входа в аккаунт.

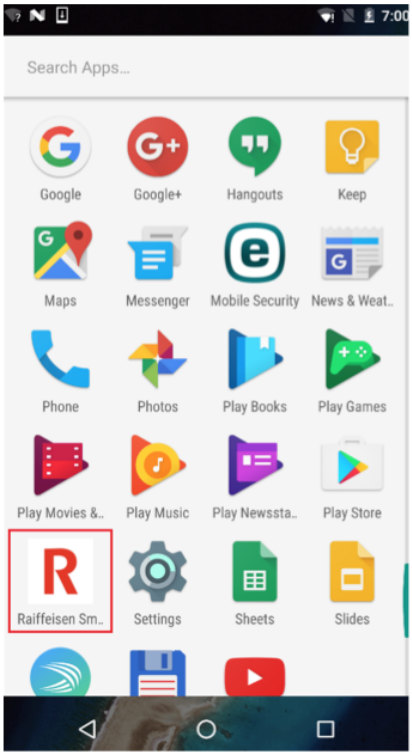
Первоначальное заражение вредоносной программой происходит через файл, который написан на JavaScript и обнаруживается антивирусными продуктами ESET как **JS/Retefe**. В качестве механизма его распространения, злоумышленники выбрали метод вложений сообщений электронной почты, маскируя его под счет-фактуру, уведомление о заказе и др. После запуска, он устанавливает в систему несколько своих компонентов, включая, сервис анонимной сети Tor. Эти вредоносные компонента используются для настройки прокси-сервера при работе с банковскими веб-сайтами.

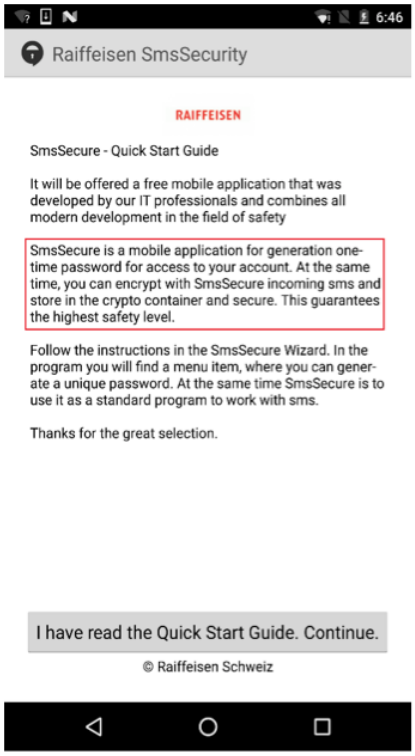
При попытке пользователя получить доступ к сайту онлайн-банкинга, он скрытно перенаправляется на фальшивую копию этого веб-сайта. Retefe также добавляет в систему фальшивый корневой цифровой сертификат, который замаскирован под легитимный. Для маскировки используется фальшивая информация о том, что сертификат был выдан и подтвержден известным центром сертификации Comodo. Этот прием существенно усложняет обнаружение вредоносной активности пользователем. При этом очевидно, что эта проблема не имеет никакого отношения к безопасности определенного банка.

