УДК 004.056.5

**ПОЯВЛЕНИЕ И ДЕЙСТВИЕ ПРОГРАММ-ВЫМОГАТЕЛЕЙ НА СОВРЕМЕННОМ ЭТАПЕ**

Шаламова Е. А.

Научный руководитель к. п. н., доцент Е. А. Васкина

*Федеральное государственное казенное образовательное учреждение высшего образования «Восточно-Сибирский институт Министерства внутренних дел Российской Федерации»,
г. Иркутск*

*Аннотация:* В современном мире угрозы поступают из различных источников, преступность вышла на информационный уровень. Злоумышленники незаметно атакуют устройства и похищают персональные данные, информацию, иные материалы. В данной работе рассмотрен один из видов киберугроз - программы-вымогатели. Описаны основные разновидности программ-вымогателей и особенности их реализации.

*Ключевые слова:* атака, киберугроза, программа-вымогатель, киберпреступник, безопасность, информация.

Программа-вымогатель – это вредоносное ПО, предназначенное для отказа пользователю или организации в доступе к файлам на их компьютере. [2] Шифруя эти файлы и требуя выкуп за ключ дешифрования, кибератакеры ставят организации в положение, когда выплата выкупа является самым простым и дешевым способом восстановить доступ к их файлам. Некоторые варианты добавили дополнительные функциональные возможности, такие как кража данных, чтобы обеспечить дополнительный стимул для жертв вымогателей платить выкуп.

Программы-вымогатели быстро стали самым заметным типом вредоносного ПО. Недавние атаки вымогателей повлияли на способность больниц предоставлять важнейшие услуги, нанесли ущерб общественным службам в городах и значительный ущерб различным организациям.

Современное увлечение программами-вымогателями началось со вспышки WannaCry (сетевой червь) в 2017 году. [1] Эта крупномасштабная и получившая широкую огласку атака продемонстрировала, что атаки с использованием программ-вымогателей были возможными и потенциально прибыльными. С тех пор были разработаны десятки вариантов программ-вымогателей, которые использовались в различных атаках.

Пандемия COVID-19 также способствовала недавнему росту числа программ-вымогателей. Поскольку организации быстро перешли на удаленную работу, в их киберзащите образовались бреши. В 3 квартале 2020 года количество атак программ-вымогателей увеличилось на 50% по сравнению с первой половиной того же года. [6]

Существуют десятки вариантов программ-вымогателей, каждый со своими уникальными характеристиками. Однако некоторые группы вымогателей оказались более плодовитыми и успешными, чем другие, что выделяет их из общего количества.

Ryuk является примером очень целенаправленного варианта программы-вымогателя. Обычно Ryuk доставляет с помощью фишинговых электронных писем или с использованием скомпрометированных учетных данных пользователя для входа в корпоративные системы с использованием протокола удаленного рабочего стола. Как только система заражена, Ryuk шифрует определенные типы файлов (избегая тех, которые важны для работы компьютера), а затем предъявляет требование о выкупе.

Ryuk хорошо известен как один из самых дорогих видов программ-вымогателей из числа существующих. Ryuk может требовать выкуп, в среднем превышающий 1 миллион долларов.[4] В результате киберпреступники, использующие Ryuk, в первую очередь сосредотачиваются на предприятиях, которые располагают ресурсами, необходимыми для удовлетворения таких потребностей.

Следующая программа-вымогатель The [Maze](https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/maze-ransomware-double-extortion-attack/) известна тем, что она является первым вариантом программы-вымогателя, сочетающим шифрование файлов и кражу данных. Когда цели начали отказываться платить выкуп, Maze начал собирать конфиденциальные данные с компьютеров жертв, прежде чем зашифровать их. Если требования о выкупе не будут выполнены, эти данные будут обнародованы или проданы тому, кто предложит самую высокую цену. Возможность дорогостоящей утечки данных использовалась в качестве дополнительного стимула для оплаты.

Группа, стоящая за вымогательством Maze, официально прекратила свою деятельность. Однако это не означает, что угроза программ-вымогателей уменьшилась. Некоторые филиалы Maze перешли на использование программы-вымогателя Egregor, и считается, что варианты Egregor, Maze и Sekhmet имеют общий источник.

Группа REvil (также известная как Sodinokibi) – это еще один вариант программы-вымогателя, предназначенный для крупных организаций.

REvil – одно из самых известных семейств программ-вымогателей в сети. За последние несколько лет Ryuk соревновался за звание самого дорогого варианта программы-вымогателя. Известно, что REvil потребовал выкуп в размере 800 000 долларов. Со временем эта программа эволюционировала, используя технику двойного вымогательства (кражу данных у предприятий и одновременно шифрование файлов). Это означает, что в дополнение к требованию выкупа за расшифровку данных злоумышленники могут угрожать разглашением украденных данных, если не будет произведен повторный платеж.

LockBit – это вредоносная программа для шифрования данных, действующая с сентября 2019 года, и недавняя программа-вымогатель как услуга (RaaS). [5]Эта программа-вымогатель была разработана для быстрого шифрования больших организаций, чтобы предотвратить ее быстрое обнаружение устройствами безопасности и командами ИТ / SOC.

Lapsus $ – южноамериканская банда вымогателей, которая была связана с кибератаками. Кибер-банда известна вымогательством и угрозами разглашения конфиденциальной информации, если требования ее жертв не будут выполнены. Группа похвасталась взломом Nvidia, Samsung, Ubisoft и других известных фирм.

Чтобы добиться успеха, вымогателям необходимо получить доступ к целевой системе, зашифровать там файлы и потребовать выкуп у жертвы. Хотя детали реализации варьируются от одного варианта программы-вымогателя к другому, все они имеют одинаковые три основных этапа [6].

