кристаллических образований, близких к призматическим. Размеры этих кристаллов колеблются в широких значениях размеров – от 0,1 до 3,5 по длине и 0,1–1,5 мкм по ширине. Присутствует также стекловидная фаза, образующая прослойки между кристаллическими образованиями, что позволяет заключить, что рост кристаллов происходил в структуре плиток из жидкой фазы, формирующейся при высокотемпературном обжиге. Формируются также кристаллы кварца, имеющие преимущественно изометричный габитус, с размером 0,2–1,4 мкм, которые формируют каркас структуры.

Поры преимущественно тупиковые, вытянутые, с пережимами и расширениями, нередко округлые или извилистые, неправильной остроугольной формы. Размеры пор составляют от 0,3 до 1,6 мкм.

Проведенные исследования позволяют заключить, что в многокомпонентном составе сырьевой смеси на основе местного полиминерального глинистого сырья и добавок возможно получение керамических плиток для внутренней облицовки стен, отвечающих требованиям нормативно-технической документации.

УДК 004.491

О.А. Лизунов, О.Т. Сулейменов
Институт информационных и вычислительных технологий Министерство образования и науки Республики Казахстан

ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММАХ-ВЫМОГАТЕЛЯХ

Аннотация. *В данной статье речь пойдет о программах-вымогателях, их классификации, целях применения, шифровальщике Babuk, а также о трех наиболее известных киберпреступных группировках, использующих шифровальщики.*

O.A. Lizunov, O.T. Suleimenov
Institute of Information and Computational Technologies of the Ministry of Education and Science of the Republic of Kazakhstan

GENERAL INFORMATION ABOUT RANSOMWARE

Abstract. *This article will focus on ransomware, their classification, purpose of use, Babuk ransomware, as well as the three most famous cybercriminal groups using ransomware.*

Введение

Повсеместная цифровизация и автоматизация различных сфер жизнедеятельности показали, что за предоставление всех благ и удобств, которые предоставляют нам информационные технологии, приходится платить большую цену из-за ущерба, наносимого киберпреступниками в результате проведения кибератак на бизнес-процессы, объекты критически важной инфраструктуры и т.д. Злоумышленников (хакеров), которые проводят подобные кибератаки называют «Black Hat» (черные шляпы).

Компания Fortinet представила отчет «2021 Global State of Ransomware Report», согласно которому среди существующих киберугроз наибольшие опасения вызывают программы-вымогатели.

Согласно исследованиям компании Avast, установлено, что число кибератак программ-вымогателей на пользователей за последние пять месяцев (июнь-октябрь) выросло на 33% по сравнению с первыми месяцами (январь-май) 2021 года.

В СМИ все чаще стала появляться информация о проведении различных кибератак с использованием шифровальщиков, большая часть которых приходится на инфраструктуру критически важных объектов. Все это связано с тем, что порог входа в киберпреступный бизнес находится на низком уровне, не требующем высокой квалификации от злоумышленников, так как программы-вымогатели стали доступны как **Ransomware-as-a-Service (**«Вымогательство как услуга»)**.**

В связи с этим, во всем мире возникла острая необходимость в обеспечении надлежащей защиты всей информационно-телекоммуникационной инфраструктуры, создании соответствующей нормативно-правовой базы, подготовке специалистов информационной безопасности и т.д.

Программы-вымогатели

Программа-вымогатель (ransomware) – тип вредоносного ПО, позволяющий блокировать доступ к компьютерной системе или предотвращать считывание записанных в ней данных (с помощью методов шифрования, блокировки доступа к системе), с целью получения выкупа от жертвы для восстановления исходного состояния системы.

Программы-вымогатели условно разделяют на две группы: блокировщики (локеры) и шифровальщики.

Блокировщик (локер) - программа, блокирующая или имитирующая блокировку ЭВМ (мобильного устройства).

Шифровальщик - программа, которая зашифровывает данные на диске ЭВМ.

По данным отчета бесплатной службы VirusTotal, выпущенным в октябре 2021 года, установлено, что почти 95% обнаруженных программ-вымогателей являются исполняемыми файлами (EXE), разработанными под ОС Windows и только 2% вредоносных программ разработаны под ОС Android. Общая диаграмма реализаций шифровальщиков представлена на рис. -1.

