Правоохранители решили подойти к расследованию творчески.

Международный альянс правоохранительных органов развернул масштабную операцию под кодовым названием Endgame для поимки главаря одного из крупнейших ботнетов — Emotet – это тип вредоносного ПО, которое похищает конфиденциальную информацию из зараженных систем, такую как учетные данные для входа, финансовые данные и т.д. Emotet в основном распространяется через спам-письма, содержащие вредоносные вложения или ссылки на вредоносные веб-сайты. Emotet также может загружать дополнительные вредоносные программы на зараженные системы, которые могут быть использованы для различных вредоносных целей." data-html="true" data-original-title="Emotet" >Emotet.

В сети появился видеоролик, на котором оперативники призывают предоставить любые сведения о личности хакера, известного под прозвищем «Odd». Эта фигура использовала множество псевдонимов на протяжении многих лет.

В ролике кратко излагается история Emotet — сети зараженных компьютеров, дважды становившейся целью правоохранителей.

Призыв о содействии последовал после серии успешных операций на этой неделе, в ходе которых были арестованы члены хакерских группировок, занимавшихся распространением вредоносного ПО. Об этих достижениях правоохранители рассказали в предыдущих видеороликах.

Из косвенной информации следует, что у следствия уже есть некоторые зацепки относительно Odd. Органы указывают на наличие данных о его возможных сообщниках и предполагают, что он может быть вовлечен и в другие противоправные операции помимо Emotet. Впрочем, детали не разглашаются.

Несмотря на то, что Ботнет — это совокупность подключенных к Интернету устройств, которые могут включать персональные компьютеры (ПК), серверы, мобильные устройства и устройства Интернета вещей (IoT), которые заражены и контролируются вредоносным ПО без ведома их владельца." data-html="true" data-original-title="Ботнет" >ботнет Emotet действует около десяти лет, о реальных личностях, стоящих за ним, достоверно почти ничего не известно. Компания ESET связывает его с хакерской группировкой Mealbybug или TA542, в зависимости от источника. Но в докладе CISA эти группы не фигурируют.

Гораздо лучше задокументированы масштабы угрозы, которую Emotet представлял для

киберпространства годами. Начав как обычный банковский троян, он разросся в один из самых крупных ботнетов в интернете, служивший платформой для распространения других вредоносов, загрузчиков и программ-вымогателей.

После первой попытки обезвредить Emotet в январе 2021 года немецкие власти использовали инфраструктуру самого ботнета для распространения антивируса, удалявшего зловред с зараженных машин. Этот спорный шаг противоречил политике других стран, например, Великобритании.

В ноябре того же года Emotet возобновил активность после 10-месячного перерыва, но уже при помощи инфраструктуры ботнета TrickBot — ситуация обратная той, когда ранее TrickBot распространялся через Emotet. Тем не менее, восстановить прежние масштабы Emotet так и не удалось, и в настоящее время все его командные серверы отключены.

Насколько правоохранители осведомлены о текущей деятельности Odd, пока не ясно. Но известно, что в последнее время такие операции зачастую применяют тактику психологического давления на киберпреступников.

Сначала это коснулось группировки LockBit — ее предполагаемого лидера длительное время преследовали издевательскими публикациями. Теперь очередь дошла до самой операции Endgame — ее объявления разделены на отдельные эпизоды, наподобие сериала. Правоохранители используют против хакеров их же методы, вроде обратных отсчетов.

Согласно таймеру на сайте Endgame, следующий видеоролик с новыми подробностями операции ожидается 5 июня.

На перекрестке науки и фантазии — наш канал