АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Сайт Ammyy Admin снова скомпрометирован

11 июля 2018 года

Предупреждаем пользователей, скачивавших 13-14 июня с официального сайта программу для удаленного доступа Ammyy Admin. Сайт разработчика был скомпрометирован, в этом временном интервале с него раздавалась троянизированная версия программы. Еще один нюанс: атакующие использовали для маскировки вредоносной сетевой активности бренд Чемпионата мира по футболу.

В октябре 2015 года сайт, предлагающий бесплатную версию Ammyy Admin, уже использовался для распространения вредоносного ПО. Прошлую атаку мы связываем с известной кибергруппой Buhtrap. Сейчас история повторяется. Мы зафиксировали проблему вскоре после полуночи 13 июня, раздача малвари продолжалась до утра 14 июня.

Удаленное администрирование и бот Kasidet в комплекте

Пользователи, скачавшие Ammyy Admin 13-14 июня, получили комплект из легитимного софта и многоцелевого трояна, который детектируется продуктами ESET как Win32/Kasidet. Рекомендуем потенциальным жертвам просканировать устройства с помощью антивирусного продукта.

Win32/Kasidet – бот, который продается в даркнете и активно используется различными кибергруппами. Сборка, обнаруженная на сайте ammyy.com 13 и 14 июня 2018 года, имела две функции:

1. Кража файлов, которые могут содержать пароли и другие данные авторизации для криптовалютных кошельков и аккаунтов жертвы. С этой целью малварь ищет следующие имена файлов и отправляет их на C&C-сервер:
— bitcoin
— pass.txt
— passwords.txt
— wallet.dat

2. Поиск процессов по заданным именам:
— armoryqt
— bitcoin
— exodus
— electrum
— jaxx
— keepass
— kitty
— mstsc
— multibit
— putty
— radmin
— vsphere
— winscp
— xshell

URL-адрес C&C-сервера (`hxxp: // fifa2018start [.] Info / panel / tasks.php`) также представляет интерес. Похоже, что атакующие решили использовать бренд Чемпионата мира по футболу для маскировки вредоносной сетевой активности.

Мы обнаружили сходство с атакой 2015 года. Тогда злоумышленники использовали ammyy.com, чтобы раздавать несколько семейств вредоносных программ, меняя их почти каждый день. В 2018 году распространялся только Win32/Kasidet, однако обфускация полезной нагрузки менялась в трех случаях, вероятно, чтобы избежать обнаружения антивирусными продуктами.

Еще одно сходство между инцидентами – идентичное имя файла, содержащего полезную нагрузку – `Ammyy_Service.exe`. Загруженный установщик AA_v3.exe может выглядеть легитимным на первый взгляд, однако атакующие использовали SmartInstaller и создали новый бинарный файл, который сбрасывает `Ammyy_Service.exe` до установки Ammyy Admin.

Выводы

Поскольку это не первый случай компрометации сайта ammyy.com, рекомендуем установить надежное антивирусное решение до загрузки Ammyy Admin. Мы сообщили разработчикам Ammyy Admin о проблеме.

Ammyy Admin – легитимный инструмент, однако им нередко пользовались злоумышленники. В результате некоторые антивирусные продукты, включая ESET, детектируют его как потенциально нежелательное приложение. Однако этот софт по-прежнему широко используется, в частности, в России.

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Индикаторы компрометации

Детектирование продуктами ESET
Win32/Kasidet

Хеши SHA-1

Установщик:
6D11EA2D7DC9304E8E28E418B1DACFF7809BDC27
6FB4212B81CD9917293523F9E0C716D2CA4693D4
675ACA2C0A3E1EEB08D5919F2C866059798E6E93

Win32/Kasidet:
EFE562F61BE0B5D497F3AA9CF27C03EA212A53C9
9F9B8A102DD84ABF1349A82E4021884842DC22DD
4B4498B5AFDAA4B9A2A2195B8B7E376BE10C903E

C&C-сервер
fifa2018start[.]info