Шифроващи вредителски програми

д-р инж. Веселин Бончев

Национална лаборатория по компютърна вирусология

Българска Академия на Науките

1. Увод

В началото на месец юни, 2016 г., програмата “Новините” на българския телевизионен канал бТВ излъчи кратко предаване за т.нар. “нов български криптовирус”. Бяха казани редица неща, които са технически неправилни. Доколкото журналистите не са специалисти по киберсигурност изобщо и по вредителски софтуер в частност, това е простимо, особено като се има в предвид, че повечето от тези неправилни разбирания са сравнително широко разпространени. Но това ни подсети за необходимостта да бъде написана общообразователна статия, която да спомогне за изясняването на понятията в тази област.

2. Какво е “рансомуер”?

2.1. Етимология на понятието

Преди всичко, понятието “криптовирус” е технически неправилно. Въпреки, че повечето хора са свикнали да поставят знак за равенство между понятията “компютърен вирус” и “вредителска програма”, това е дълбоко неправилно. Както е дефинирал още “бащата” на компютърните вируси, д-р Фред Коен, компютърният вирус е саморазмножаваща се програма. (Всъщност, дефиницията дадена от д-р Коен е математическа и включва понятия като “множества”, “крайни автомати”, “машини на Тюринг”, “квантори за общност” и други подобни, но нека да не се задълбаваме толкова надълбоко.) Тоест, ако една програма се саморазмножава, то тя е компютърен вирус, дори и да не прави нищо друго. И обратното – ако една програма не се саморазмножава, то тя не е вирус, независимо колко други вредителски действия извършва. Програмите, за които ставаше дума в предаването, опредено са вредителски, тъй като те шифроват файловете на потребителя без неговото разрешение. Обаче почти нито една от тях не се саморазмножава – т.е., не е вирус.

Същевременно, напоследък у нас в средствата за масова информация започна често да се употребява думата “криптиране”, както и нейните производни. Тази дума е ненужен американизъм. По-правилно е да се използва думата “шифроване”, която е производна на много по-отдавна утвърдената в българския език дума “шифър”. (Въпреки че, строго погледнато, и тази дума е чуждица – тя произлиза от арабската дума “ал-сифр”, което означава “нула”. Думата “цифра” има същия произход.) Освен това, “крипто-” каквото и да е означава, че нещото е шифровано – докато тук става дума за програми, които сами по себе си не са шифровани, а шифроват файловете на потребителя.

Правилният български термин за подобен род вредителски програми е “шифроващи вредителски програми”. За съжаление, този термин, макар и технически правилен, е твърде дълъг и тромав за употреба. Да настояваме за употребата му е все едно да настояваме за употребата на (технически правилния и български термин) “сектор за начално зареждане” вместо безсмисления американизъм “бут сектор”, който се използва от почти всички компютърни специалисти. Така че, очевидно ще сме принудени да се примирим с употребата на чуждица – но поне нека да използваме такава, която е технически правилна. Както вече беше обяснено по-горе, програмите, които в средствата за масова информация се наричат “криптовируси”, всъщност не са нито “криптирани”, нито са компютърни вируси.

Как се наричат тези програми в други езици? Повечето термини, свързани с компютрите, идват от английски. И този случай не прави изключение. На английски този род програми се наричат “ransomware”, което е комбинация от думите “ransom” (откуп) и “software” (програмна система). На практика, този термин е възприет и от почти всички други езици. Забележително изключение са французите, които и без това имат навика да измислят собствени думи за всичко, включително и за компютърните термини. На френски този род програми се наричат “rançongiciel”, което е комбинация от думите “rançon” (откуп) и “logiciel” (програма). За съжаление, авторът на тази статия се провали в усилията си да измисли хубав български термин за този род програми по подобие на французите, така че ще се наложи да се примирим с американизма и да използваме “рансомуер”. Макар и не-български, този термин поне е технически правилен (за разлика от термина “криптовирус”), пък и думата “софтуер” (вместо българското, но много по-тромаво “програмно осигуряване”) вече доста отдавна се е утвърдила в нашия език.

2.2. Дефиниция

След като се разбрахме за това, какво понятие ще използваме, не е зле и да обясним ясно и разбрано, какво точно обозначаваме с него. Накратко, така се наричат *вредителските програми, които шифроват информацията на потребителя без негово разрешение и авторите на които искат изплащането на определена парична сума (откуп) за разшифроването ѝ*.

2.3. Малко история

Вероятно първият документиран случай на рансомуер е т.нар. “AIDS Information Trojan”, изолиран през 1989 г. Той се е намирал на дискета, разпространена от антрополога д-р Джоузеф Поп, която твърдяла, че съдържала информация, позволяваща на потребителя оцени риска да се зарази от СПИН. При изпълнението на програмата, намираща се на тази дискета, тя кодирала имената на файловете (но не и съдържанието им), намиращи се на дисковете на потребителя и извеждала съобщение, което настоявало потребителят да преведе определена сума пари на фирмата PC Cyborg Corporation, регистрирана в Панама, за да бъдат файловете му разшифровани.

Д-р Поп е бил идентифициран като автор на операцията от Скотланд Ярд, арестуван в Холандия на летище Шипол, и задържан в затвора Брисктън, Англия. Били са му предявени 11 обвинения в шантаж. Неговата защита била, че не изнудвал пари за собствено облагодетелстване, тъй като постъпващите суми били превеждани в полза на изследователска дейност за борба със СПИН. Съмнително е, дали тази защита би била успешна, но д-р Поп постепенно започнал да се държи все по-странно и накрая бил признат за психично негоден да бъде изправен пред съда и бил върнат обратно в Съединените Щати.

Междувременно английският компютърен вирусолог Джим Бейтс разработил програма, която разкодирвала кодираните имена на файлове и която позволявала на потребителя да възстанови дисковете си без да е необходимо да плаща никакъв откуп.

През 1996 г. американските криптолози Адам Юнг и Моти Юнг посочват в една своя статия, че подобен род атаки биха били много по-успешни при използването на т.нар. асиметрична шифровка (малко повече за това – след малко). През 2005-2006 г. се появяват редица други програми, шифроващи определени файлове на потребителя и настояващи за някакъв вид заплащане, за да бъдат те разшифровани – като троянските коне Gpcode, Archiveus, Krotten, Cryzip, Ransom, MayArchive и др. Например, различните варианти на Gpcode изискват изплащането на суми от порядъка на 100-200 щатски долара чрез вече несъществуващата електронна валута e-gold. (Друга особеност на повечето варианти от това семейство е, че функциите им за шифровка са реализирани доста любителски и лесно могат да бъдат разбити без да е необходимо да се заплаща откупът.) Други такива програми изпол-

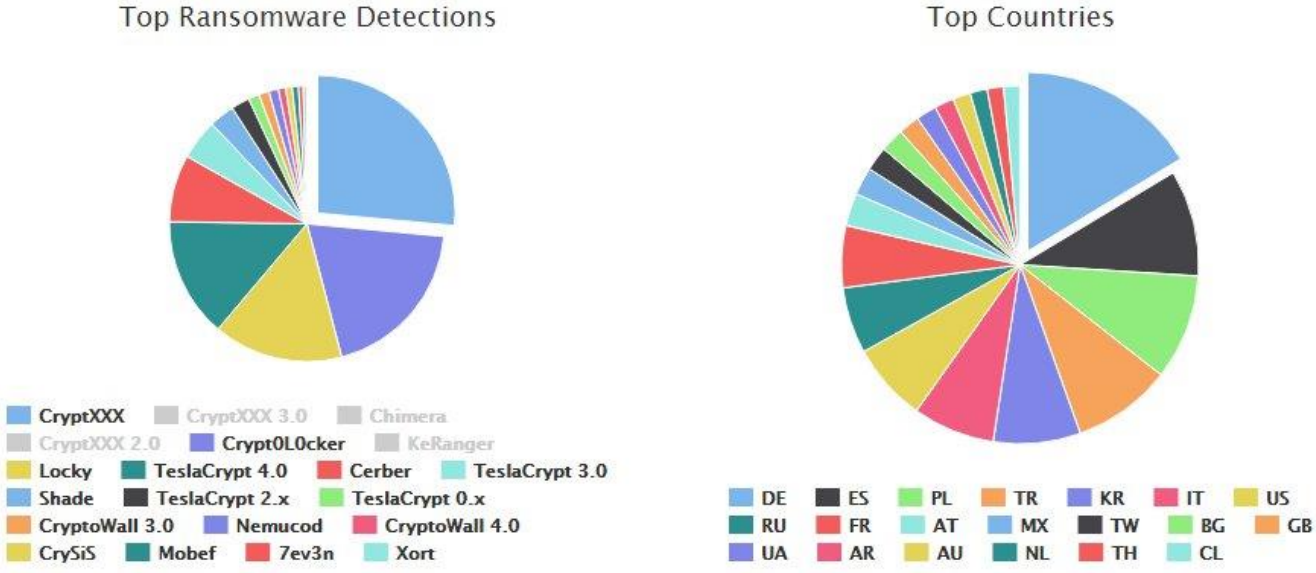
зват други методи за получаване на откупа – превод на пари чрез службата Western Union (които могат да бъдат получени сравнително анонимно), изпращане на SMS до специален високоплатен номер, закупуване на продукт от определен сайт и т.н.

