ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ РЕАЛИЗАЦИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Макатерчик А.В.[1]

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Маликов В.В. – канд. тех. наук

Аннотация. Программы-вымогатели (англ. – Ransomwhere) являются распространенным типом вредоносного программного обеспечения (ВПО). Для блокирования преступной деятельности злоумышленников, а также изучения способов идентификации конкретного ВПО можно использовать подход, основанный на анализе технологий реализации ВПО, в том числе количественных данных, используемых при криминальных платежах.

Ransomwhere или программы-вымогатели остаются самым распространенным видом вредоносного программного обеспечения (ВПО), несмотря на определенное снижение числа подобных атак, вызванное повышенным вниманием со стороны правоохранительных органов, арестом участников хакерских групп – операторов RaaS (RaaS, «вымогатель как услуга») [1].

За период существования шифровальщиков был наработан и комплекс мер по противодействию данным видам атак, восстановлению информации жертв таких атак и блокированию преступной деятельности злоумышленников.

Данные меры реализуются как крупными компаниями и организациями, так и на инициативе отдельных физических лиц. Так проект Майкла Гиллеспи ID-Ransomware, созданный в начале 2016 года позволяет по полученной записке с требованием выкупа устанавливать семейство ВПО, которое атаковало системы жертвы, и указания по восстановлению файлов. В 2021 году проект ID-Ransomware уже активно используется специалистами по реагированию на инциденты.

Для блокирования преступной деятельности злоумышленников, а также изучения способов идентификации конкретного ВПО можно использовать подход, основанный на анализе технологий реализации ВПО.

Исследование выполнено в отношении следующего ВПО: Netwalker (Maito), Qlocker, REvil/Sodinokibi, WannaCry.

В ходе исследования были сформированы структурные и функциональные схемы исследуемых ВПО, некоторые из которых представлены на рисунке 1 и 2.

