Список використаної літератури:

1. Загальний регламент про захист даних (GDPR). [Електронний документ]. – URL: https://gdpr-text.com/ua/
2. Регламент європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних. [Електронний документ]. – URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

Ключові слова: персональні дані, GDPR, захист персональних даних в ЄС.
Ключевые слова: персональные данные, GDPR, защита персональных данных в ЕС.
Key words: personal data, GDPR, personal data protection in the EU.

ЧАНЫШЕВ РАШИД ИБРАГИМОВИЧ

Национальный университет «Одесская юридическая академия»,
доцент кафедры информационных технологий,
кандидат юридических наук, доцент

ВИРУСЫ-ШИФРОВАЛЬЩИКИ (RANSOMWARE), УГРОЗЫ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Примерно десять лет назад появилась новая разновидность вредоносных компьютерных программ – вирусы-шифровальщики («Ransomware»). Их возникновение стало возможным только после появления криптовалют, так как именно криптовалюты сделали безопасным механизм получения выкупа.

Вирусы-шифровальщики работают следующим образом: на управляющем атакой сервере C&C (Command and Control server) создается пара ключей ассиметричного шифрования. При этом публичный (открытый) ключ встраивается в тело вируса. После заражения вирусом очередного компьютера на управляющем сервере генерируется ключ для симметричного шифрования, с помощью которого происходит шифрование файлов на компьютере – жертве. Передача самого симметричного ключа осуществляется при помощи методов ассиметричного шифрования (например, RSA-256) – симметричный ключ зашифровывается на управляющем сервере с помощью приватного (закрытого) ключа, вирус на атакованном компьютере расшифровывает его с помощью встроенного в него публичного ключа, после чего происходит процесс шифрования.

После окончания шифрования вирус выводит на экран компьютера сообщение с требованием выкупа с оплатой при помощи одной из криптовалют, например биткойна. При этом обычно указывается срок, в течение которого должна быть произведена оплата («счетчик»).

Величина требуемого выкупа, с учетом текущего курса криптовалют, может колебаться в размере от $300 до $5 000 000.

В том случае, если злоумышленниками получен выкуп – вирус производит процедуру расшифровки файлов на зараженном компьютере. При этом нет никакой гарантии, что этот процесс расшифровки будет вообще произведен или завершится благополучно, так как вымогатели уже получили выкуп и у них нет причин для организации достаточно сложного и небезопасного процесса технической поддержки в тех случаях, когда с расшифровкой возникают проблемы.

Следует отметить, что сам принцип зашифровки файлов на зараженном компьютере при помощи вируса-шифровальщика появился достаточно давно, еще в конце 80-х годов 20 века. В 1994 году появление вируса-шифровальщика OneHalf привело к настоящей компьютерной эпидемии [1]. Однако в те времена подобные вирусы действовали «бескорыстно» и, по своей сути, являлись всего лишь злостным хулиганством.

В настоящее время ситуация изменилась, и вирусы-шифровальщики постепенно становятся угрозой номер один. Так, например, в начале 2021 года с помощью вируса-шифровальщик Cring была произведена атака на ряд европейских промышленных предприятий, что привело к временной остановке производственных процессов и причинило значительный финансовый ущерб [2]. В отличии от обычных компьютерных вирусов вирусы шифровальщики представляют из себя реальную угрозу для жизни и здоровья людей, так как атакам подвержены компьютеры медицинских учреждений, на которых храниться жизненно важная информация о диагнозах и методах лечения людей. Так, в 2020 году более 750 поставщиков медицинских услуг потеряли в результате атак шифровальщиков почти $4 000 000 000 [3].

Особенностью современных вирусов-шифровальщиков является их техническое совершенство, атакам не могут противостоять не только частные пользователи, но и подразделения предприятий, профессионально занимающиеся вопросами обеспечения компьютерной и информационной безопасности.