Но истинският разцвет на рансомуера става възможен едва след 2009 г., когато е създадена и популяризирана т.нар. криптовалута биткойн. Описанието на основните принципи, стоящи зад криптовалутите е доста сложно и излиза извън рамките на тази статия. Достатъчно е да се спомене само, че тя реализира протокол за предаване на стойност между две лица, който не зависи от доверие в трета страна (например, банка или служба за превод на пари). Освен това, предаването е сравнително анонимно и участващите страни (както изпращащата, така и приемащата; последното е от особено значение за шантажиста) е изключително трудно да бъдат идентифицирани. Докато самата транзакция (преводът на стойност) е обществено достояние, видимо е само че определена стойност се прехвърля между два (или повече) адреса, а не кои именно лица стоят зад тези адреси. Това свойство правят криптовалутите (от които биткойн е най-разпространената) изключително подходящи за излизащи извън рамките на закона сделки, извършвани анонимно по Интернет. (Разбира се, криптовалутите могат да се използват – и в повечето случаи се използват – за напълно законни цели.)

Съвременната експлозия на рансомуер може да се датира като започнала на 5-ти септември, 2013 г., когато се появява и получава широко разпространение троянският кон CryptoLocker, който обединява основните черти на съвременния успешен рансомуер: разпространение чрез спам по електронната поща, шифроване на потребителските файлове, използване на асиметрична система за шифровка, и изискване заплащането на откупа да бъде направено във вид на биткойн.

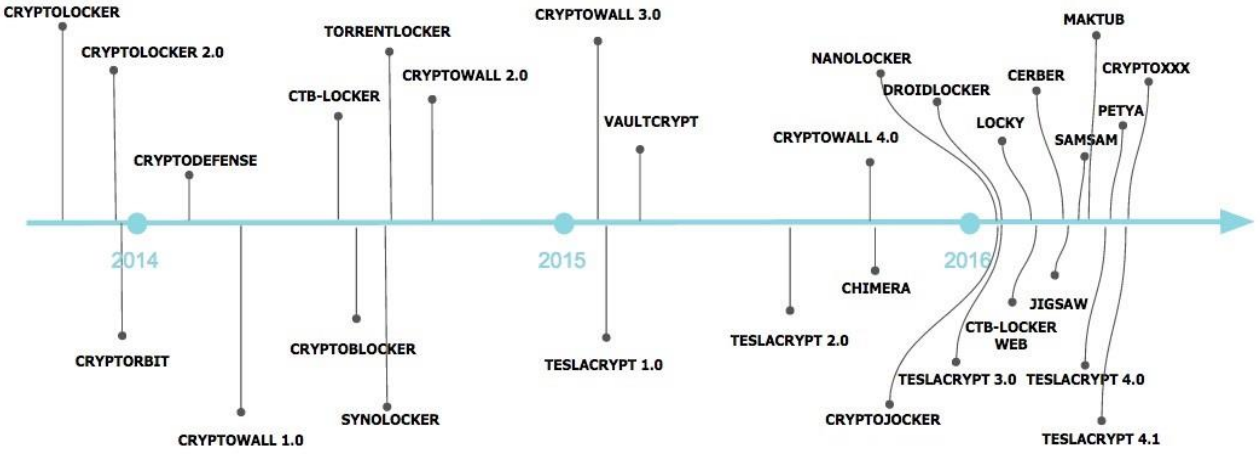
В наши дни има хиляди различни варианти на рансомуер с различна степен на разпространение и зловредност. Непрекъснато се създават и нови варианти. Огромен е и броят на жертвите – индивидуални потребители, учебни заведения, цели компании... Има и куриозни случаи, като например един полицейски участък в Лос Анджелис (който трябвало да плати откупа, защото всичките му бази данни се оказали шифровани), редица болници (които се наложило да спрат приемането на пациенти защото базите им данни станали неизползваеми) и т.н. Съгласно информацията на ФБР, само за първото тримесечие на 2016 г., жертвите на различни видове рансомуер са платили сумарно над 209 милиона долара. За сравнение, тази сума е “само” около 24 милиона долара за цялата 2015 г.

Повечето от съществуващия рансомуер е за операционната система Windows, но има отделни варианти и за операционните системи Linux и OSX. Има и варианти за мобилни те-



лефони (предимно такива, работещи с операционната система Android), та дори и за интели-

гентни термостати. Повечето от тях не шифроват информацията на потребителя, тъй като това е технически трудно (едно приложение за Android нормално няма достъп до файловете, създадени на устройството от други приложения), а само "заключват" телефона, правейки го неизползваем до заплащането на откупа. В редките изключения, когато се използва шифровка, тя се прилага само към файловете, намиращи се на сменяемата карта с памет, тъй като информацията, намираща се на нея е свободно достъпна за всички приложения.



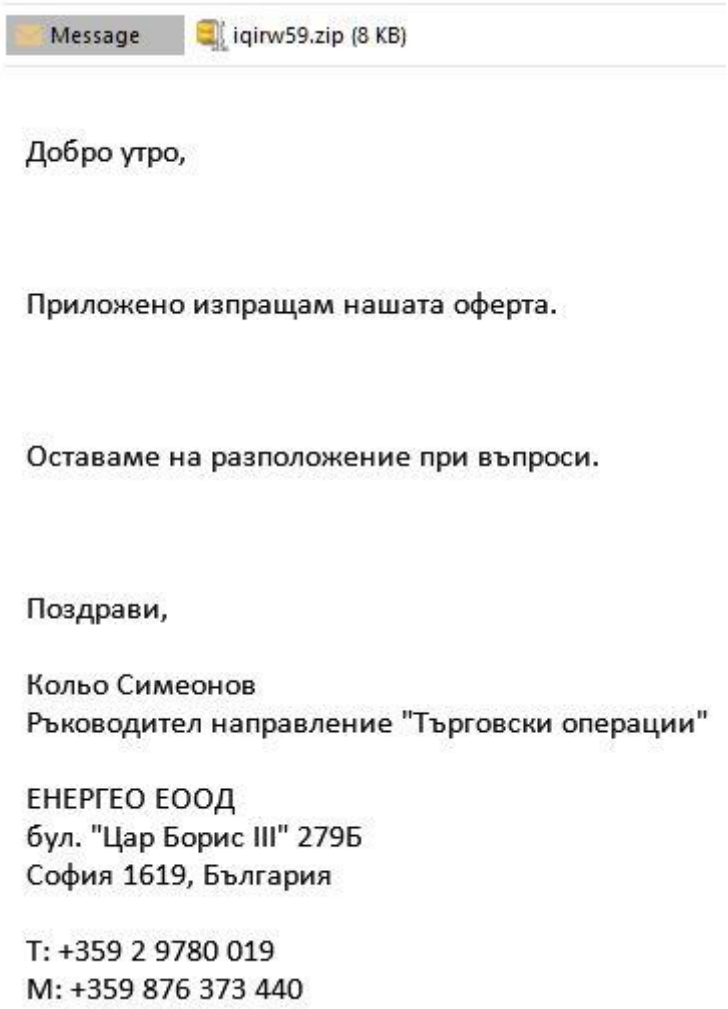
Напоследък започна да се наблюдава и създаването на рансомуер за така наречената "Интернет от предмети" ("Internet of Things") – т.е., интелигентни устройства, съдържащи специализирани компютри, които са свързани към Интернет. Има регистрирани случаи, когато рансомуер е заразил телевизор, работещ под управлението на операционната система Android и друг, който е заразил интелигентен ръчен часовник.

2.4. Откъде идва рансомуерът?

Както и при повечето други видове кибер атаки, определянето на националността и географското местоположение на нападателите, разработващи и изпращащи рансомуер е изключително трудно. В много случаи зад рансомуера стоят не отделни лица а цели престъпни организации, често пъти с международно участие. Причината е, че от подобен вид операции се печелят огромни суми пари. Повечето хора биха се съгласили да платят една сравнително скромна сума (100-200 долара) за да си върнат ценни файлове от които нямат резервни копия. Когато пострадалите са милиони (а именно за такива цифри най-често става дума), дори и малък процент от тях да се поддадат на шантажа, печалбата за шантажистите пак е от порядъка на милиони долари. Тъй като всички транзакции във вид на биткойн са обществено достъпни, ако се знае адресът на получателя (той се показва на потребителя след шифроването на файловете), всеки би могъл да определи какви суми са били преведени на този адрес (макар и не и от кого са преведени, както и кой именно е получателят). Дори още при първия широко разпространен успешен рансомуер, CryptoLocker, печалбата е била от порядъка на 27 милиона щатски долара!

Макар и в сравнително малък брой случаи, произходът на някои варианти рансомуер е бил установен. Според тези случаи, преобладаващият източник на рансомуер е Русия, въпреки че "добре представени" са и Съединените Щати, Латинска Америка, редица страни от Западна Европа, Китай и т.н.