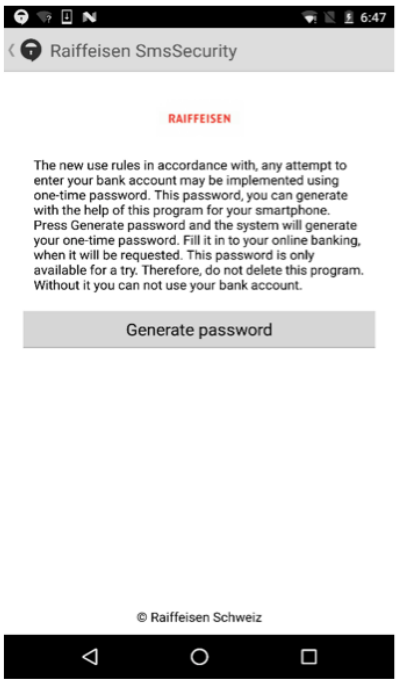


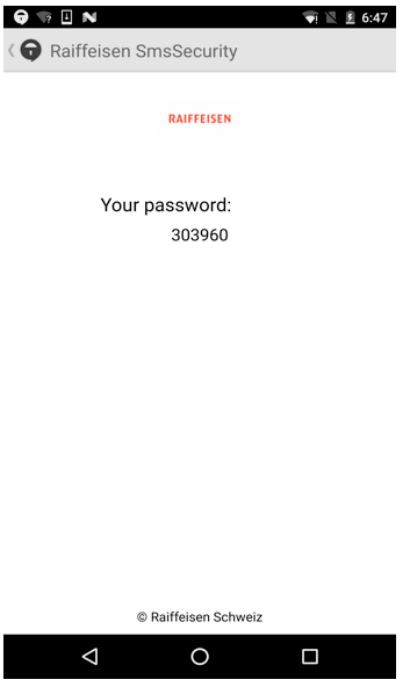
Код вредоносной программы успешно может компрометировать все основные веб-браузеры, включая, Internet Explorer, Mozilla Firefox и Google Chrome. В некоторых случаях, Retefe пытался убедить пользователя установить мобильный компонент, который обнаруживается антивирусными продуктами ESET как Android/Spy.Banker.EZ. Этот мобильный компонент используется для обхода двухфакторной 2FA-аутентификации. Ниже представлены скриншоты этого мобильного компонента.











Аналитики ESET также проанализировали и другой вариант вредоносной программы, который обнаруживается как JS/Retefe.B. Эта модификация использует довольно громоздкий метод доступа к анонимной сети Tor. Он заключается не в использовании сети Tor напрямую, а через сервис Tor2Web.

Retefe находился под объективом антивирусных исследователей и ранее, когда в начале этого года вредоносная программа активно использовалась для компрометации банков Великобритании. С тех пор, авторы добавили в него мобильный компонент, а также расширили список целей.

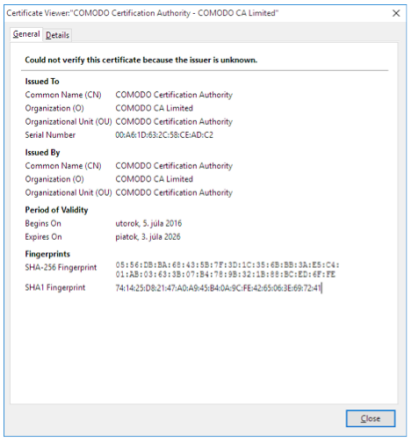
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

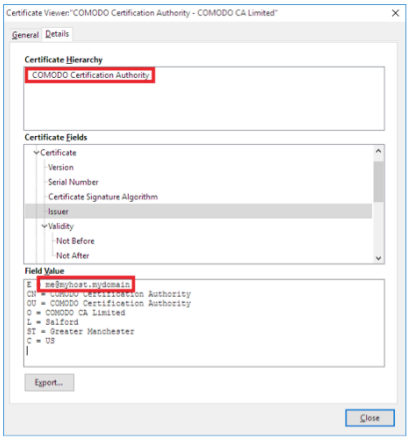
Проверка системы на заражение

Пользователям сервисов онлайн-банкинга, которые указаны ниже, рекомендуется вручную проверить наличие следующих индикаторов компрометации вредоносной программой или же использовать следующую веб-страницу ESET для проверки.

