За российскими дипломатами 7 лет следят с помощью шпионского ПО - CNews

By Роман Георгиев

Published: 2019-10-11 · Archived: 2026-04-05 22:00:09 UTC

11 Октября 2019 11:51 11 Окт 2019 11:51 |

Компания ESET выявила кампанию кибершпионажа, нацеленную на русскоязычных дипломатов и чиновников. Операторов особенно интересовали их телефоны, в том числе самые старые.

Протокол AT и сеть Tor

Компания ESET объявила об обнаружении шпионской кампании, нацеленной на российских дипломатов и государственные ведомства. Кампания длится около семи лет.

Шпионское ПО, получившее название Attor, обладает рядом специфических и довольно редко наблюдаемых функций. Среди них - использование зашифрованных модулей, коммуникации с операторами через сеть Tor, а также плагин, разработанный для создания цифровых отпечатков GSM-устройств с использованием протокола AT.

Злоумышленники сфокусировали свое внимание на дипломатических и государственных учреждениях. По информации ESET, атаки производятся самое позднее с 2013 г., и направлены в первую очередь на тех, кто особенно заинтересован в защите своей конфиденциальности.

Модульный шпионаж

Шпионская платформа, как ее назвали эксперты, имеет модульный характер; отдельные элементы отвечают за конкретные задачи. Эксперты выявили восемь модулей (или плагинов): первый отвечает за установку и сохранность вредоноса в системе, второй функционирует как системный монитор, третий как средство записи аудио; также выявлены инструмент для снятия скриншотов, кейлоггер, который также сохраняет содержимое буфера обмена, средство выгрузки файлов, диспетчер команд и модуль связи с C&C-сервером.

Кибершпионская кампания, нацеленная на русскоязычных дипломатов, длится, начиная с 2013 года

Attor демонстрирует особенную заинтересованность в конкретных процессах, особенно тех, которые связаны с российскими социальными сетями и шифровальными утилитами. Также его интересуют процессы VPN-сервисов, защищенные почтовые клиенты Hushmail и The Bat! и утилита для шифрования дисков TrueCrypt.

Библиотеки вредоносной программы существуют на жестком диске только в сжатом и зашифрованном виде: разархивирование происходит только в оперативной памяти. Вероятно, таким образом авторы вредоноса надеялись предохранить его от обнаружения, и последние семь лет им удавалось этой цели достичь.

Attor также обладает рядом механизмов для загрузки и подключения новых плагинов, самообновления и автоматической выгрузки собранных данных на сервер операторов.

Скрытый арсенал

Системный монитор Attor привлек наибольшее внимание исследователей: как выяснилось, этот модуль использует метаданные файлов для создания цифровых отпечатков каждого устройства, используя при этом команды протокола AT, разработанного еще в 1980 г. для установления связи с GSM/GPRS-модемами и телефонами, подключенными в данный момент к компьютеру. По мнению экспертов ESET, целью авторов Attor было обнаруживать старые модемы и телефоны, и получение важных сведений о них - таких как IMEI, IMSI, MSISDN. По-видимому, в дальнейшем операторы Attor, используя эти данные, дополняли основной вредонос специализированными плагинами для вывода данных уже с этих конкретных устройств.

К настоящему времени ESET удалось проанализировать несколько десятков случаев заражения. Тем не менее, выяснить первоначальный вектор заражения и установить полный спектр данных, выводом которых занимается Attor, до сих пор не удалось. Эксперты ESET полагают, что восемь выявленных плагинов для Attor - также лишь часть его арсенала.

«Совершенно очевидный случай продвинутого кибершпионажа, - считает **Олег Галушкин**, генеральный директор компании SEC Consult Services. - По всей видимости, разработкой занималась спецслужба не слишком дружественного РФ иностранного государства, о чем прямо свидетельствует эффективность киберкампании и то, что ее в течение нескольких лет не удавалось обнаружить. Однако конкретная атрибуция в таких случаях - крайне проблемная и, в конечном счете, неблагодарная вещь».

- Как сопровождать СУБД на множестве серверов баз данных

Роман Георгиев