В случая, който предизвика написването на тази статия, се твърди, че рансомуерът е български. Това, несъмнено, се основава на факта, че той бе разпратен по електронната поща във вид на оферта, написана на български език и преструваща се, че е изпратена от компанията ЕНЕРГЕО ЕООД:



Съобщението несъмнено е написано от човек, за когото българският е роден език. Разбира се, човек с добро образование по литературен български вероятно би могъл да се изрази и по-елегантно, но и така е очевидно, че текстът е писан от българин, а не, например, от чужденец с бегло познание на българския език или чрез използването на услуга за автоматичен превод като Google Translate. За съжаление, това само по себе си още не означава нищо. Напълно възможно е създателите на рансомуера просто да са платили на нищо неподозиращ българин да напише този текст. Или, още по-вероятно, текстът просто е откраднат от легитимно съобщение, изпратено от ЕНЕРГЕО. Телефонните номера са валидни, но не са на ЕНЕРГЕО.

Конкретните съобщения, които сме виждали, бяха изпратени от сървър, намиращ се в Италия. За съжаление, това е сървър за уебмейл, подобен на Yahoo! Mail или GMail, на който всеки би могъл да се регистрира и да изпраща съобщения, така че и това знание с нищо не спомага за определянето на националния произход на тази вредителска програма. Ако трябва да бъдем напълно коректни, единственото, което имаме право да твърдим е, че докато този рансомуер е бил насочен и към български потребители, ние не знаем къде именно е бил направен. Подобни съобщения, написани на съответния език, са били разпращани и до потребители и в други страни. Твърде е възможно истинският източник отново да е някоя престъпна банда в Русия или Украйна, но ние просто не разполагаме с необходимата информация, за да направим такова заключение. Твърдението, че произходът на програмата е български, е най-малкото прибързано, слабо обосновано и безотговорно.

3. Как работи рансомуерът?

В тази секция ще разгледаме основните принципи, на които се базират шифроващите вредителски програми.

3.1. Вектори на разпространение

Рансомуерът прониква в компютъра на потребителите по три основни пътя: спам по електронната поща, използване на компрометирани уеб сайтове и вредителски реклами (malwertising).

3.1.1. Спам

Може би най-разпространеният метод, използван от разпространителите на рансомуер е спамът по електронната поща. Според някои данни, около 93% от спама по електронната поща е свързан, по един или друг начин, с рансомуера. Има специализирани пазари, където могат сравнително евтино да бъдат закупени милиони адреси на електронната поща, на които да се изпраща спам. Обикновено спамът съдържа някакво съобщение, което да накара потребителя да цъкне на прикачения към съобщението файл. Типичен пример за такова съобщение е показано на илюстрацията в секция 2.4. Тонът на съобщението може да е изкушителен (“спечелили сте от лотарията”, “изгодни оферти”) или заплашителен (“акаунтът Ви ще бъде затворен”, “изтеглени са пари от сметката Ви”).

В някои случаи (при така наречените насочени атаки), спамът не е случайно разпратен, а е конструиран специално за атакуваната организация. Например, съобщението може да изглежда като изпратено от текущия директор на фирмата (с правилно име и адрес на електронната поща) до финансовия отдел и в него да се говори за някаква (въображаема) финансова неуредица, която спешно трябва да бъде изправена.

Прикаченият към спама файл може да има най-различни форми. В наши дни това почти никога не е директно изпълним (EXE) файл, защото модерните системи за електронна поща автоматично филтрират такива файлове (тъй като практически не съществува легитимна причина за изпращането им по електронна поща). Обикновено това е документ за Microsoft Word или Excel, PDF файл, JavaScript файл и т.н. Ако е документ на Word или Excel, в него обикновено има макроси. Модерните версии на тези програми по подразбиране блокират макросите в документите. Затова, документът е така конструиран, че да убеди потребителя да позволи изпълнението на макроси – например, твърди се, че е създаден с “по-нова версия на Word”, или пък е “защитен” и е необходимо макросите да могат да се изпълняват, за да се види съдържанието му.

В по-редки случаи документът експлоатира някаква уязвимост в приложението, което го отваря (Word, Excel, Adobe Acrobat и т.н.). В други случаи файлът е “изпълним”, защото представлява програма, написана на някакъв скриптиращ език (JavaScript, VBScript, Batch, PowerShell и др.). Понякога даже файлът се намира в архив (ZIP или RAR), който е шифрован с парола, като паролата е спомената в съобщението. Целта на този трик е да не се позволи на антивирусните програми, сканиращи електронната поща, да видят истинското съдържание на прикачения файл.

Този файл обикновено е само първият етап на инсталирането на рансомуера на машината, а не самият рансомуер. Файлът обикновено е малък и действието му – сравнително просто. Когато бъде изпълнен, той сваля от някакъв отдалечен сайт, който е под контрола на създателя на рансомуера, самия рансомуер и го стартира на заразената машина. Понякога този процес може да се състои и от повече от два етапа. Разбира се, има и изключения – например руският рансомуер RAA е написан изцяло на скриптиращия език JavaScript и присъства изцяло в разпращания по електронната поща спам.

3.1.2. Компрометирани сайтове

В по-редки случаи рансомуерът се разпространява от сайтове, които са били компрометирани (хакнати). Съдържанието на уеб страниците им е променено така, че автоматично да изпълнява някаква програма на машината, чийто уеб браузър разглежда страниците на компрометирания сайт. Обикновено това се постига с помощта на някакъв т.нар. exploit – експлоатирана уязвимост в браузъра. Има цели комплекти, които опитват голямо множество известни уязвимости в старите версии на различните браузъри и които комплекти се продават на черните пазари за вредителски програми. Един от най-разпространените и най-мощни такива комплекти е т.нар. Angler Exploit Kit.

Особено "опасни" са сайтовете, свързани със съмнителна или направо незаконна дейност (за сваляне на изпиратстван софтуер, за торенти, за разпространение на програми, генериращи регистрационни ключове за популярен софтуер и т.н. – идеята тук е, че тези, които и без това се занимават с незаконна дейност, е по-малко вероятно да се оплачат, ако сами станат жертва на такава дейност), както и "изоставени" сайтове, които отдавна не се поддържат от създателите им.

Понякога хакери разбиват защитата на напълно легитимен сайт (най-често чрез експлоатиране на уязвимости в използвания от сайта софтуер; WordPress е атакуван особено често) и променят съдържанието му така, че да инсталира рансомуер на компютрите на посетителите.

3.1.3. Вредителски реклами

Третият метод за разпространение на рансомуер, който все по-често се използва напоследък, е чрез така наречените "вредителски реклами" (malvertising). Идеята тук е следната.

Много сайтове предоставят безплатно съдържание, което потребителите намират за полезно. За да не искат заплащане от страна на потребителите, като в същото време да са в състояние да покриват разходите си, собствениците на такива сайтове показват реклами на страниците на сайтовете си. При това, те не показват конкретни реклами, намиращи се на компютрите им. Вместо това, те контрактуват показването на реклами с други фирми, които са се специализирали в този род дейност. Като резултат, собственикът на сайта изобщо няма представа какви реклами се показват на потребителите. Нещо повече, на различните потребители често пъти се показват различни реклами, в зависимост от това, към какво са проявили интерес в миналото. Фирмите, показващи реклами, заплащат на собственика на сайта за "рекламното пространство". Самите те получават парите си от фирмите, които предлагат рекламираните продукти.

Като резултат от тази многоетапна договореност, отговорността сякаш изчезва. Собственикът на сайта не знае, какви реклами се показват на посетителите на сайта – той просто си получава парите от фирмата, доставяща рекламите. От своя страна, фирмата, специализирала в доставка на реклами, не се интересува какво точно рекламират тези реклами – стига да ѝ бъде платено за тях от фирмата, която иска да рекламира продукта си.

На всичкото отгоре, за да се повиши вероятността рекламираният продукт да се продаде, тези фирми имат интерес да го рекламират именно на хора, които по принцип изглежда да се интересуват от такъв вид продукти. Затова често пъти рекламите съдържат активен код (JavaScript, Flash и др.), чиято цел е да "следи" потребителите и навиците им при посещение на сайтове, надявайки се да разбере от какво именно тези потребители се интересуват, та да им се показват реклами именно за такива неща.

Проблемът в цялата тази идея е, че "активен код" означава "код, който се изпълнява от браузъра. на потребителя, разглеждащ страницата с рекламата". Наистина, съвременните браузъри полагат огромни усилия, за да не позволят на този код да направи нещо вредно

(например, да свали и изпълни произволна програма на машината, на която работи браузърът). За съжаление, един браузър представлява един огромен и сложен софтуерен проект, а във всички такива проекти непрекъснато биват намирани програмни грешки – така наречените "бъгове". Някои от тези бъгове позволяват да се извършват неща, които по идея браузърът не бива да позволява да бъдат извършвани – като изпълнението на програми на машината, на която работи браузърът, както беше споменато по-горе.

Затова напоследък авторите на рансомуер все по-често конструират специални "реклами", които използват такива уязвимости в браузърите (или в добавъчния към тях софтуер, като например Flash, Sliverlight и др.) за да инсталират рансомуера на уязвимите компютри. Коварното тук е, че поради многоетапния процес на показване на реклами, който беше обяснен по-горе, потребителят може да бъде заразен при посещението на напълно легитимен сайт, за което собственикът на сайта си няма никаква представа и дори не е директно отговорен. Процесът дори не е лесно да се възпроизведе, защото различните посетители, като правило, виждат различни реклами. Ако някой от тях разбере, че е бил заразен от вредителска реклама и се оплаче, не е лесно това оплакване да се провери чрез просто посещение на въпросния сайт.

