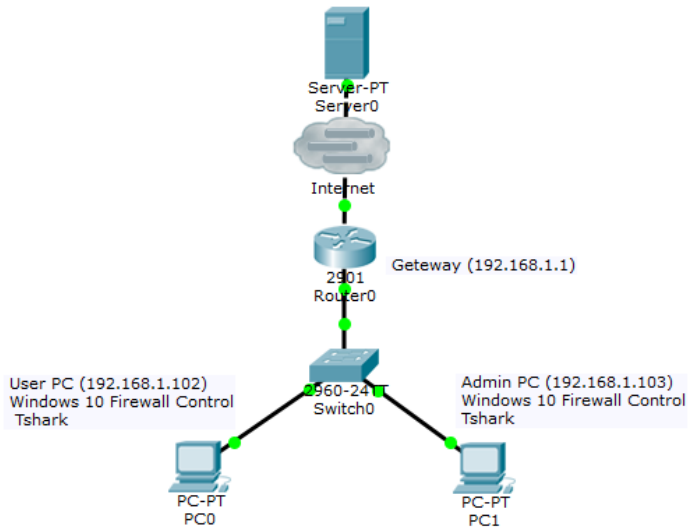
ProtectMaster
Email: info@protectmaster.org
Тел: +380947112959



После недавнего скандала во время обыска в компаниях "Укргазвидобування" и "Dragon Capital" из-за использования программного комплекса “Стахановец”, который якобы передает данные на сервера ФСБ, мы решили самостоятельно проверить правда ли “Стахановец” сливал данные в РФ и более 300 крупных компаний просто не замечали данной утечки.

Лабораторный стенд:

- Для исследований было развернуто 2 виртуальные машины с ОС Windows 10 в режиме сетевого моста.
- Для мониторинга и логирования трафика воспользуемся утилитой Tshark.
- Еще нам пригодится Windows 10 firewall control для логирования создаваемых исследуемым ПО подключений.




На сайте разработчика предлагают скачать пробную версию программного обеспечения, ей и воспользуемся. Полагаем, что пробные версии, как никто сливают статистику разработчику. Для получения пробной версии необходимо заполнить анкету, после чего на почту высылается ссылка для скачивания.

Для программы есть 2 варианта установки:

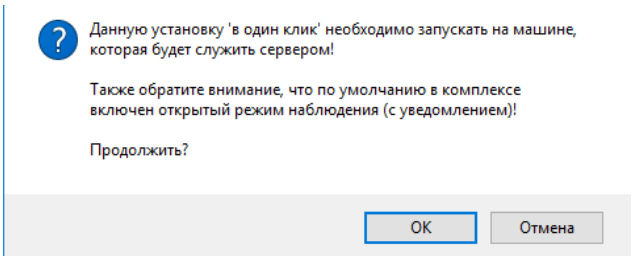
- продвинутая, подразумевает, что необходимо установить и настроить БД и веб интерфейс приложения самостоятельно;
- установка в один клик устанавливает все компоненты на одну машину и задает стандартные настройки для сервера.

| | | | |
|---|---|---|---|
| setup_advanced.exe | 27.04.2017 14:10 | Приложение | 54 619 КБ |
| setup_oneclick.exe | 27.04.2017 14:11 | Приложение | 262 823 КБ |

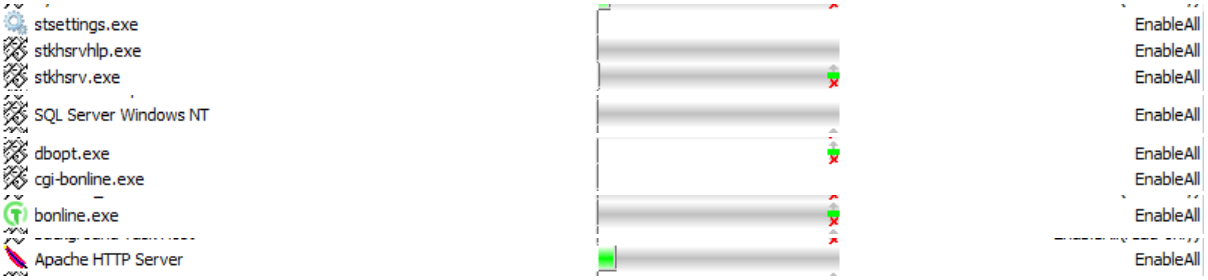
Т.к. опытный пользователь (администратор) скорее всего следит за происходящим в компании и не допустит утечки данных, воспользуемся версией “в

один клик”, возможно это внушит ПО уверенность, что за ним не следят и оно с радостью начнет отправлять данные ФСБ или хотя бы на IP не из нашей локальной сети.