Первый этап: Инфекция и векторы распространения.

Программа-вымогатель, как и любое вредоносное ПО, может получить доступ к системам организации несколькими различными способами. [2] Однако операторы программ-вымогателей, как правило, предпочитают несколько конкретных переносчиков инфекции.

Одно из них – фишинговые электронные письма. Вредоносное электронное письмо может содержать ссылку на веб-сайт, на котором размещена вредоносная загрузка, или вложение, в которое встроена функция загрузки. Если получатель электронной почты попадается на фишинг, то программа-вымогатель загружается и запускается на его компьютере.

Другой популярный вирус-вымогатель использует такие сервисы, как протокол удаленного рабочего стола (RDP).С помощью RDP злоумышленник, который украл или угадал учетные данные для входа сотрудника, может использовать их для аутентификации и удаленного доступа к компьютеру в корпоративной сети. С помощью этого доступа злоумышленник может напрямую загрузить вредоносное ПО и запустить его на компьютере, находящемся под его контролем.

Другие могут попытаться напрямую заразить системы, например, как WannaCry использовал уязвимость EternalBlue. Большинство вариантов программ-вымогателей имеют несколько переносчиков инфекции.

Второй этап: Шифрование данных.

После того, как программа-вымогатель получила доступ к системе, она может начать шифровать свои файлы. Поскольку функциональность шифрования встроена в операционную систему, это просто включает в себя доступ к файлам, шифрование их с помощью ключа, контролируемого злоумышленником, и замену оригиналов зашифрованными версиями. Большинство вариантов программ-вымогателей проявляют осторожность при выборе файлов для шифрования, чтобы обеспечить стабильность системы. В некоторых вариантах также будут предприняты шаги по удалению резервных и теневых копий файлов, чтобы затруднить восстановление без ключа дешифрования.

Третий этап: Требование выкупа.

Как только шифрование файла завершено, программа-вымогатель готова предъявить требование о выкупе. Различные варианты программ-вымогателей реализуют это множеством способов, но нередко фон дисплея меняется на записку с требованием выкупа или текстовые файлы, размещенные в каждом зашифрованном каталоге, содержащем записку с требованием выкупа. Как правило, эти заметки требуют определенного количества криптовалюты в обмен на доступ к файлам жертвы. Если выкуп будет выплачен, оператор программы-вымогателя либо предоставит копию закрытого ключа, используемого для защиты симметричного ключа шифрования, либо копию самого симметричного ключа шифрования. Эта информация может быть введена в программу дешифрования (также предоставляемую киберпреступником), которая может использовать ее для обратного шифрования и восстановления доступа к файлам пользователя.

Хотя эти три основных этапа существуют во всех вариантах программ-вымогателей, разные программы-вымогатели могут включать разные реализации или дополнительные подпункты. [3] Например, такие варианты программ-вымогателей, как Maze, выполняют сканирование файлов, сведений реестра и кражу данных перед шифрованием данных, а программа-вымогатель WannaCry сканирует другие уязвимые устройства для заражения и шифрования.

Таким образом, сегодня информатизации риск заражения компьютерных систем является главной угрозой мировой инфраструктуры и систем управления. Киберпреступники все чаще наносят атаки, находят уязвимости в программном обеспечении и похищают персональные данные пользователей. Необходимо обезопасить себя специальными программами по защите устройств от киберузроз, что избежать колоссальные потери

Список литературы

1. Жуматий, В. П. Методика применения программного модуля для изучения принципов функционирования и способов нейтрализации вредоносных программ-вымогателей / В. П. Жуматий, М. И. Кулешов // Актуальные проблемы деятельности подразделений УИС : Сборник материалов Всероссийской научно-практической конференции. В 2-х частях, Воронеж, 23 мая 2019 года. Том Часть 1. – Воронеж: Издательско-полиграфический центр "Научная книга", 2019. – С. 139-143. – EDN XBZKHL.
2. Лизунов, О. А. Общие сведения о программах-вымогателях / О. А. Лизунов, О. Т. Сулейменов // Передовые технологии и материалы будущего : Сборник статей IV Международной научно-технической конференции. В 3-х томах, Минск, 09 декабря 2021 года. Том 2. – Минск: Белорусский государственный технологический университет, 2021. – С. 107-112. – EDN UCCCQS.
3. Митряев, И. С. Разграничение понятий информационной безопасности и кибербезопасности как элементов информационного пространства / И. С. Митряев, Н. Р. Калимуллин // Аграрное и земельное право. – 2021. – No 9(201). – С. 158-161. – DOI 10.47643/1815-1329\_2021\_9\_158.
4. Митряев, И. С. Тенденции применения кибератак программ-вымогателей / И. С. Митряев // Инновации. Наука. Образование. – 2021. – № 47. – С. 985-991. – EDN HBIIFJ.
5. Провоторский, А. О. Защита от программ-вымогателей / А. О. Провоторский, К. В. Шипеева // Электронный научный журнал. – 2017. – № 4-1(19). – С. 182-184. – EDN WEWTHA.
6. Что такое кибербезопасность? Различные типы кибербезопасности. Электронный ресурс]. Режим доступа: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/> (дата обращения: 05.07.2023).
7. Шутова, В. О. Киберугрозы: программы вымогатели, фишинг и способы защиты от их нападения / В. О. Шутова // Современные научные исследования и инновации. – 2022. – № 1(129). – EDN PMMNPG.

*Abstract: In the modern world, threats come from various sources, crime has reached the information level. Malefactors imperceptibly attack devices and steal personal data, information, other materials. This paper considers one of the types of cyber threats - ransomware. The main types of ransomware and features of their implementation are described.*

*Keywords: attack, cyberthreat, ransomware, cybercriminal, security, information.*