Строго погледнато, отговорността за такива случаи е на фирмата, доставяща реклами. Тя би трябвало да има по-строги критерии и да не се съгласява да доставя реклами, които съдържат вредителски програми. Но най-често тези фирми нямат необходимата техническа компетентност за да разпознаят една реклама като вредителска, пък и повечето от тях се интересуват единствено от това, да им бъде платено от фирмата, която рекламира "продукта" си. Същевременно, собственикът на сайта би трябвало да има възможността да избира коя именно фирма да му доставя рекламите и да избягва тези, с лоша репутация – но дори и това не винаги е възможно.

Коварното на този вид атака е, че от гледна точка на потребителя, машината му бива заразена без той да прави нищо достойно за критикуване – просто посещава легитимни и добре известни сайтове. Не сваля пиратски програми или филми и не цъка по прикачени файлове получени по електронната поща.

Някои известни и широко-популярни сайтове, които бяха засегнати от вредителски реклами през 2016 г. включват сайтовете на New York Times, BBC и др.

3.1.4. Други вектори на разпространение

Изброените дотук вектори на разпространение са най-често използваните. Освен тях, в по-редки случаи се използват и следните:

- *Комбинация от спам и компрометиран сайт*. В този случай рансомуерът не се съдържа директно в спама, получен по електронната поща. Вместо това, спамът съдържа линкове, които, ако бъдат цъкнати, отварят в браузъра сайт, който е компрометиран (или направо вредителски) и който инсталира рансомуера на компютъра на потребителя чрез експлоатирането на някаква уязвимост от комплект с такива уязвимости, намиращ се на сайта.
- *Разпространяване от други вредителски програми*. В някои случаи други вредителски програми, които сами по себе си не са рансомуер, се използват за да разпространяват и инсталират такъв на заразените от тях компютри. Например, мрежата от ботове Dridex, която се използва за незаконно завладяване и отдалечено управление на компютри, обикновено с цел последните да се използват за разпращане на спам или за кражба на финансова информация, в някои редки случаи е била използвана, за да бъде инсталиран рансомуер на заразените компютри.

- *Инсталиране след незаконно проникване в компютъра*. Например, престъпната банда, разпространяваща рансомуера Bucbi го инсталира, след успешно проникване в компютъра на жертвата чрез използване на уязвимости във вградената система на Windows за отдалечено управление на компютри, Remote Desktop.
- *Инсталиране след пробив в сървъра*. Рансомуерът SamSam бива инсталиран, след като нападателите успеят да пробият защитите на публично достъпния уеб сървър на фирмата (обикновено чрез използване на уязвимости в софтуера, работещ на този сървър) и оттам проникнат в компютрите, свързани към локалната мрежа на фирмата.
- *Саморазмножение*. Рансомуерът ZCryptor има способността да се саморазмножава като редица вируси, чрез копирането си върху свързаните към компютъра флашки и създаването на autorun.inf файл там, който да се изпълни автоматично, когато флашката бъде закачена на нов компютър, предизвикване заразяването на новия компютър от рансомуера.
- *Чрез линкове в SMS съобщения, сочещи към неофициални хранилища на мобилни програми.* По този начин, разбира се, се разпространява само рансомуерът за мобилни устройства.

3.2. Методи на шифровка

След като проникне в машината на жертвата, рансомуерът шифрова важната информация там. Обикновено това са файлове с данни (разпознавани по разширенията им) но понякога се шифроват цели части от диска, чието съдържание е необходимо за достъп до информацията на него.

В криптографията съществуват два основни вида шифровки – *симетрична* и *асиметрична*. Подробното им описание излиза извън рамките на тази статия; тук ще ги опишем само в най-общи черти.

При *симетричната* шифровка се използва един и същ ключ както за шифроване, така и за разшифроване. Основният проблем при нея е, че ключът трябва да бъде предаден на страната, която ще го използва за разшифроване, и то по защитен от подслушване канал – защото ако този ключ бъде прихванат от евентуалния противник, цялата шифрована комуникация може да бъде разчетена. Но защитени от подслушване канали често пъти не са на разположение, или пък имат много малка пропускателна способност – иначе съобщението би могло да се предаде по тях без каквато и да било шифровка. Типични примери за алгоритми за симетрична шифровка са DES, AES, RC4, Blowfish и др.

При *асиметричната* шифровка (наричана още шифровка с обществено достъпен ключ) се използва двойка ключове. Единият от тях става само за шифроване (и за проверка на цифрови подписи), а другият – само за разшифроване (и цифрово подписване). Двата ключа са свързани, но да се изведе ключът за разшифроване от ключа за шифроване е изключително трудно алгоритмически. Например, ако всеки атом във Вселената беше персонален компютър, би било необходимо цялото досегашно време на съществуване на Вселената за да могат тези компютри да изчислят ключа за разшифроване от ключа за шифроване.

Всяка от комуникиращите страни генерира двойка такива ключове. Ключовете за разшифроване всяка страна запазва в най-строга тайна, а ключовете за шифроване се разпращат по незащитен от подслушване канал. При комуникиране изпращащата страна шифрова съобщението с шифроващия ключ на приемащата страна (който е известен на всички, включително и на евентуалния подслушващ противник), а приемащата страна използва своя (таен) ключ за разшифроване, за да разшифрова това съобщение. Основният проблем при асиметричната криптография е достоверността на шифроващите ключове. Тоест, изпраща-

щата страна трябва да е сигурна, че използва за шифроване на съобщението именно шифроващия ключ на приемащата страна, а не ключ за шифроване на подслушващия противник. Типични примери за асиметрична шифровка са методите RSA, ECC, ElGamal и др.

Друг проблем на асиметричната криптография е, че тя е изключително бавна и изчислително трудоемка за работа с големи съобщения. Затова на практика почти винаги се използва комбиниран подход. Съобщението се шифрова със симетричен алгоритъм и случайно генериран ключ, след което само ключът (който е малък по размер) се шифрова с асиметричен алгоритъм и се изпраща заедно със самото шифровано съобщение.

Ранните варианти на рансомуер често използваха симетрични алгоритми за шифроване на файловете, като някои от тях (напр. TeslaCrypt) освен това допускаха глупостта да крият ключа на нападнатата машина – в конфигурационен файл или в регистъра. Разбира се, в този случай е сравнително тривиално този ключ да бъде извлечен и шифрованите файлове – разшифровани.

За съжаление, модерният рансомуер действа значително по-интелигентно и използва комбинирания метод, описан по-горе. Веднага щом като зарази дадена машина, той се свързва със сървър, който е под контрола на създателя му. Сървърът автоматично генерира двойка ключове за асиметрична шифровка. Ключът за разшифроване остава на сървъра. Ключът за шифроване се изпраща на заразената машина. След като го получи, вредителската програма на заразената машина генерира случаен ключ за симетрично шифроване (най-често за всеки отделен файл се използва различен такъв ключ), шифрова файла, шифрова ключа за симетрично шифроване с ключа за асиметрично шифроване, унищожава ключа за симетрично шифроване и записва шифрованото му копие в шифрования файл.

Допълнително, шифрованите файлове обикновено се преименуват (като или се променя само разширението им или цялото им име) и се унищожават системните области във файловата система, които биха могли да бъдат използвани за възстановяване на файловете (например, т.нар. “shadow copies”).

Ако този алгоритъм бъде реализиран успешно и компетентно (нещо, с което не всеки автор на рансомуер успява да се справи), разшифроването на шифрованите файлове е невъзможно без наличието на ключа за асиметрично разшифроване, който съществува само на сървъра., контролиран от автора на рансомуера, и който се изпраща на потребителя само след получаване на откупа.

Почти във всички случаи става дума за шифроване на отделни файлове (обикновено – файлове с данни с често използвани разширения: JPG, PNG, GIF, DOC, XLS, PDF, и т.н.), които се намират в личното дърво от папки на потребителя. Но има и изключения, например рансомуерът Petya шифрова главната таблица на файловете (master file table) на диска, което прави целия диск недостъпен. Някои видове рансомуер освен това “заключват” компютъра, т.е. правят невъзможно да се прави с него каквото и да е, освен да се посети сайта за плащане на откупа.

3.3. Изплащане на откупа

След като информацията бъде шифрована, рансомуерът уведомява потребителя за това и предявява исканията си за откуп. Обикновено това става чрез показването на текстов файл със съдържанието на исканията в Notepad, или чрез създаването на HTML файл и показването му в браузъра, като понякога се сменя и фоновото изображение на десктопа.

При изплащане на откупа (най-често във вид на биткойн, защото проследяването му до получателя е изключително трудно), жертвата на шантажа получава в някакъв вид средството, необходимо за разшифроване на шифрованите файлове. Строго погледнато, за това е необходим само ключът за асиметрично разшифроване, както беше обяснено в предишната секция. Обаче средният потребител едва ли би знаел какво да прави с него, поради което на

практика се изпраща цяла програма, която съдържа този ключ и която извършва разшифроването.