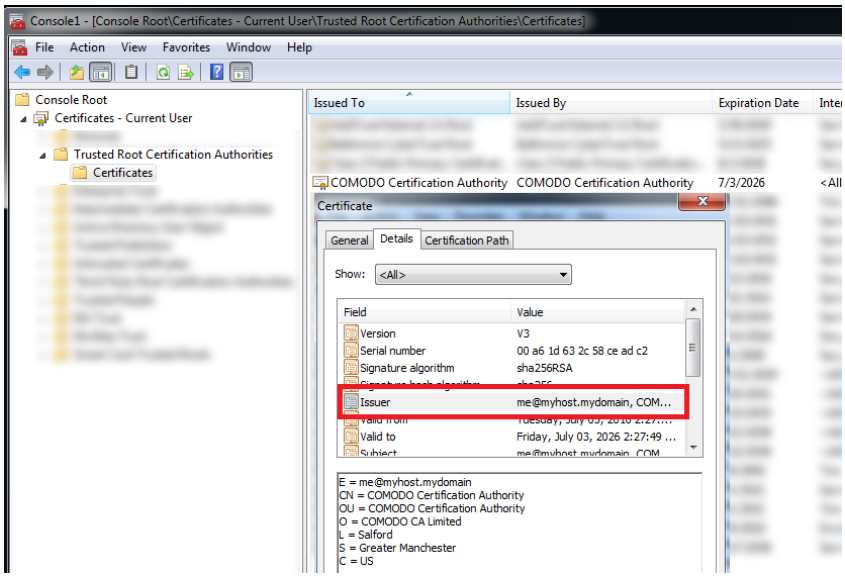
Одним из индикаторов компрометации является присутствие фальшивого корневого цифрового сертификата, который, якобы, был выдан центром сертификации Comodo. При этом адрес электронной почты выдавшей организации соответствует адресу me@myhost.mydomain.

Для веб-браузера Mozilla Firefox следует открыть менеджер сертификатов.





Для прочих веб-браузеров, присутствие сертификата можно проверить с помощью MMC (Microsoft Management Console).



Мы наблюдали два таких фальшивых сертификата, информация о которых представлена ниже.

```
Serial number: 00:A6:1D:63:2C:58:CE:AD:C2
Valid from: Tuesday, July 05, 2016
Expires: Friday, July 03, 2026
Issuer: me@myhost.mydomain, COMODO Certification Authority
```

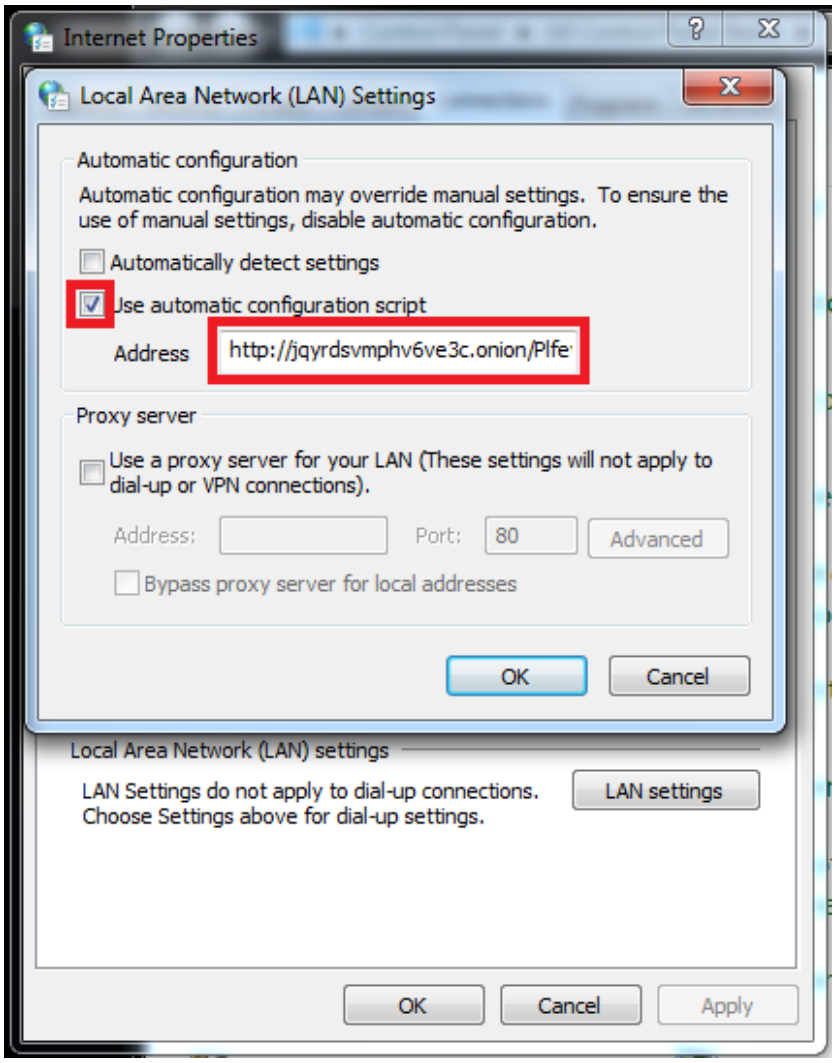
```
Serial number: 00:97:65:C4:BF:E0:AB:55:68
Valid from: Monday, February 15, 2016
Expires: Thursday, February 12, 2026
Issuer: me@myhost.mydomain, COMODO Certification Authority
```