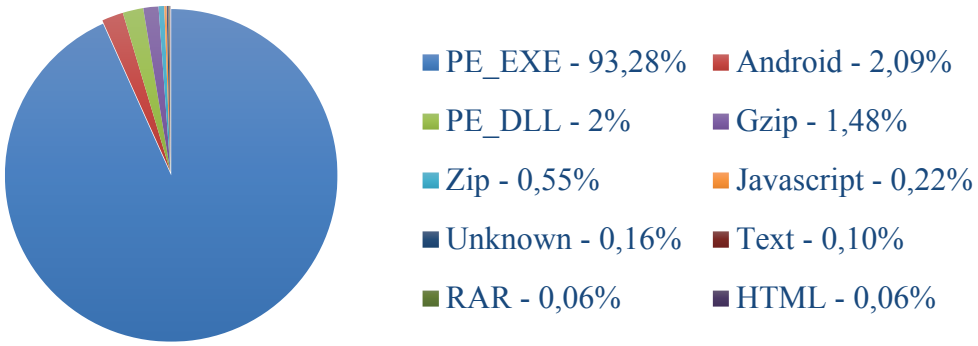

Рис. 1 – Процентное соотношение реализаций шифровальщиков

Экспертами VirusTotal был проведен анализ большого количества образцов программ-вымогателей, в результате которого вредоносные файлы были разделены на семейства, количество которых составило около 130, из которых было выделено 10 самых активных семейств, которые представлены на рис. 2.

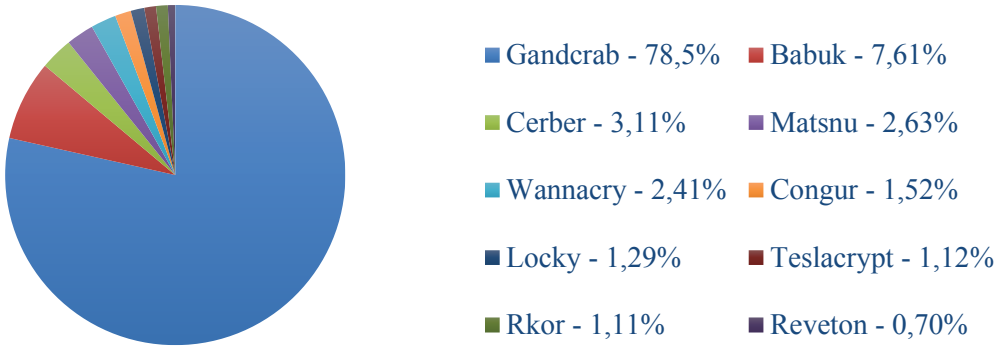

Рис. 2 - 10 самых активных программ-вымогателей

Хотелось бы отметить, что шифровальщики своими действиями затрагивают сразу три фундаментальных свойства информационной безопасности – конфиденциальность, целостность, доступность.

Основными целями при проведении кибератак с использованием шифровальщиков являются:

1. Нанесение ущерба государственным интересам.
2. Похищение конфиденциальной информации.

3. Блокировка доступа авторизованных пользователей к данным с целью получения денежного вознаграждения.

Шифровальшик «Babuk»

В сентябре т.г. на одном хакерском форуме был выложен исходный код шифровальщика под названием «Babuk». Для специалистов по информационной безопасности это оказалось большим подарком, так как полученные исходники и ключи позволили сэкономит время на изучение принципов работы вредоносной программы, используемых алгоритмов шифрования и быстро создать декрипторы.

С помощью шифровальщика «Babuk» киберпреступники активно атаковали организации по всему миру, требуя за расшифрование файлов выкуп в размере 60-85 тыс. долларов США в биткойнах. В числе пострадавших от шифровальщика оказались: сеть магазинов мобильных устройств Phone House, один из ведущих американских производителей систем управления оружием PDI Group и полицейское управление Вашингтона.

После кибератаки на полицейское управление Вашингтона, разработчики шифровальщика заявили о прекращении своей деятельности.

12 октября т.г. одна из крупнейших в мире групп по анализу коммерческих угроз «Cisco Talos Intelligence Group» обнаружила вредоносную активность, предположительно видоизменного шифровальщика «Babuk», поражающего преимущественно пользователей в США, с меньшим количеством заражений в Великобритании, Германии, Украине, Финляндии, Бразилии, Гондурасе и Таиланде.