Почти винаги рансомуерът показва на потребителя подробни инструкции за това, как да се сдобие с биткойни (нещо, с което повечето потребители изобщо не са запознати). Има и изключително професионални случаи, когато авторите на рансомуера създават специални сайтове за подпомагане на потребителя, с възможност за изясняване на проблемите на живо в специален чат.

Не бива да забравяме, че разпространението на рансомуер с цел получаване на откуп е един вид бизнес, макар и незаконен бизнес. Тези, които се занимават с него са подчинени на всички закони на бизнеса – те се опитват да максимизират печалбата и да минимизират разходите. Самото програмиране на вредителската програма често пъти се договаря с професионални програмисти, сайтовете за поддръжка и "обслужване" на клиенти имат професионален дизайн, дори на потребителя се дават безплатни "мостри" от стоката – т.е., дава му се възможност да разшифрова безплатно един-два файла по избор, за да бъде убеден, че обслужването ще бъде качествено. Самото разпространение на рансомуер често пъти също не се извършва директно от престъпната групировка, стояща зад него, а се "договаря" (срещу заплащане) с други престъпни елементи, които са се специализирали в този род дейност.

4. Какво да се прави, при нападение от рансомуер?

Ако вече сте нападнати от рансомуер (т.е., на екрана вече е показано съобщението, изискващо откуп), общо взето играта е вече загубена и може да бъде направено твърде малко. Значително по-добре да избегнете заразата, за което ще бъдат представени редица съвети в следващата секция. Но ако белята вече се е случила, все пак могат да бъдат дадени някои полезни съвети.

4.1. Не плащайте откупа!

На пръв поглед, ако сумата искана от автора на вредителската програма е сравнително скромна, много хора биха се изкушили да я платят, за да си разшифроват файловете и да не се занимават повече с глупости. Дори шифровката да е калпава и да може да бъде разбита, дори жертвата да има резервни копия на шифрованите файлове, времето, необходимо за пълно възстановяване на системата може да бъде оценено по-високо от стойността на откупа, особено като се вземе в предвид, че фирмата няма да бъде работоспособна за това време и че хората, извършващи възстановяването на системата вероятно са високоплатени и си имат и друга работа, която няма да са в състояние да вършат през това време. Въпреки това, съветът ми е да не се поддавате на това изкушение. Помислете за следното:

1) Дори и да си платите откупа, може да не получите средство за разшифроване на шифрованите файлове. Наистина, престъпниците, които стоят зад тези атаки имат интерес да имат "добра репутация" за плащане на откупа – в противен случай, ако се разчуе, че не спазват своята част от "сделката", хората ще престанат да плащат и печалбите им ще спаднат. Но не забравяйте, че все пак имате работа с престъпници, на които не може да се има доверие. Случаи, когато плащането на откупа не е довело до резултати има известни, макар и не много. Понякога престъпната операция вече е разбита от органите на властта и просто няма кой да ви изпрати средството за разшифроване.

2) Може да ви бъдат поискани допълнителни суми. Поне в един известен случай, след като една болница в Съединените Щати платила откупа, престъпниците се усетили, че става дума за цел с висока стойност и поискали още пари за да доставят средството за разшифроване.

3) Средството за разшифроване може да не работи. Например, поради програмна грешка в рансомуера CryptXXX 3.0, шифрованите файлове са безвъзвратно повредени и разшифроващото средство просто не върши работа.

4) За "улеснение" на потребителя, средството за разшифроване често пъти не е ключ (т.е., текст), а програма, която съдържа ключа и извършва разшифроването. Програма, създадена от престъпници и на която не може да се има доверие. (Третият закон на компютърната сигурност гласи: "Ако изпълните програмата на нападателя на вашия компютър, това вече не е вашият компютър.") Дори и да разшифрова файловете ви (което не е гарантирано), тя може да нанесе други щети на машината ви – например, да отвори задна вратичка, през която нападателите отново да влязат, може да "открадне" (и изпрати на нападателите) ценни файлове с данни и др.

5) Ако платите откупа, вие на практика финансирате престъпната операция и помагате на престъпниците да продължават атаките си. Това определено не е етично (помислете си за бъдещите жертви), а в определени случаи може да е дори и незаконно.

6) Ако сте фирма, у нас няма законен начин да платите откупа. За всеки разход, извършван от фирмата, тя трябва да разполага с фактура, която да представи в случай на ревизия. Разбира се, престъпниците няма да ви издадат никаква фактура. Чувал съм за куриозни случаи, като фирми, които карали служителите си да изискват фактури когато купуват за себе си неща като миещи препарати, бутилирана вода и т.н., за да може с тези фактури да се отчетат направените за откупа разходи – но това, разбира се, е незаконно. Освен ако директорът на фирмата не е съгласен да плати откупа от личните си средства, няма официален и законен начин за заплащането му.

4.2. Ако се усетите навреме, изключете Интернет връзката.

Ако прочетете внимателно секция 3.2 за асиметричната шифровка, ще разберете, че рансомуерът, който я използва (а почти всички съвременни варианти на рансомуер го правят), трябва да се свърже със сървър, който е под контрола на автора му, за да получи ключа за шифроване. В някой случаи двойката ключове за асиметричната шифровка се генерира на заразената машина, а не на сървъра. Но дори и в този случай, ключът за разшифроване трябва да бъде изпратен на сървъра. (преди да бъде унищожен на заразената машина) – т.е., пак е необходима връзка по Интернет.

Ако навреме се усетите, че може да сте се заразили с рансомуер, опитайте се да изключите връзката си с Интернет, преди описаната по-горе комуникация да бъде осъществена. Дори файловете ви да бъдат шифровани, ако ключът за разшифроване още не е изпратен на сървъра., има шанс той да бъде прихванат от специалист, който има съответните познания.

4.3. Опитайте се да определите източника на заразата.

Ако рансомуерът е шифровал файловете по цялата ви локална мрежа, опитайте се да определите работната станция, от която е тръгнала заразата. Един трик, който често пъти дава резултат, е да погледнете файла с искането за откуп и по свойствата му да определите на кой потребител в мрежата той принадлежи. Именно на работната станция на този потребител се намира рансомуерът.

Защо това е от значение? Ако се обърнете към специалист, който да се опита да разбие шифровката, много е важно той да знае с кой именно рансомуер си има работа. Приблизителният вариант обикновено може да се определи по различни признаци, като съдържанието на бележката за откуп и/или как точно са преименувани шифрованите файлове. Но най-сигурно е да се анализира копие от самия рансомуер; тогава конкретният вариант може да

бъде идентифициран точно. Такава идентификация е важна, защото различните варианти, дори когато много си приличат помежду си, може да използват леко различаващи се методи на шифровка, а използването на погрешен метод за разшифроване понякога може да има фатални последици за съдържанието на шифрованите файлове.

Пак поради същата причина, въздръжте се от изкушението да пуснете антивирусна програма, която може да намира и премахва рансомуера – поне не го правете преди да сте запазили резервно копие от него, което да предоставите на специалистите.

4.4. Опитайте се да разбиете шифровката.

Да се реализира криптографски алгоритъм правилно и компетентно е доста трудно, поради което авторите на някои видове рансомуер са се провалили в това начинание и шифровката може да бъде разбита. В други случаи ключовете за разшифроване могат да бъдат получени по други начини. Ето само няколко примера:

- TeslaCrypt 1.0 твърди, че използва асиметрична шифровка. Истината, обаче, е че той използва симетрична шифровка и крие ключа в конфигурационен файл на нападнатия компютър. Извличането му оттам е сравнително елементарно.
- TeslaCrypt 2.0 прави същата боза, само че "крие" ключа в регистъра, вместо във файл. Извличането му оттам отново е тривиално.
- TeslaCrypt 3.0 наистина използва асиметрична шифровка – шифроване с елиптични криви. Обаче подбира кривите доста неудачно, поради което ключът може да бъде разбит. Операцията се свежда до разлагане на прости множители на едно 150-цифрово число. В зависимост от броя и размера на множителите, това е напълно по силите на съвременен персонален компютър в рамките на няколко минути до няколко часа.
- При TeslaCrypt 4.0 шифровката вече е реализирана "както трябва" и не може да бъде разбита. Обаче авторите му били обзети от угризения на съвестта (или може би от страх, че полицията е по петите им), отказали се от операцията си, публикували извинение, като и главния си ключ за разшифроване. Това позволило на антивирусната компания ESET да разработят програма, базирана на този ключ, която да разшифрова всеки файл, шифрован от този вариант.
- Престъпната група, стояща зад рансомуера CoinVault е била разбита от холандската полиция. На иззетите сървъри е била намерена базата данни от разшифроващи ключове. Антивирусната фирма Kaspersky Lab (която е помогнала за разбиването на групата) е получила достъп до ключовете и е направила безплатен инструмент за разшифроване на файловете, шифровани от този рансомуер.
- KeRanger използва системния часовник, за да инициализира генератора си на случайни числа, който се използва за генериране на ключове за симетрично шифроване на файловете. Въпреки че тези ключове се шифроват с асиметрична шифровка, след което оригиналите се унищожават, те могат лесно да бъдат отгатнати по времето на последна промяна на шифрованите файлове.
- Някои ранни версии на CryptoLocker не изтриват т.нар. shadow copies на файловете, поради което последните могат да бъдат възстановени.
- Ransom-All изобщо забравя да шифрова файловете, така че съобщението му, искащо заплащането на откуп, може просто да бъде игнорирано.