Другим индикатором компрометации является присутствие в системе вредоносного скрипта Proxy Automatic Configuration (PAC), который указывает на следующий .onion домен.

```
hxxp://%onionDomain%/%random%.js?ip=%publicIP%
```

При этом переменная %onionDomain% представляет собой onion домен, произвольно выбранный из конфигурационного файла. Переменная %random% представляет собой строку из восьми символов алфавита A-Za-z0-9. %publicIP% указывает на публичный адрес. Пример такой ссылки представлен ниже.

```
hxxp://e4loi7gufljhzfo4.onion.link/xvsP2YiD.js?ip=100.10.10.100
```

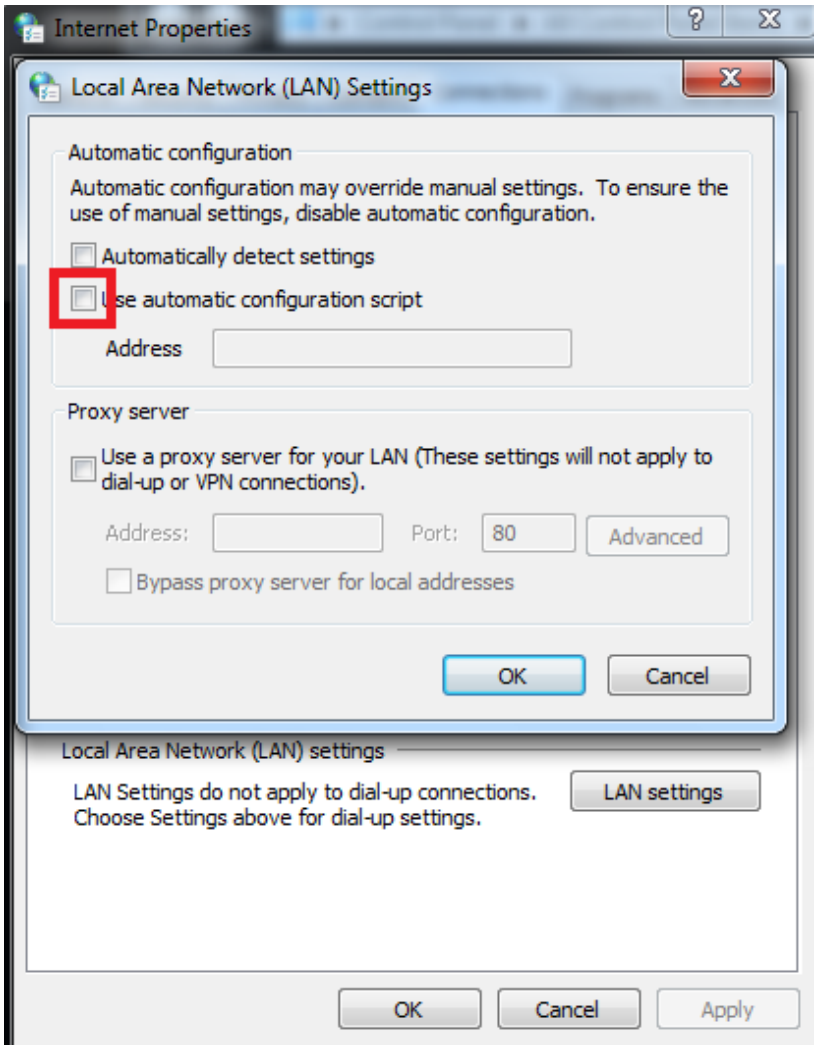


Индикатором компрометации также является присутствие на устройстве под управлением Android вредоносной программы Android/Spy.Banker.EZ.

В случае обнаруженного заражения системы вредоносной программой Retefe, следующие действия нужно выполнить для ликвидации этого заражения.

1. Если вы использовали одну из систем онлайн-банкинга, на компрометацию которой нацелена вредоносная программа, измените свой пароль на доступ в аккаунт онлайн-банкинга, а также проверьте присутствие нелегитимных операций с банковским счетом.

2. Удалите из системы скрипт Proxy Automatic Configuration (PAC)



3. Удалите из системы вышеупомянутый цифровой сертификат.