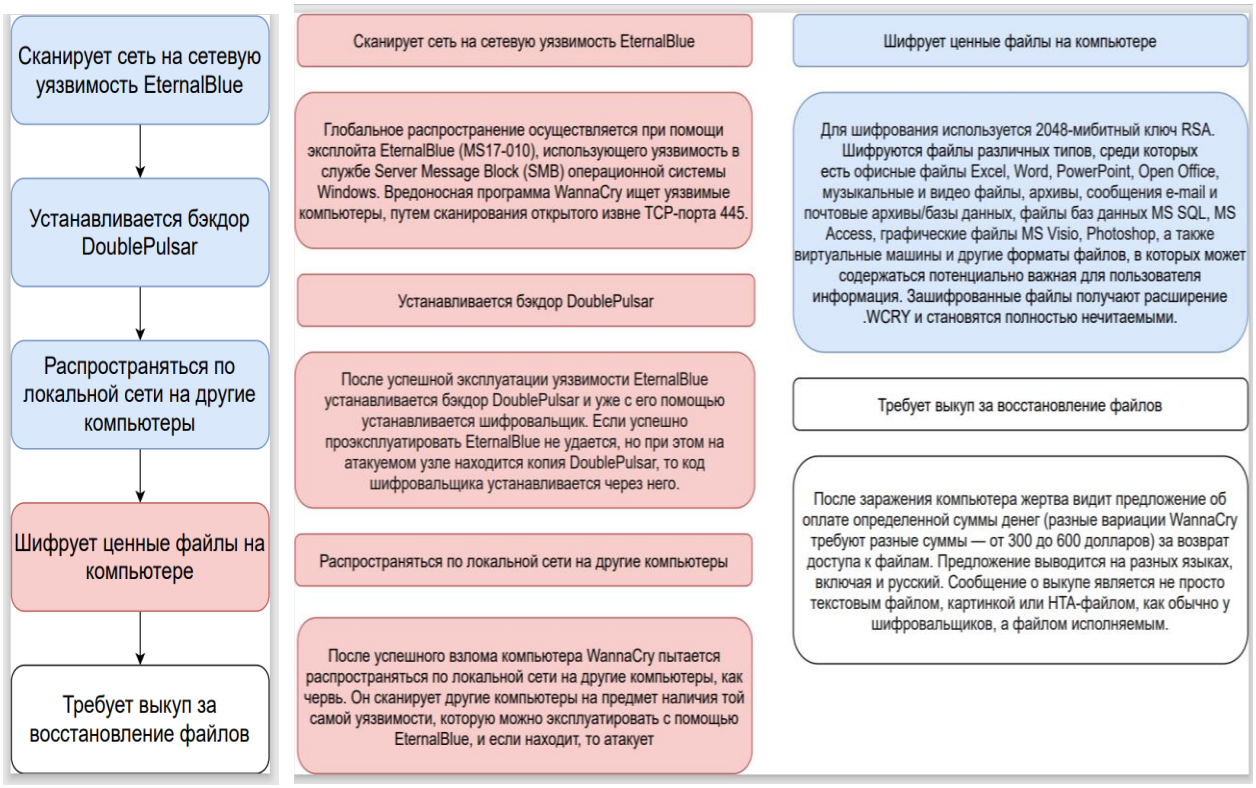

Рисунок 1 – Структурная и функциональная схема WannaCry

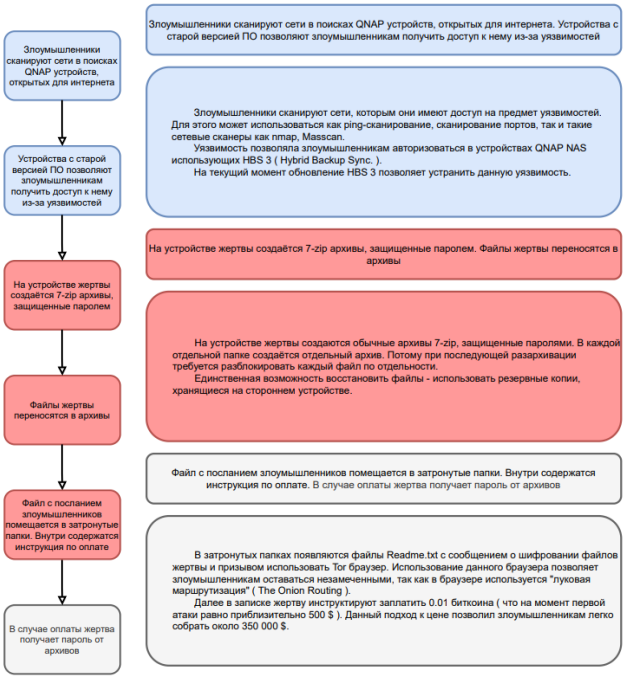

Рисунок 2 – Структурная и функциональная схема WannaCry

По результатам исследования можно сделать вывод: операторами ВПО используется одинаковая схема экономического функционирования (рисунок 3) детальное исследование которой позволяет установить, что для блокировки деятельности операторов достаточно эффективным может являться создание систем обнаружения и блокировки инструментов совершения криминальных платежей.

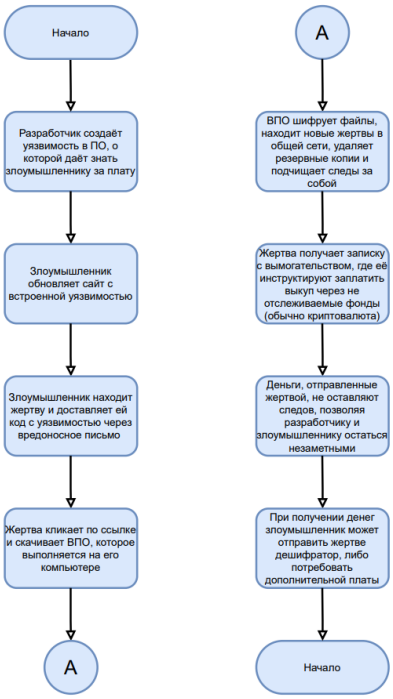

Рисунок 3 – Схема экономического функционирования RaaS

Список использованных источников:

1. Positive Technologies: число уникальных кибератак снизилось впервые за несколько лет — «Хакер»// https://xakep.ru/ [Электрон. ресурс]. – 2022. – Режим доступа: https://xakep.ru/2021/12/09/third-quarter-stats/. – Дата доступа: 07.03.2022.

2. Ransomwhere // https://ransomwhe.re [Электрон. ресурс]. – 2020. – Режим доступа: https://ransomwhe.re/#browse. – Дата доступа: 15.03.2022.

3. ID Ransomware // https://id-ransomware.malwarehunterteam.com/ [Электрон. ресурс]. – 2020. – Режим доступа: https://id-ransomware.malwarehunterteam.com/ – Дата доступа: 15.03.2022.