И така нататък, и така нататък. За съжаление, тези случаи са сравнително малко. Има десетки хиляди различни видове рансомуер, но шифровката само на стотици от тях може да

бъде разбита, така че не се надявайте много на успех. И непременно се обърнете към специалист, който ще може да идентифицира конкретния вариант и ще знае дали и как точно шифровката му може да бъде разбита.

4.5. Възстановете шифрованите файлове от резервни копия.

Това всъщност е най-сигурният и ефективен начин за премахване на вредите, нанесени от рансомуера. Вие редовно си правите резервни копия на важната информация, нали? Ако случайно отговорът ви на този въпрос е отрицателен (и особено ако сте отговорен за поддръжката на компютрите във фирма!) оставете всичко, с което се занимавате в момента и веднага направете такова копие! След което отделете известно време за да планирате ефикасна стратегия за редовно правене на такива копия. Малко повече ще отделим на този въпрос в следващата секция.

5. Как да се предпазим от рансомуер?

Предпазването винаги е за предпочитане пред лечението. В тази секция ще дадем някои съвети за това, какво да направим с цел намаляването на рисковете от рансомуер.

5.1. Редовно си обновявайте операционната система.

В големите софтуерни проекти като операционната система и различните идващи с нея приложения (браузъри, библиотеки и др.) непрекъснато биват откривани програмни грешки. Някои от тях са много сериозни и позволяват на злоумишленици да изпълняват от разстояние техен програмен код на вашия компютър, което може да доведе до заразяване с рансомуер (а и до редица други неприятности).

Всеки първи вторник на месеца Майкрософт разпространява “кръпки” за продуктите си (операционна система, браузър, Office и т.н.), които изправят грешките, открити в тях през последния месец. Задължително прилагайте тези кръпки при първа възможност. Понякога те затварят сериозни уязвимости в компютъра ви, която намалява опасността от зараза при работа в Интернет.

Разбира се, това се отнася не само за Майкрософт. Повечето производители на софтуер предлагат безплатно обновяване на продуктите си, когато в тях бъдат открити сериозни проблеми. Същата препоръка се отнася и за този случай – инсталирайте новите версии веднага щом е възможно. Конфигурирайте програмните продукти да се обновяват сами и автоматично, ако това е възможно. Особено важно е да се обновяват продуктите на Adobe (Flash, Adobe Reader), защото те са много широко използвани и в тях изключително често се откриват застрашаващи сигурността на компютъра грешки.

Същото се отнася и до антивирусната ви програма – проверете дали тя наистина работи (а не ѝ е изтекъл лиценза, например) и дали успешно и редовно се обновява.

5.2. Не цъкайте на прикачени файлове.

Това би трябвало да се разбира от само себе си, но изглежда, че много потребители все още не могат да се научат. Ако получите по електронната поща съобщение с прикачен към него файл, не отваряйте файла като цъкате по него, освен ако не сте 100% сигурни, че това е безопасно. (Например, ако очаквате да получите този файл, защото вече сте водили разговор по въпроса с кореспондента си.) По-конкретно:

- Не разчитайте, че само защото съобщението изглежда да е изпратено от ваш познат, то е безопасно – тази информация много лесно се фалшифицира.
- Не разчитайте, че файлът е безопасен само защото има безопасно видимо разширение (напр., “.TXT”). По подразбиране, Windows крие разширенията на

файловете, и файл, наречен например “ФАКТУРА.TXT.JS” ще бъде показан като “ФАКТУРА.TXT”.

- Не разчитайте, че файлът е безопасен, само защото има “безопасна” иконка (например, на Microsoft Word или Notepad). Ако файлът е изпълним, много е лесно да му се сложи произволна иконка.

Дори когато сте сигурни, че файлът е безопасен, не го отваряйте с цъкане в съобщението. Вместо това, запишете го на диска си, стартирайте приложението, което би трябвало да е предназначено да го отваря (например, Microsoft Word) и отворете файла от това приложение, вместо да цъкате директно самия файл.

5.3. Блокирайте прикачените файлове с опасни разширения.

Този съвет се отнася по-скоро за фирми, отколкото за индивидуални потребители. Конфигурирайте сървъра си за електронна поща така, че да филтрира съобщенията, съдържащи прикачени файлове с “опасни” (т.е., изпълними) разширения. Как именно да ги филтрирате зависи от конкретния сървър за електронна поща, който използвате – системният ви администратор би трябвало да е наясно какво и как да направи.

Файлове със следните разширения определено могат да съдържат изпълним код и няма разумна причина за изпращането им по електронна поща, така че съобщенията, които ги съдържат, непременно трябва да бъдат филтрирани:

.ADE, .ADP, .ANI, .APPLICATION, .BAS, .BAT, .BTM, .CHM, .CMD, .COM, .CPL, .CRT, .EXE, .GADGET, .HLP, .HT, .HTA, .INF, .INS, .ISP, .JAR, .JOB, .JS, .JSE, .LNK, .MSC, .MSH, .MSH1, .MSH1XML, .MSH2, .MSH2XML, .MSHXML, .MSI, .MSP, .MST, .OCX, .PCD, .PIF, .PS1, .PS1XML, .PS2, .PS2XML, .PSC1, .PSC2, .REG, .SCF, .SCR, .SCT, .SHS, .URL, .VB, .VBE, .VBS, .WS, .WSC, .WSF, .WSH

Същевременно, имайте в предвид, че редица файлове могат да бъдат “контейнери”, които макар и сами по себе си да не са опасни, могат да съдържат опасен код. Това са различните видове архиви:

.001, .7Z, .ACE, .ARJ, .BZ2, .BZIP2, .CAB, .CPIO, .DEB, .DMG, .FAT, .GZ, .GZIP, .HFS, .ISO, .LHA, .LXMA, .LZH, .NTFS, .RAR, .RPM, .SQUASHFS, .SWM, .TAR, .TAZ, .TBZ, .TBZ2, .TGZ, .TPZ, .TXZ, .VHD, .WIM, .XAR, .XZ, .Z, .ZIP

Популярната архивираща програма **7Zip** може да отваря повечето от тях – факт, който понякога се използва от авторите на рансомуер с цел заобикалянето на филтрирането на файлови разширения. Самият изпълним файл се изпраща на потребителя в някаква архива от горния тип и в съобщението потребителят се инструктира да го отвори, като цъкне на нея и след това на съдържащия се в нея файл. Понякога архивата е защитена с парола (например, за да не могат антивирусните програми, сканиращи пощата, да видят злонамереното съдържание) като в съобщението пише каква е паролата, за да може получателят да отвори архивата.

Някои сървъри за електронна поща (и особено антивирусни програми, предназначени за сканиране на електронната поща) могат да видят съдържанието на архивите. Дори ако съдържанието на намиращите се в тях файлове е недостъпно (например, защото архивата е защитена с парола), имената и разширенията им са видими и ако сред тях има файлове с “опасни” разширения, съобщението съдържащо архивата трябва да бъде филтрирано.

Най-сетне, не забравяйте, че редица документи (файлове, с разширения **.DOC, .DOCM, .DOCX, .DOT, .MDA, .MDB, .MDE, .MDZ, .MSG, .ODF, .PDF,**

.PPA, PPS, .PPT, PPTM, .PRJ, .PUB, .RTF, .XLA, .XLB, .XLS, .XLSM, .XLSX, .XLT и др.) могат да съдържат изпълним код (макроси, скриптове и др.). Ако сървърът ви за електронна поща или използваните към него антивирусни програми го позволяват, филтрирайте документите, които съдържат макроси. По-специално за защита от макросите в документи на Microsoft Office ще спомена малко по-нататък.

5.4. Направете безопасно цъкането по скриптови файлове.

Съветът, даден в секция 5.1 е добър, но не е надежден, в смисъл че не може да се разчита, че потребителите ще го спазват стриктно. Ситуацията може да се подобри като направите така, че двойното цъкане на файл, съдържащ скрипт, да отваря текстов редактор за редактиране на скрипта (например, Notepad), вместо да изпълнява самия скрипт. (Скриптове все още ще могат да се изпълняват от командния ред или чрез цъкане с десния бутон на мишката върху файла и избиране на съответната команда от появяващото се контекстно меню; този трик ще ви предпази просто от неволното двойно цъкане върху файла.)

Файловите разширения, които трябва да се обработват по този начин са следните:

.BAT, .BTM, .CMD, .INF, .JS, .JSE, .MSC, .MSH, .MSH1, .MSH1XML, .MSH2, .MSH2XML, .MSHXML, .PS1, .PS1XML, .PS2, .PS2XML, .PSC1, .PSC2, .REG, .SCF, .VB, .VBE, .VBS, .WS, .WSC, .WSF, .WSH

Да вземем само един пример, разширението **.JS**.

За да постигнете желания ефект на самостоятелен компютър (т.е., ако сте индивидуален потребител), направете следното:

1) Control Panel > Default Programs > Set Associations
2) Изберете желаното файлово разширение, в нашия пример **.JS**.
3) Цъкнете бутона Change Program.
4) Изберете Notepad. (Ако го няма в списъка, цъкнете бутона Browse и намерете файла notepad.exe на диска си; обикновено е в папката C:\Windows.)
5) Цъкнете бутона OK.