Примечание: *в конце октября т.г. чешская компания по разработке ПО для кибербезопасности «Avast» выпустила декриптор, с использованием утекшего исходного кода и ключей расшифрования, позволяющий бесплатно расшифровать файлы жертв, подвергнувшихся атаке шифровальщика «Babuk».*

Декриптор может быть использован для файлов с расширением: .babuk, .babyk, .doydo.

Используемые алгоритмы шифрования в «Babuk».

Для генерации ключа используется асимметричный алгоритм шифрования «Curve25519». От полученного ключа получается хеш-образ «SHA-512», который используется в качестве ключа для симметричного потокового шифра «HC-128».

Среда разработки и язык программирования:

MS Visual Studio, C++.

Киберпреступные группировки Evil Corp, REvil и DarkSide

Evil Corp также известная под названиями Indrik Spider и Dridex – киберпреступная группировка, которая по мнению Министерства финансов США считается крупнейшей хакерской группировкой в истории. Предположительно, образовалась в 2007 году.

Киберпреступники начинали свою деятельность с троянской программы и ботнета нового типа ZeuS. Затем, злоумышленники сосредоточились на распространении банковской троянской программы Dridex. По истечении определенного времени, киберпреступники перешли к распространению шифровальщиков, в том числе предположительно шифровальщика «Babuk».

В декабре 2019 г. казначейство США заявило, что за все время своей деятельности группировка Evil Corp нанесла гигантский ущерб банковской системе США в размере свыше 100 млн. долларов США.

Ransomware Evil (REvil), также известная как Sodinokibi — киберпреступная группировка, считающаяся одной из самых активных в мире, которая использовала и предоставляла услуги программ-вымогателей.

Руководство США оценило причиненный ущерб киберпреступной группировкой REvil, проводившей кибератаки на критическую инфраструктуру США и нанесших огромный урон стране, как угрозу национальной безопасности США.

В связи с этим, поимкой киберпреступников занимались не только ФБР и секретная служба США, но и военные аналитики киберкомандования Министерства обороны США.

Наиболее масштабная кибератака REvil была проведена в отношении бразильской мясоперерабатывающей компании JBS S.A.

DarkSide — киберпреступная группировка, разрабатывающая вредоносное ПО и работающая по модели «Вымогательство как услуга». Впервые была отмечена в августе 2020 года.

Наиболее масштабная кибератака DarkSide была проведена в отношении компании Colonial Pipeline.

По данным исследовательской компании Elliptic, в период с августа 2020 года по апрель 2021 года DarkSide получила выкуп от своих жертв в размере около 90 млн. долларов США в биткоинах.

Заключение

Таким образом, программы-вымогатели по праву можно назвать кибероружием 21 века. За последние годы от действий шифровальщиков государственному и частному сектору был нанесен огромный урон.

В связи с низким порогом входа в киберпреступную деятельность по распространению программ-вымогателей, предоставлением киберпреступниками «услуг по вымогательству», получением злоумышленниками большого дохода от распространения вредоносного ПО, появлению в открытом доступе исходного кода шифровальщика «Babuk» и переходом сотрудников компаний на удаленный формат работы свидетельствует о том, что угроза от программ-вымогателей для государственного и частного сектора в краткосрочной и среднесрочной перспективе сохранится.

Благодарность

Статья подготовлена в рамках проекта программно-целевого финансирования OR11465439 «Разработка и исследование алгоритмов хеширования произвольной длины для цифровых подписей и оценка их стойкости» Министерства образования и науки Республики Казахстан.

Список использованных источников

1. https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf
2. https://habr.com/ru/post/569304/
3. https://devsday.ru/blog/details/68055
4. https://www.cisa.gov/stopransomware/ransomware-guide
5. https://blog.talosintelligence.com/2021/11/babuk-exploits-exchange.html

УДК 58.02:502.316

А. А. Мастич, О.А. Липская
Гомельский Государственный политехнический колледж
Гомель, Республика Беларусь

ВЛИЯНИЕ АНТРОПОГЕННОГО ФАКТОРА НА ПРОИЗРОСТАНИЕ ЕЛИ КОЛЮЧЕЙ В УСЛОВИЯХ ГОРОДА ГОМЕЛЯ

Аннотация. *Работа посвящена выявлению и оценке влияния антропогенного фактора на ход роста ели колючей в условиях города Гомеля. Установлено, что в местах с наибольшей антропогенной нагрузкой наблюдается не только замедление роста и развития насаждения, но и ухудшение внешних признаков насаждения.*