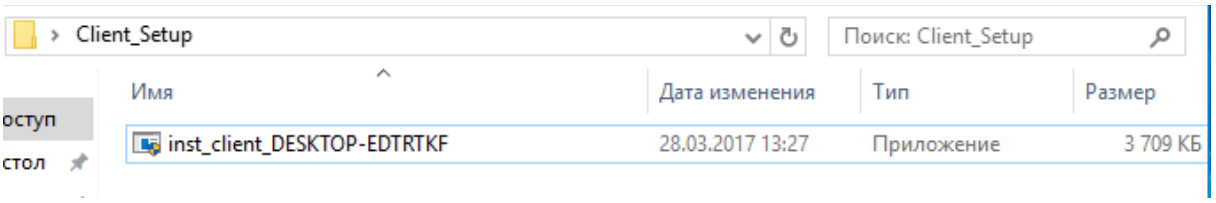
Перед установкой нас предупреждаю, что данная версия программного обеспечения является бесплатной и пользователи, за которыми будет вестись наблюдение, будут знать о том, что за ними следят.



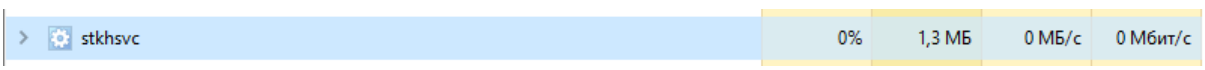

Ниже представлен список процессов, использующих сетевые подключения, которые были добавлены после установки сервера “Стахановец”.



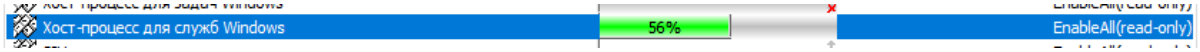

После установки на рабочем столе появится папка с приложение, которое нужно запустить на компьютере, за которым будет осуществлено наблюдение.




Клиентское приложение создает в системе дополнительный процесс, представленный ниже:




С сетью “stkhsvc” общается через “Хост-процесс для служб Windows”.



ProtectMaster
Email: info@protectmaster.org
Тел: +380947112959



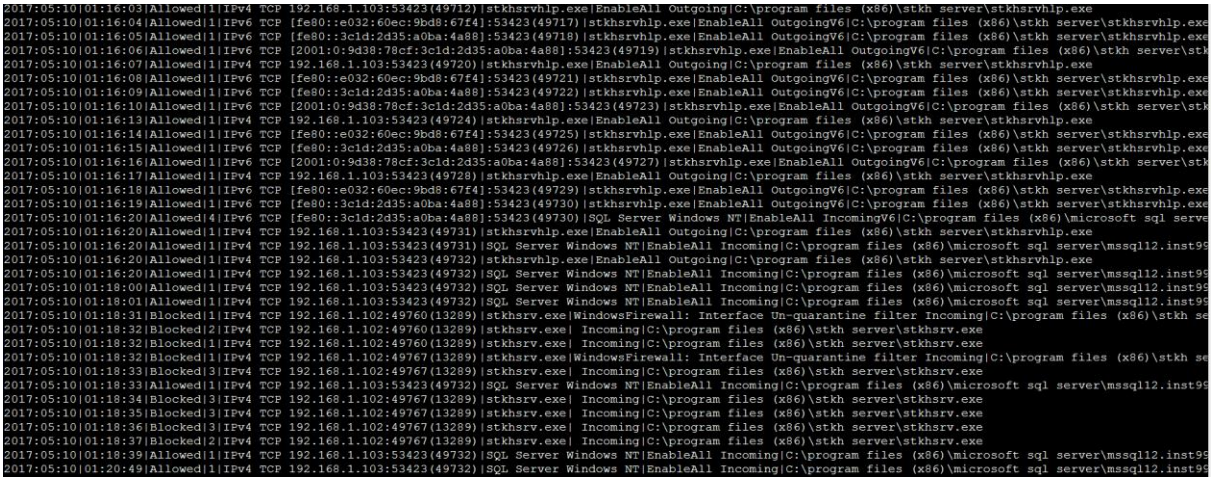
Данная информация пригодится, чтобы проанализировать логи брандмауэра на предмет подключений к внешним IP.

