«Operation Endgame» наносит мощный удар по IcedID, Pikabot, Smokeloader и прочим цифровым угрозам.

С 27 по 29 мая 2024 года в рамках международной правоохранительной операции под кодовым названием «Operation Endgame» (операция «Конец игры») было захвачено более 100 серверов, используемых для крупных вредоносных кампаний с использованием таких программ, как IcedID, Pikabot, Trickbot, Bumblebee, Smokeloader и SystemBC.

Полицией было проведено 16 обысков в разных странах Европы, что привело к аресту четырёх человек: одного в Армении и трёх в Украине. Кроме того, правоохранителям удалось идентифицировать восемь беглецов, связанных с этими операциями. Уже в ближайшее время они будут добавлены в список «Самых разыскиваемых преступников» Европола.

Основным инструментом киберпреступников были так называемые «дропперы» — специализированные программы, которые обеспечивают первоначальный доступ к устройствам. Эти программы, первоначально разработанные как банковские трояны, эволюционировали и теперь используются для доставки более опасных компонентов, таких как программы для кражи информации и программы-вымогатели.

Киберпреступники рассылали вредоносные электронные письма или скрывали вредоносное ПО в установщиках, распространяемых через рекламные сети и торрент-трекеры. Они применяли тактики уклонения, такие как обфускация кода и имитация легитимных процессов, чтобы избежать обнаружения.

Изъятая полицией инфраструктура включала более 2000 доменов, использовавшихся для незаконных кибероперациий, и теперь находится под контролем властей. В «Operation Endgame» приняли участие полицейские силы Германии, США, Великобритании, Франции, Дании и Нидерландов.

Поддержка была оказана экспертами из Bitdefender, Cryptolaemus, Sekoia, Shadowserver, Team Cymru, Prodaft, Proofpoint, NFIR, Computest, Northwave, Fox-IT, HaveIBeenPwned, Spamhaus и DIVD.

«В ходе расследований было установлено, что один из главных подозреваемых заработал не менее 69 миллионов евро в криптовалюте, сдавая в аренду криминальные инфраструктурные площадки для развёртывания программ-вымогателей», — говорится

в заявлении Европола.

Дополнительная информация о подозреваемых и самой операции будет опубликована на специальном портале Европола сегодня в 17:00 по МСК.