АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Деятельность кибергруппы Sednit под микроскопом – часть 2

26 октября 2016 года

Наши специалисты опубликовали вторую часть детального исследования деятельности и вредоносного ПО кибергруппы Sednit. В предыдущей части мы публиковали информацию о фишинговых сообщениях и механизмах компрометации пользователей со стороны этой группировки, а также упомянули используемые ими эксплойты. В новой части нашего исследования речь пойдет о вредоносном ПО, которое используется Sednit для компрометации пользователей.

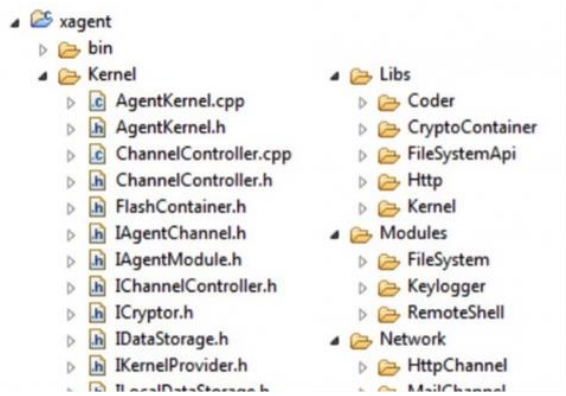
Группировка специализируется на компрометации только тех целей, которые заранее были выбраны для кибератаки, то есть кибератака носит направленный характер и осуществляется после проведенной разведки этих целей. Вредоносный инструмент (toolkit) авторов состоит из трех основных компонентов: бэкдоров SEDRECO, XAGENT и сетевого агента XTUNNEL.

Злоумышленники используют для компрометации жертв оба бэкдора, что позволяет одному из них оставаться активным даже в том случае, если другой будет обнаружен антивирусным продуктом. Таким образом, это дает им дополнительную уверенность в том, что контроль над системой жертвы не будет потерян.

Бэкдор SEDRECO предоставляет операторам Sednit выполнять различные операции на скомпрометированной системе, включая, чтение и запись файлов, отслеживание нажатий клавиш клавиатуры, осуществлять поиск файлов в системе и на сетевых ресурсах. Специалисты ESET также установили, что SEDRECO может использовать в своих целях специальные плагины, которые передаются ему управляющим C&C-сервером.

Бэкдор SEDRECO использует программный код, который мы наблюдали и в другом бэкдоре группировки Sednit под названием XAGENT. XAGENT помогает операторам извлекать интересующую их информацию из зараженной системы посредством протокола HTTP или сообщений электронной почты. Он также может взаимодействовать с другим компонентом под названием USBSTEALER, который специализируется на краже данных с изолированных air-gapped

компьютеров. Нашим специалистам удалось получить исходный код компонента XAGENT, который работает на Linux.

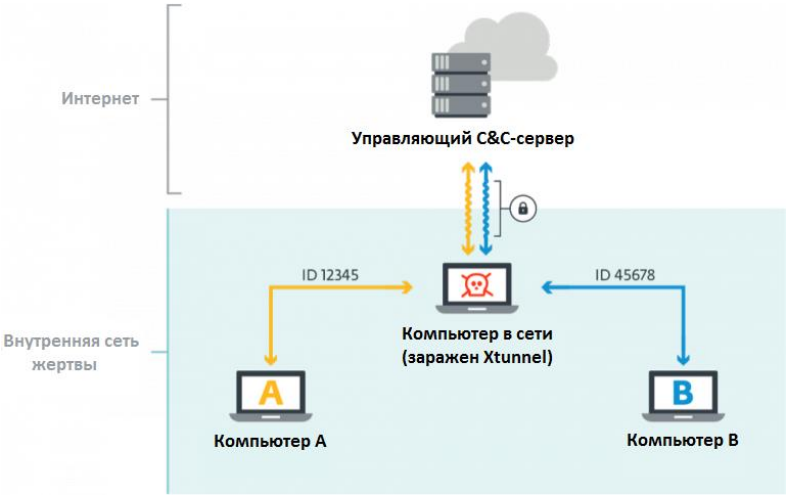


Как известно, различные модификации XAGENT активно используются кибергруппировкой с ноября 2012 г. по настоящее время. В число жертв этого бэкдора входят компьютеры руководящего органа Демократической партии США Democratic National Committee (DNC).

Хотя наши специалисты наблюдали версии бэкдора XAGENT для таких платформ как Windows, Linux и iOS, скорее всего, существует версия этого вредоносного ПО и для Android.

Хорошо продуманное авторами вредоносное ПО XAGENT состоит из нескольких модулей, обеспечивающих различные функциональные возможности. Этот фактор, а также свойства, исследованных специалистами ESET образцов вредоносного ПО, показывают, что атакующие адаптировали каждую кибератаку на конкретную цель. Это помогает злоумышленникам минимизировать риск раскрытия всего кода XAGENT для антивирусных аналитиков.

Другой упомянутый выше компонент под названием XTUNNEL представляет собой инструмент сетевого прокси, который используется операторами для перенаправления сетевого трафика из сети жертвы на свои серверы.



Первый известный экземпляр XAGENT датируется маем 2013 г., более поздние его экземпляры были найдены на серверах Комитета демократической партии DNC в мае 2016 г. и немецкого парламента в июне 2015 г., причем авторы продолжают развивать код вредоносной программы. Наши эксперты подтвердили, что в разработку XTUNNEL, SEDRECO и XAGENT были вложены значительные ресурсы.

Sednit опирается на Xagent и Sedreco для осуществления кибершпионской деятельности. Обе вредоносные программы интенсивно развивались в течение последних лет. Схожие усилия были вложены и в разработку Xtunnel. Эти вредоносные инструменты являются ключевыми для понимания деятельности Sednit.

Однако, было бы не совсем правильным представлять себе, что группировка опирается только на эти инструменты. Например, они также могут использовать на скомпрометированных компьютерах инструменты сбора паролей, некоторые из которых создаются авторами под конкретную атаку. То же самое касается инструментов для захвата скриншотов рабочего стола.

Полную версию второй части нашего исследования можно прочитать здесь.