Разрешим всем созданным сервисам доступ к локальной сети и сети интернет и включаем логирование всех подключений? используя Windows 10 firewall control. Также запустим tshark на запись всего трафика.

Периодически на протяжении 3х дней будем имитировать работу, создавая документы, читая почту и новости в соц. сетях. И как очень строгий начальник будем следить за своими действиями, используя различные функции “Стахановец”.

По истечении 3х дней работы проанализируем собранные данные. Для серверной машины все проще, т.к. мы легко можем отделить трафик “Стахановца” от остальных приложений по названию процессов, которые нас интересуют. В логах не оказалось запросов на какие-либо сервера вне локальной сети.

*На скриншоте ниже представлен пример логовов, созданных windows 10 firewall control*




На клиентской машине, т.к. “Хост-процесс для служб” используется не только “stkhsvc”, но множеством системных служб, необходимо проверить кому принадлежат IP адреса, к которым обращался “Хост-процесс для служб Windows”. После удаления дубликатов, локальных, multicast и broadcast осталось 53 IP адреса, местоположение серверов проверено через https://www.maxmind.com/ru/geoip-demo.

*Представлена только часть IP, чтобы не перегружать отчет информацией.*

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 157.56.120.207 | IE | Дублин, Ленстер, Ирландия, Европа | | 53.3389, -6.2595 | 1000 | Microsoft Corporation | Microsoft Azure | outlook.com | |
| 40.77.229.13 | IE | Дублин, Ленстер, Ирландия, Европа | | 53.3389, -6.2595 | 1000 | Microsoft Corporation | Microsoft Azure | windows.com | |
| 131.253.61.80 | US | США, Северная Америка | | 37.751, -97.822 | 1000 | Microsoft Corp | Microsoft Corporation | | |
| 104.111.244.140 | NL | Амстердам, Северная Голландия, Нидерланды, Европа | 1091 | 52.35, апр.67 | 100 | Akamai Technologies | Akamai Technologies | akamaitechnologies.com | |

В таблице оказались такие названия:

- Microsoft Corporation
- Microsoft Corp
- Akamai Technologies
- First Telecommunication Center LLC
- Level 3 Communications
- Dataline LLC
- Microsoft bingbot
- Facebook Ireland Ltd
- Microsoft Limited

Но ничего связанного с ФСБ или Российской Федерацией, если судить по названию нет.

Подобная описанной выше операция была проведена с трафиком, записанным tshark. Для выделения всех IP из трафика можно использовать команду:

```
tshark -r <input file> -T fields -e ip.dst -e ip.src > path\output.txt
```

Также, как и в прошлом случае среди стран, которым отправлялись данные были США, Нидерланды, Ирландия, но небыло Российской Федерации.

**Заключение:**

Конечно, подобный эксперимент не являются доказательством того, что “Стахановец” не отправлял данные. И больше носит повествовательный характер. Однако дает небольшой “плюс один” ко мнению, что разработчиков решили оклеветать.

Конечно, у компаний, к которым пришли доблестные сотрудники, могла быть установлена совершенно другая версия той же программы, в которой есть функционал для слежения, но поверить, что системные администраторы подобных компаний не замечали утечек, крайне сложно.

Платная версия программы наверняка может попадать под определение “ШПЗ” из-за возможности **скрыто** следить за действиями пользователя, однако каких-либо свидетельств, что в открытой демо версии информация идет куда-то, кроме сервера приложения, в ходе эксперимента не выявлено.

**P.S.** Дампы, использованные в данном эксперименте, решено не выкладывать, чтобы не раскрывать IP некоторых сервисов, у желающих не должно возникнуть проблем при желании повторить эксперимент.