Ако сте мрежови администратор, можете да използвате group policy за да направите това на всички компютри в мрежата си:

1) Start > Administrative Tools > Group Policy Management Console
2) User Configuration > Preferences > Control Panel Settings
3) Цъкнете с десния бутон на Folder Options и изберете New > Open with от контекстното меню.
4) Въведете файловото разширение (**js** в нашия пример) и пътя до програмата, която да го отваря (**%windir%\notepad.exe**) и изберете Set as default.
5) Цъкнете бутона OK.

5.5. Използвайте средство за блокиране на рекламите.

За да се предпазите от вредителски реклами, използвайте някаква добавка към браузъра си, която блокира рекламите по сайтовете. Две от най-добрите са AdBlock Plus и uBlock Origin. Има ги както за Firefox, така и за Chrome. Първата има версия и за Internet Explorer.

Използването на блокировчик за рекламите има и други предимства. Например, сайтовете, които посещавате, ще изглеждат много “по-чисти” и по тях няма да има реклами, ко-

ито отвличат вниманието, и които понякога даже засенчват основното съдържание на сайта. Освен това, зареждането на страниците на сайтовете ще става забележимо по-бързо.

Това обаче, може да има и някои отрицателни странични ефекти. Например, някои сайтове се опитват да се борят с блокировчиците на реклами като отказват да показват съдържанието си, ако усетят, че посетителят използва такъв. Въпреки това, съветът ми е просто да се откажете да четете такива сайтове – заслужава си, като се има в предвид от каква опасност се предпазвате.

5.6. Блокирайте Flash и скриптовете, ако можете.

Този съвет е мощно средство да ликвидирате опасността от заразяване с рансомуер от компрометиран сайт или от вредителска реклама – просто изключете в браузъра си способността му да изпълнява JavaScript и Flash. За съжаление, в наши дни почти всички популярни сайтове използват много активно Flash и особено JavaScript. Ако ги изключите, най-вероятно много от сайтовете, които посещавате редовно, ще станат неизползваеми. Има две сравнително по-приемливи алтернативи:

1) Ако използвате Firefox, инсталирайте си добавката NoScript. Еквивалентната добавка за Chrome се нарича ScriptSafe. Тази добавка ви позволява да включвате и изключвате изпълнението на скриптове за отделни сайтове.

2) Конфигурирайте Flash така, че да се изпълнява само след като цъкнете върху съдържащия го обект на страницата на сайта, а не автоматично. За Firefox това се прави така: Tools > Add-ons > Plugins > Shockwave Flash > Ask to activate. Процедурата за Chrome е: Settings > Show advanced settings > Privacy > Content settings > Plugins > Manage individual plugins > Adobe Flash Player, погрижете се на “Always allowed to run” да *няма* отметка.

5.7. Използвайте антивирусна система (не просто скенер).

Списъкът от съвети за това, какво да правите, за да се предпазите от вредителски програми би бил непълен без съвета да използвате антивирусна програма. Обърнете внимание, обаче, че обикновен скенер едва ли ще е достатъчен за да ви предпази от първия етап на атаката. Това е, защото той обикновено се състои от малка програма, която веднъж изпълнила се на машината на жертвата, се свързва с някакъв сървър и сваля оттам самия рансомуер.

Тази малка програма обикновено е макрос в документ за Microsoft Word или Excel, или пък скрипт (най-често JavaScript) във вредителска реклама или компрометиран сайт. Тя е внимателно конструирана от създателя си така, че съществуващите до момента скенери да не я хващат. Разбира се, скенерите скоро ще бъдат обновени, след като стане известно за атаката, но дотогава авторът отново ще е променил програмата така, че тя да не се открива. Тъй като програмата е малка и проста, генерирането на нови нейни варианти е лесно и често пъти е автоматизирано.

Така че, скенерът най-вероятно ще пропусне тази програма. Но съвременните антивирусни системи са много повече от скенери. Те имат компоненти, които ще засекат че заразената машина се опитва да се свърже със съмнителен сървър по Интернет и да свали оттам изпълним файл, който също не е известен като широкоразпространена полезна програма. Когато рансомуерът се опита да шифрова файловете на засегнатата машина (а често пъти и файловете в локалната мрежа, до която тази машина има достъп), някои антивирусни системи може да се усетят, че се случва нещо подозрително (последователен достъп до голям брой файлове, използване на системните функции за шифровка, изтриване на файловете след прочитането им и т.н.) и да вдигнат тревога.

И, разбира се, както беше споменато в секция 5.1, убедете се, че антивирусната ви програма наистина работи, лицензът ѝ не е изтекъл, и че тя редовно се обновява.

5.8. Обезопасете макросите в Office.

Както видяхме в секция 3.1.1, един от най-разпространените методи, използвани от рансомуера за проникване в машините на жертвите, е чрез спам съобщения, разпращани по електронната поща. Много често тези съобщения съдържат прикачен файл, който е някакъв вид документ за Microsoft Office – обикновено за Word или Excel. Документът съдържа макроси, които се грижат да свалят и изпълнят основната част на рансомуера.

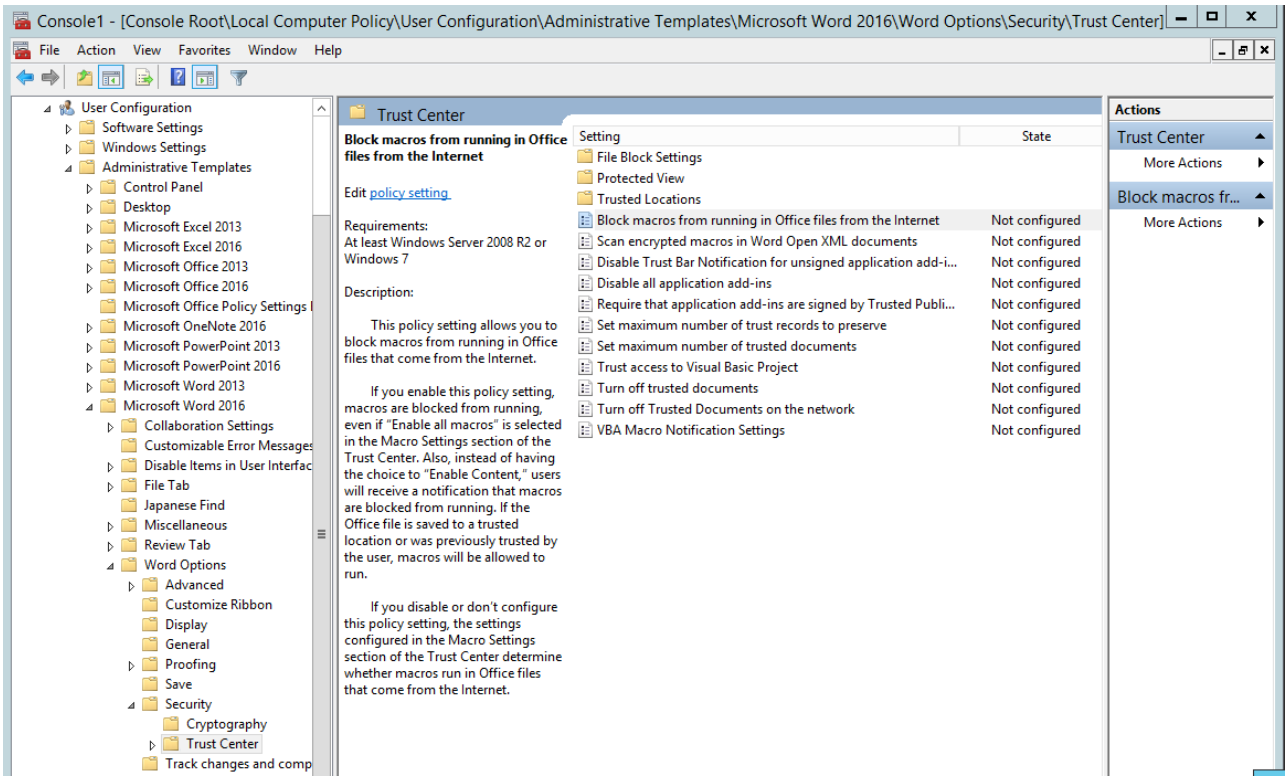
По подразбиране, Office забранява изпълнението на макросите, намиращи се в документите, освен ако не са цифрово подписани с ключ, за който потребителят е указал, че му има доверие. За съжаление, тази идея има редица проблеми. Преди всичко, малко потребители имат дисциплината да подпишат цифрово всички макроси, които ще използват. Това важи с особена сила за потребителите на Excel, които редовно записват свои собствени макроси, улесняващи автоматизирането на работата им с електронни таблици. Освен това, дори ако изпълнението на макросите бъде блокирано, потребителят получава известие за това и му се дава възможността да го разблокира с просто цъкане върху бутон на екрана. А документите, с които пристига рансомуерът, обикновено са така написани, та да убедят потребителя да разреши изпълнението на макросите.