4. В качестве проактивной защиты используйте надежное средство безопасности с функцией обеспечения безопасности операций онлайн-банкинга.

Ниже представлен список веб-сайтов онлайн-банкинга, на компрометацию которых нацелен Retefe.

*.facebook.com
*.bankaustria.at
*.bawag.com
*.bawagpsk.com
*.bekb.ch
*.bkb.ch
*.clientis.ch
*.credit-suisse.com
*.easybank.at
*.eek.ch
*.gmx.at
*.gmx.ch
*.gmx.com
*.gmx.de

*.gmx.net
*.if.com
*.lukb.ch
*.onba.ch
*.paypal.com
*.raiffeisen.at
*.raiffeisen.ch
*.static-ubs.com
*.ubs.com
*.ukb.ch
*.urkb.ch
*.zkb.ch
*abs.ch
*baloise.ch
*barclays.co.uk
*bcf.ch
*bcj.ch
*bcn.ch
*bcv.ch
*bcvs.ch
*blkb.ch
*business.hsbc.co.uk
*cahoot.com
*cash.ch
*cic.ch
*co-operativebank.co.uk
*glkb.ch
*halifax-online.co.uk
*halifax.co.uk
*juliusbaer.com
*lloydsbank.co.uk
*lloydstsb.com
*natwest.com
*nkb.ch
*nwolb.com
*oberbank.at
*owkb.ch
*postfinance.ch
*rbsdigital.com
*sainsburysbank.co.uk
*santander.co.uk
*shkb.ch
*smile.co.uk
*szkb.ch
*tescobank.com
*ulsterbankanytimebanking.co.uk
*valiant.ch
*wir.ch
*zuercherlandbank.ch
accounts.google.com
clientis.ch
cs.directnet.com

e-banking.gkb.ch
eb.akb.ch
ebanking.raiffeisen.ch
hsbc.co.uk
login.live.com
login.yahoo.com
mail.google.com
netbanking.bcge.ch
onlinebusiness.lloydsbank.co.uk
tb.raiffeisendirect.ch
uko.ukking.co.uk
urkb.ch
wwx.banking.co.at
wwx.hsbc.co.uk
wwx.oberbank-banking.at
wwwsec.ebanking.zugerkb.ch