Долгое время для заражения компьютеров использовались достаточно простые методы фишинга, задачей которых было вынудить пользователя открыть вредоносное вложение или перейти на по ссылке на фишинговый сайт. К настоящему времени для внедрения вирусов-шифровальщиков стали использоваться встроенный в Windows протокол удаленного рабочего стола (RDP), доступ с использованием незакрытых уязвимостей через виртуальные частные сети (например, через Fortigate SSL VPN), с помощью распространения поддельных обновлений программного обеспечения и с использованием макровирусов в документах MS Office [4].

При этом процесс атаки и внедрения вируса осуществляется с помощью человека-оператора, задачей которого является получение доступа через зараженный компьютер ко всей локальной сети предприятия.

В случае успешно проведенной атаки оператор производит поиск резервных копий, в том числе расположенных не только на самом компьютере, но и на подключенных к сети предприятия сетевых хранилищах, в том числе и облачных.

В результате такой целенаправленной атаки вирусом-шифровальщиком будут зашифрованы не только файлы на самих компьютерах, но и все доступные через удаленный доступ резервные копии.

Переход к удаленной форме работы во время пандемии коронавируса привел к тому, что к локальным сетям предприятий был вынужденно предоставлен удаленный доступ с домашних компьютеров и смартфонов работников. Поскольку домашние компьютерные устройства защищены намного хуже, чем корпоративные (если вообще защищены), такая практика значительно облегчила доступ злоумышленникам к защищенным сетям предприятий. Для получения доступа достаточно узнать логин и пароль, используемый работником на своем личном устройстве. Тем самым проверенная годами система организации защитного периметра для внутренней сети предприятия фактически перестала работать [5].

Смартфоны подвержены угрозам не менее чем персональные компьютеры. Процесс блокировки смартфона часто не требует даже шифрования его содержимого. При этом большинство пользователей не только не использует антивирусные программы на своих смартфонах, но и просто не знает об их существовании. Угроза эта весьма существенная, так как к настоящему времени более 50 процентов используемых в бизнесе компьютерных устройств являются мобильными, причем подавляющее число из них являются частными, а не корпоративными устройствами, используемых на предприятиях по принципу BYOD (bring your own device – «принеси свое устройство»).

Сталкиваясь с описанными выше проблемами, предприятия, ставшие жертвами вирусов -шифровальщиков, все чаще идут на то, чтобы решить проблему путем выплаты требуемого злоумышленниками выкупа.

Объемы выплат уже достигли размеров, вызывающих беспокойство у государственных контролирующих органов. С их точки зрения, подобные выплаты являются де-факто спонсированием терроризма и организованной преступности.

Так, 1 октября 2020 года Департамент казначейства США (US Treasury Department) опубликовал инструкции, в которых указано, что предприятия, пострадавшие от действий вирусов-шифровальщиков и собирающиеся выплатить выкуп, обязаны предварительно связаться с Управлением по контролю за иностранными активами Казначейства (OFAC, Office of Foreign Assets Control) и получить разрешение на выплату выкупа.

В противном случае к предприятиям, выплатившим выкуп без уведомления и разрешения OFAC, будут применены санкции (проведение судебного расследования и выплата крупного штрафа) [6].

Как следствие, предприятия, пострадавшие от вымогателей, оказываются «меж двух огней».

Тем самым предприятия фактически подталкиваются к финансированию и заблаговременному проведению комплекса мер по организации противодействия данной угрозе.

Поскольку жертвами вирусов-шифровальщиков становятся не только крупные предприятия, имеющие подразделения, отвечающие за компьютерную безопасность, но и частные лица, вынужденные принимать подобные меры самостоятельно, можно дать ряд практических рекомендаций.

Например, следует пересмотреть методы к создания резервных копий, так как используемые в настоящее время можно считать устаревшими. Метод резервного копирования файлов в облачные хранилища больше не является надежным, так как особенностью этого метода является автоматическая синхронизация файлов в облаке с их копиями на локальном компьютере. В случае заражения компьютера вирусом-шифровальщиком зашифрованные им файлы будут автоматически синхронизированы с их копиями в облачном хранилище. Кроме того, вирусы-шифровальщики имеют возможность получения доступа по сети к таким распространённым устройствам как NAS (Network Attached Storage), используемых как частными лицами, так и предприятиями для оперативного создания и хранения резервных копий.