Наистина, ако сте администратор на компютърна мрежа във фирма, можете да забраните напълно изпълнението на всякакви макроси с помощта на global policy, при това така, че потребителите на работните станции да не могат да разрешат изпълнението им. Но това не е практична идея, защото потребителите на Excel ще се разбунтуват. Има много по-добър начин, в зависимост от това, коя именно версия на Microsoft Office използвате.

5.8.1. Обезопасяване на макросите в Microsoft Office 2016.

Ако използвате Microsoft Office 2016, можете да забраните изпълнението на макроси (без потребителят да може да го разреши) *само* в документи, получени по Интернет (т.е., по електронната поща, свалени през браузъра и т.н.). Макросите, намиращи се във вашите собствени, вътрешно създадени документи, ще се изпълняват без проблеми.

За да го постигнете, направете следното: от Group Policy Management Console, отидете на Local Computer Policy > User Configuration > Administrative Templates > Microsoft Word 2016 > Word options > Security > Trust Center. Изберете Block macros from running in Office files from the Internet и го конфигурирайте да бъде “enabled”. Направете същото и за Microsoft Excel 2016 и Microsoft PowerPoint 2016.



5.8.2. Обезопасяване на макросите в Microsoft Office 2013.

От Group Policy Management Console, отидете на Local Computer Policy > User Configuration > Administrative Templates > Microsoft Word 2013 > Word options > Security > Trust Center > Trusted Locations и конфигурирайте някаква папка на сървъра си, която е достъпна за всички потребители (напр. \\server\public\office\macros). Изпълнението на макросите в документите, намиращи се в тази папка, ще бъде разрешено за всички потребители. Инструктирайте потребителите си да записват макросите, които искат да използват, в документи намиращи се в тази папка. Конфигурирайте това и за другите програми от Office – Excel, PowerPoint и т.н.

Същевременно, забранете използването на макроси, които не са цифрово подписани, без потребителят да има възможността да заобиколи забраната. За целта, в Trust Center конфигурирайте опцията "VBA Macro Notification Settings" да бъде "enabled" и сложена на "Disable all except digitally signed macros".

5.9. Преименувайте VSSADMIN.EXE.

Съвременният рансомуер използва административната програма на Windows, наречена **`VSSADMIN.EXE`**, за да изтрие резервните копия на файловете – така наречените shadow copies. Един сравнително евтин "трик" е да я преименувате на нещо друго – например на **`WHATEVER.EXE`**, но си изберете някакво друго, свое име, а не нещо стандартно, което би могло да бъде отгатнато от авторите на рансомуера.

За да извършите преименуването, изпълнете следната процедура:

1) Цъкнете на бутона Start и в полето за търсене въведете "Command Prompt" (без кавичките). Ще излезе списък резултати от търсенето, който най-вероятно ще има само един елемент, наречен "Command Prompt".

2) Цъкнете с десния клавиш на мишката върху този елемент и изберете "Run as Administrator" от контекстното меню, което ще се покаже.

3) Защитната система на Windows, наречена UAC, може да ви поиска потвърждение, че наистина искате да направите това, и даже и паролата на администратора. Отговорете утвърдително и въведете паролата, ако се налага.

4) Ще се отвори прозорецът на командния промпт. В него въведете следните команди:

5) **`cd %WinDir%\system32`**

   Това прави текуща папката, в която се намира програмата **`VSSADMIN.EXE`**.

6) **`takeown /F vssadmin.exe /A`**

   Това променя притежателя на тази програма (която по принцип принадлежи на потребителя System) на текущия потребител (Administrator), за да може той да я променя.

7) **`cacls vssadmin.exe /E /G "Administrators":C`**

   Това дава на потребителите от групата на администраторите (какъвто е и текущият потребител) правата да променят свойствата на програмата, включително и името ѝ.

8) **`ren vssadmin.exe whatever.exe`**

Това променя името на файла **`VSSADMIN.EXE`** на новото име, което сме избрали (в нашия пример – **`WHATEVER.EXE`**).

9) Затворете прозореца на командния промпт.

5.10. Правете си редовно резервни копия!

Както беше споменато в секция 4.5, най-сигурното средство срещу рансомуера е редовното правене на резервните копия на ценната информация. Въпреки това, има някои тънкости, за които трябва да се внимава:

- От време на време проверявайте дали наистина можете да възстановите информацията от резервните копия. Ако нещо сте объркали и не можете, желателно е да го откриете (и да го оправите!) преди да ви е нападнал рансомуер.

- Правете резервни копия толкова често, колкото е необходимо, за да може загубата на информация да не се отрази отрицателно на работата ви. Например, ако сте частно лице, информацията на личния ви (несвързан с работата ви) компютър вероятно не се променя съществено по-често от веднъж в месеца – затова правенето на резервни копия веднъж месечно вероятно е достатъчно. Но ако сте фирма, за която загубата дори на един ден информация може да има фатално отражение на бизнеса – правете резервни копия в края на всеки работен ден. Разбира се, не е нужно да копирате всичко от компютъра си; повечето програми за правене на резервни копия могат да копират само тези файлове, които са се променили (или са били създадени) след последното правене на резервни копия. Освен това, за повечето фирми от съществено значение са предимно данните им, а не инсталираните на компютрите програми – тъй като вероятно последните са сравнително малък и стандартен набор и лесно могат да се инсталират отново. Пък и рансомуерът обикновено шифрова именно файлове с данни, а не програми.

- Въпреки че в секция 4.3 ви посъветвахме по принцип да не бързате с отстраняването на вредителската програма, ако вече сте се решили да възстановите информацията си от резервни копия, тук важи точно обратният съвет. Обезателно премахнете рансомуера преди заразената машина да има достъп до носителя, на който се намират резервните копия. Това е необходимо, защото в противен случай тези резервни копия могат да бъдат шифровани в момента, в който рансомуерът получи достъп до тях.

- Резервните копия трябва да се правят на външен носител, който да не е постоянно свързан с машината, а да се свързва с нея само когато се правят резервните копия (или когато информацията се възстановява от тях). В никакъв случай не правете гафа, направен от полицейския участък в Лос Анджелис, който държал резервните копия на информацията си в отделна папка на същата машина, на която се намирала информацията. Не дръжте резервните си копия на и във вид на файлове на някой сървър, ако машината ви е постоянно свързана с него. Това включва както сървъри на локалната мрежа, така и станалите напоследък популярни “облакови” услуги (т.е., на някакъв отдалечен сървър, с който се свързвате по Интернет, като DropBox, OneDrive и др.). Докато правенето на резервни копия на такива сървъри е много просто, удобно и лесно автоматизируемо, то е опасно, защото постоянната връзка означава, че ако машината ви се зарази с рансомуер, последният също ще има връзка със сървъра и би могъл да шифрова (или просто да изтрие) всички резервни копия, които намери там. Наистина, някои такива услуги (например, DropBox) съхраняват редица стари версии на файловете, които се

пазят там и ви позволяват да възстановите версия от преди времето на шифровката. Въпреки това, този процес е доста сложен и уязвим на грешки, особено ако количеството файлове е голямо или пък имената им са били променени драстично. Затова най-сигурният подход е да използвате такава система за правене на резервни копия, която изпраща информацията до специализиран сървър, който я записва на местен носител, но самите резервни копия не са видими като файлове от вашата машина.

6. Заключение

Шифроващите вредителски програми в момента са една експлозивно процъфтяваща престъпна индустрия. Те нанасят щети в размера на стотици милиони долари годишно по целия свят. Те са и един от най-често срещаните проблеми, с който потребителите в България се обръщат за помощ към нашата Лаборатория. Този проблем несъмнено ще продължи да се развива в обозримо бъдеще. Той трябва да бъде приеман много сериозно и потребителите, както частни лица, така и фирми, са длъжни да направят всичко, което е по силите им, за да се предпазят от него и да могат лесно да се възстановяват след евентуална успешна атака.

Литература

Young, A.; M. Yung (1996). *Cryptovirology: extortion-based security threats and countermeasures*. IEEE Symposium on Security and Privacy. pp. 129–140. doi 10.1109/SECPRI.1996.502676 ISBN 0-8186-7417-2.

Danchev, Dancho. *New ransomware locks PCs, demands premium SMS for removal*, ZDNet, 22 April 2009.

Blue, Violet. *CryptoLocker's crimewave: A trail of millions in laundered Bitcoin*, ZDnet, 22 December 2013.

Gallagher, Sean. *FBI says crypto ransomware has raked in >$18 million for cybercriminals*, Ars Technica, 25 June 2015.

Constantin, Luchian. *File-encrypting ransomware starts targeting Linux web servers*, PC World, 9 November 2015.

Hern, Alex. *Major sites including New York Times and BBC hit by 'ransomware' malvertising*, The Guardian, 16 March 2016.

Hasherazade, Petya. *Taking the Ransomware to the Low Level, Malwarebytes Labs*, 1 April 2016.

Hennigan, W. J., Bennett, B. *Criminal hackers now target hospitals, police stations and schools*, Los Angeles Times, 6 June 2016.

Davis, Reremy. *Report: 93 percent of phishing emails contained ransomware*, SC Magazine, 6 June 2016.

Franceschi-Bicchierai, Lorenzo. *Hackers Make the First-Ever Ransomware for Smart Thermostats*, Motherboard, August 7 2016.