Следовательно, требуется организовать процесс создания и надежного хранения резервных копий, к которым в принципе нет доступа по сети, например, на жестких дисках, физически подключаемых к компьютеру только на время создания резервной копии. Конечно, такое решение является весьма трудозатратным и неудобным, но это единственный вариант защиты от современных вирусов-шифровальщиков.

Список использованной литературы:

1. Легенды вирусостроения: В тисках шифратора. [Электронный ресурс]. – URL: http://surl.li/syiv – Дата обращения: 28.04.2021 р.
2. Шифровальщики-вымогатели The Digest «Crypto-Ransomware». [Электронный ресурс]. – URL: http://surl.li/syje – Дата обращения: 28.04.2021 р.
3. Хакеры стали чаще атаковать больницы. [Электронный ресурс]. – URL: http://surl.li/syjg/ – Дата обращения: 01.05.2021 р.
4. Phoenix Cryptolocker Ransomware New ransomware observed in attack against a large organisation. [Electronic resource]. – URL: http://surl.li/syjj – Last access: 04.05.2021.
5. Концепция периметра безопасности устарела. Но как усложнить жизнь хакерам? [Электронный ресурс]. – URL: http://surl.li/syjm – Дата обращения: 04.05.2021 р.
6. US Treasury says some ransomware payments may need its express approval. [Electronic resource]. – URL: http://surl.li/syjq. – Last access: 04.05.2021.

Ключові слова: віруси-шифрувальники, ransomware, інформаційна безпека комп'ютерних систем, методи створення резервних копій.
Ключевые слова: вирусы-шифровальщики, ransomware, информационная безопасность компьютерных систем, методы создания резервных копий.
Key words: encipher viruses, ransomware, information security computer systems, backup creation methods.

ЛОБОДА ЮЛІЯ ГЕННАДІЇВНА

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат педагогічних наук, доцент

АКТИВІЗАЦІЯ ПІЗНАВАЛЬНОЇ ДІЯЛЬНОСТІ МАЙБУТНІХ ФАХІВЦІВ ПРИ СТВОРЕННІ КОМП'ЮТЕРНИХ ПРОГРАМ

Особливість методики викладання, застосованої під час реалізації умови актуалізація самостійності майбутніх фахівців до створення сучасних комп'ютерних програм, полягає в тому, що студенти вже знайомі з мовами об'єктно-орієнтованого програмування або з будь-якою іншою мовою програмування і мають певний досвід створювати комп'ютерні програми.

Останнім часом зросла популярність комп'ютерних застосувань для ухвалення рішень, створених на базі браузерів. Крім того, вони зручні для створення проектів, що дозволяють підключатися до локальної мережі через з'єднання з Інтернет, і призначені для працівників, що перебувають вдома або в дорозі. Основне завдання розробника полягає в демонстрації користувачеві застосування простого та зрозумілого способу здобуття даних, що цікавлять його. Феноменальне зростання Інтернет і швидкий розвиток корпоративних мереж призвели до того, що створені комп'ютерні програми, легко та просто перекладають «на рейки» Інтернет вже наявні бази даних [1].

Вибір мови програмування залежить багатьох факторів і є сучасною технологією з можливостями: розробки власних графічних призначень для користувача інтерфейсів і створення мультимедійних застосувань; створення додатків, пов'язаних з обміном даними в Інтернет або локальній мережі; у роботі з базами даних і створенні працездатного інтерфейсу для різних локальних баз даних і баз даних клієнт/сервер; створення промислового інтерфейсу, реалізованого в системі Windows; для інформаційних службовців або системних адміністраторів, яким необхідно прийняти кваліфіковане рішення щодо того, який виробник інтерфейсу Windows буде вибраний їх організацією як стандарт.

Під час роботи над проектом створення комп'ютерних програм майбутній фахівець опановує два види інформації: