RANSOMWARE ATTACKS AND COUNTERMEASURES

VICTORIA R. YANAKIEVA, TEODORA T. STOYANOVA

ABSTRACT: *One of the most important aspects of ensuring the security of computer systems is the identification, analysis and classification of possible threats to them. Ransomware is a malware that infects a computer device, resulting the information in its memory becoming unavailable to users. The prognosis for 2018 is that a significant increase in ransomware attacks is expected. For this reason, a number of organizations are looking for ways to deal with these growing threats.*

KEYWORDS: *Malware, Ransomware, cyberattack, WannaCry, Petya/NotPetya, BadRabbit.*

RANSOMWARE АТАКИ И ПРОТИВОДЕЙСТВИЕ*

ВИКТОРИЯ Р. ЯНАКИЕВА, ТЕОДОРА Т. СТОЯНОВА

АБСТРАКТ: *Един от най-важните аспекти на осигуряване на сигурността на компютърните системи е определянето, анализа и класификацията на възможните заплахи за тях. Ransomware е злонамерен софтуер, който заразява компютърното устройство, в резултат на което информацията в неговата памет става недостъпна за потребителите. Прогнозата за 2018 г. е, че се очаква значително увеличание на ransomware атаките. Поради тази причина, редица организации търсят начин да се справят с тези зачестили заплахи.*

1 Въведение

Целта на всяка компютърна информационна система е предоставяне на пълна, достоверна и своевременна информация. При всички информационни процеси в такива системи и мрежи в реални условия, тази информация е уязвима, както поради случайни, така и поради злонамерени дестабилизиращи фактори (заплахи), което налага да се вземат мерки за нейната защита, чрез които се постига нужното ниво на информационна сигурност [1].

Може да се приеме, че терминът информационна сигурност се отнася за състоянието на защитеност на жизнено важните интереси в информационната сфера на фирмите и хората в тях от вътрешни и външни заплахи [2].

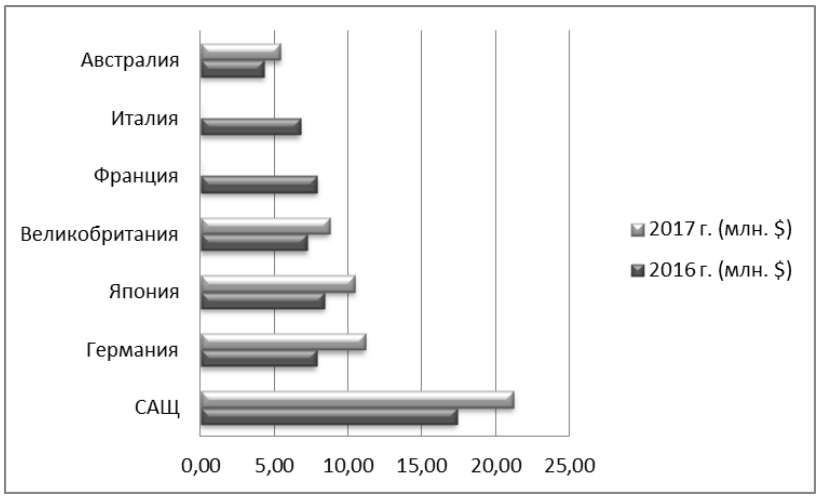
Необходимостта от защитата на различни информационни системи (частни и държавни) от външни заплахи, като изтичане на чувствителна за организацията информация, е очевидна на всички етапи от развитието на системите за защита на информацията. През последните години се обръща все по-голямо внимание на този вид заплаха поради щетите, нанасяни от нея на компаниите и организациите.

Чрез кибератаките се цели да се промени или разбие компютърна система или мрежа, която съхранява или предава дадена информация или програма.

Съгласно редовното годишно изследване на авторитетния американски институт Ponemon, на фиг. 1 се представят оценените средни разходи за престъпления в киберпространството за седем страни, включващи 254 отделни компании, през последните две години (2016-2017 г.). Компаниите в САЩ отчитат най-високата обща средна стойност, а в Австралия - най-ниската. През 2017 г. Германия бележи значително

* Настоящата статия е частично финансирана по проект № РД-08-159/09.02.2018, „Надеждност и защита на информация в социалните мрежи, графичните и 3D обекти в добавена и виртуална реалност“

увеличение на общите разходи за киберпрестъпленията (липсват данни за Италия и Франция за 2016 г.).



Фиг. 1. Средни разходи за престъпления в киберпространството за седем държави

Система за защита на информацията (СЗИ) (security system) е организирана съвкупност на всички органи, средства, методи и мероприятия, предвидени в информационна система за осигуряване на защита на информацията от разгласяване, изтичане и несанкциониран достъп към нея [3].

2 Видове заплахи

Класификацията на видовете заплахи може да бъде направена по различни критерии, но тя не е фиксирана, тъй като с развитие на техниката и технологиите се увеличават видовете заплахи [3,4]. Според природата им на произход, те могат да бъдат естествени (напр. природни явления, независещи от човека) и изкуствени (предизвикани от хората). Последните, според мотивацията на хората, се подразделят на случайни (непреднамерени) и умишлени (преднамерени), които са свързани с користни цели на субектите.

Според източника спрямо обекта на защита, заплахите са външни и вътрешни. На фиг. 2. е показана тази връзка [3].

Процентът на външните заплахи за дадена организация е много висок. Атаките могат да бъдат активни или пасивни. При активните се генерират пакети или участват в мрежата, докато при пасивна атака се подслушва мрежата или се проследяват потребителите [5].

От външните преднамерени заплахи - злонамерените атаки се извършват чрез прикачени файлове към имейл или чрез посещение на подозрителни заразени уебсайтове. Като някой от най-често срещаните видове заплахи са:

- *Spyware*

Този типове злонамерен софтуер остава скрит, докато събира ценна информация. Достатъчно е да се деинсталира, за да бъде премахнат от компютъра.

- Trojan horse (Троянски кон)

Злонамереният софтуер тип „троянски кон“ заразява компютъра, най-често маскиран като антивирусен софтуер или компютърна игра.

- *Drive-by-downloads*

Злонамереният код е вграден предимно в новинарски уебсайтове и след посещение на страницата започва сканиране на компютъра за уязвимости в сигурността, т.е. остарели приложения, плъгини за браузъри, приложения за чат и т.н.

- *Botnet*

След заразяване със злонамерен код, чрез интернет компютъра се свързва с контролен компютър. Най-уязвим софтуер са браузърите, Adobe Flash, Adobe Reader и Java. Актуализирането на приложенията може да блокира 65% от атакуващите вектори.

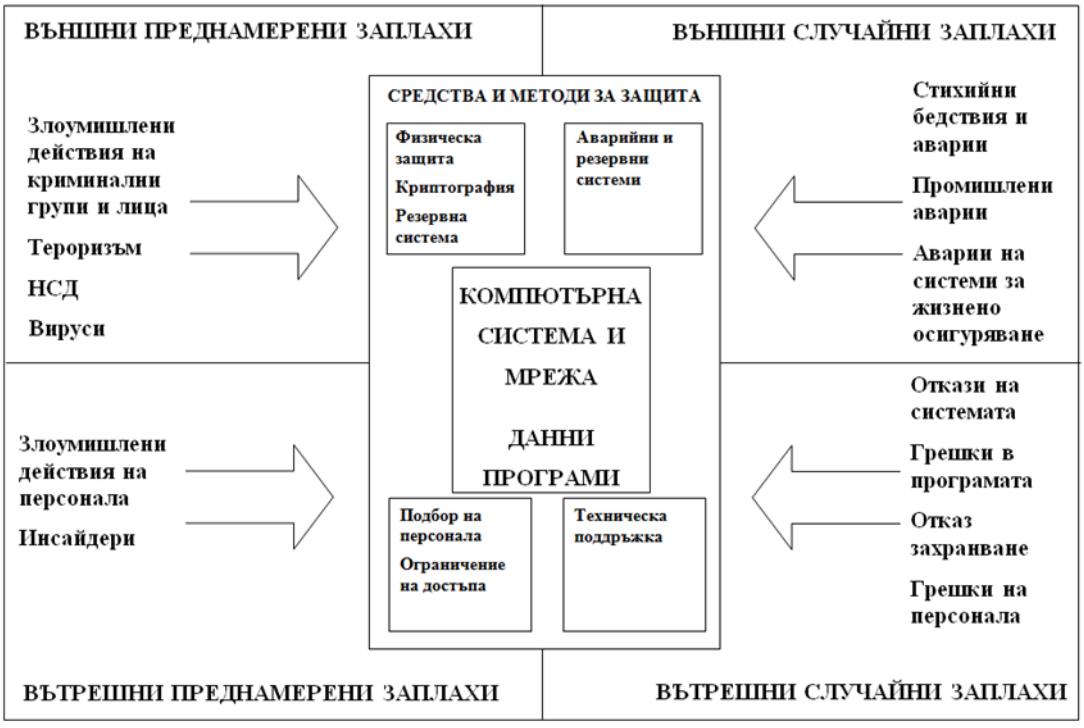
- *Adware*

Adware често се изтегля заедно с безплатните програми. Той е злонамерен софтуер, използван за проследяване на онлайн поведението на заразения потребител.

- *Ransomware*

Най-разпространените видове ransomware криптират всички или някои от данните на компютъра и след това изискват голямо плащане (откуп), за да се възстанови достъпа до данните. Този тип злонамерен софтуер е предпочитан, до голяма степен благодарение на криптовалутата Bitcoin [5,6,7].

Съществуват редица други видове злонамерен софтуер, но настоящата статия се фокусира върху актуалните през последните три години ransomware заплахи [8].



Фиг. 2. Връзка на заплахите с обекта на защита

3 Ransomware атаки

Според доклад на Verizon за разследване на пробиви и изтичане на данни за 2017 г., ransomware е петата най-разпространена форма на злонамерен софтуер през 2016 г., издигайки се от позиция 22 през 2014 г. Всъщност от 2016 г. насам са се появили над 200 нови вида ransomware.

Най-засегнатите страни от 1 април до 3 октомври 2017 г са: САЩ (17,2%), Великобритания (11,1%), Белгия (8,6%) и т.н. [9]

Ransomware атаките са значително по-бързи и по-евтини за изпълнение в сравнение с много други кибер заплахи, и имат много по-висока печалба.

Предимствата на ransomware злонамерен софтуер са:

• По-лесно е да се изпрати криптовалута, отколкото традиционните пари.

• По-малко хора участват в операцията, от където следва, че хакерите имат по-голяма печалба.

Има няколко различни начина, по които хакерите избират организациите, към които да приложат ransomware атака. В повечето случаи се насочват към университетите, защото те са с по-малка защита и различна потребителска база, което улеснява проникването в защитата им.

Държавни агенции, адвокатски кантори или медицински центрове са предпочитани от хакерите, защото е по-вероятно бързо да платят откуп тъй като, се нуждаят от незабавен достъп до файловете си [10].

Анализът на Check Point показва, че през 2015 г. ransomware атаките причиняват щети от 325 милиона долара. За следващата година атаките са се увеличили 15 пъти, струвайки 5 милиарда долара [11].

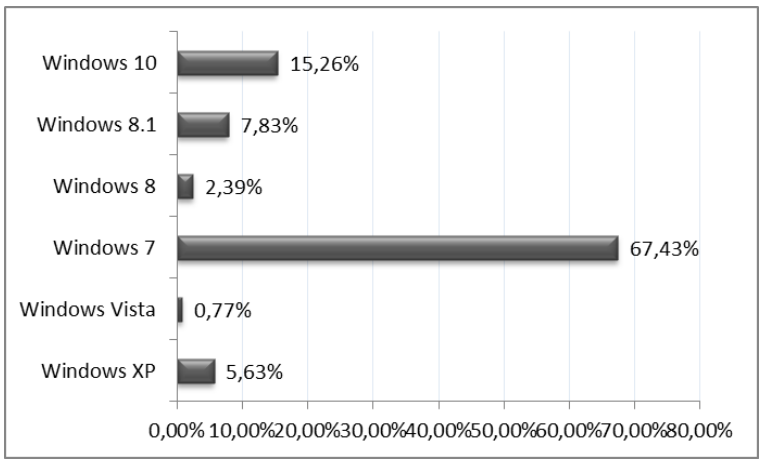
Най-актуалните през последните две години ransomware атаки са WannaCry, Petya/NotPetya и BadRabbit.

3.1 WannaCry

WannaCry е зловреден софтуер създаден през май 2017 г., с вероятен произход Северна Корея. Познат е като WanaCrypt, Wana Crypt0r и Wana Decrypt0r. Използва EternalBlue exploit, откраднат от хакерите The Shadow Brokers от американската агенция за национална сигурност, и причинява щети на летища, банки, университети, болници и др. Разпространява се в около 150 страни по света, главно Русия, Украйна, САЩ и Индия. За възстановяване на файловете е необходимо плащане с Bitcoin криптовалута, като при просрочване на даденото време от 72 часа цената се удвоява. Седем дни след заразяване със злонамереният софтуер следва изтриване на файловете от компютъра. WannaCry сканира за TCP и UDP портове 139 и 445 (SMB) от компютрите [11].

Данните от Kaspersky показаха, че по-голямата част от инфектираните с WannaCry компютри са с операционна система Windows 7, показано на фиг. 3.

WannaCry представлява 45,3% от всички ransomware атаки.



Фиг. 3. Съотношение на версиите на операционна система Windows, засегнати от WannaCry

3.2 Petya/NotPetya

Petya е ransomware софтуер, който заразява целевия компютър, криптира някои от данните в него и извежда на екрана съобщение, обясняващо как може да се плати в Bitcoin, за да получат ключовете, нужни за декриптиране на данните. В първоначалния вариант на зловреден софтуер Petya, която започна да се разпространява през март 2016 г., достига компютъра на жертвата, прикрепен към имейл. Представлява пакет с два файла: изображение и изпълним файл, често с "PDF" в името на файла. След кликване върху този файл и приемане на предупреждението за Windows User Access Control, Petya рестаритира компютъра и инсталира свой собствен зареждащ скрипт. Файлове са в компютъра и не са шифровани, но жертвата няма достъп до частта от файловата система, която указва къде са. В този момент хакерите изискват плащане в Bitcoin, за да декриптират твърдия диск.

През юни 2017 г. се създава подобрена версия на злонамерения софтуер Petya, наречен NotPetya, разпространяващ се бързо, като засегнатите сайтове са фокусирани в Украйна, но се появяват както в Европа, така и извън нея. Новият вариант бързо се разпространява от компютър на компютър и от мрежа в мрежа, без да изисква спам имейли или социално инженерство, за да получи административен достъп. Въпреки, че е разновидност на Petya, NotPetya не попада в графата ransomware вируси [12,13]. NotPetya има някои допълнителни правомощия, които според експертите по сигурността го правят по-опасен от WannaCry.

3.3 BadRabbit

BadRabbit се разпространява чрез фалшиви актуализации на Flash, идващи от компрометирани популярни домейни. Той е сравнително нов ransomware софтуер и споделя 13% от своя код с този на Petya, но ключовите криптиращи функции се обработват от легитимен инструмент за криптиране (DiskCryptor). За разлика от NotPetya, BadRabbit използва уникални Bitcoin портфейли за всяка жертва.

Според данните, представени от ESET по време на актуализирането, 65% от жертвите днес са в Русия, следвани от Украйна (12,2%), България (10,2%), Турция (6,4%) и Япония (3,8%) [14].

4 Противодействие

Има инструменти, специално разработени за борба с ransomware. Проектът No More Ransom - основан през 2016 г. от холандската полиция, Европол EC3, Kaspersky и McAfee и в партньорство с над 100 други организации по целия свят, помогна за декриптирането на 28 000 устройства и обхваща над 100 вида ransomware.

С цел защита на данните фирмите създаващи софтуер добават в настройките опция, включваща:

- Автоматично запазване на копие на базата с данни – директорията може да бъде друг дял на диска, USB памет, виртуално устройство или мрежов адрес.
- E-mail адрес за изпращане на резервните копия на базата данни.

Има няколко действия, чрез които да се противодейства и заплахата да бъде избегната:

- Архивиране на актуални данни.

Стандартното архивиране, което позволява защита от загуба на данни много често не е сигурно, защото хакерите получили достъп до служебни акаунти биха могли да си присвоят архивираната информация. Решението на подобен проблем е използването на

специфични криптографски алгоритми (собствено проектирани) с цел допълнителна защита на информацията на дадена организация [15,16].

• Използване на антивирусен софтуер с добра репутация.

Важен фактор е добрата антивирусна, но и тя не е решение на проблема. Нужно е една малка промяна в кода на ransomware вируса, за да остане неоткриваем. Необходимо е редовно обновяване на антивирусния софтуер.

• Актуализация на операционната система на компютъра [10].

Установено е, че над 50% от системите, засегнати от атаките на ransomware, работят с остаряла операционна система - Windows 7. Необходима е актуализация на операционната система или използването на операционна система като Linux, която е практически неуязвима за вируси.

• Обучение на служителите за правилна кибер-хигиена

Задаване на ясни правила за отваряне на e-mail връзки и прикачени файлове. Забрана за посещаване на несвързани със служебните задължения на служителите сайтове.

• Подсигуряване на мрежата

Изграждане на защитна стена, блокираща достъпа до уязвими портове и услуги в локалната мрежа. Имплементиране в защитната стена на организацията на филтри за уеб съдържание, блокиращи ненадеждни и доказано компрометирани домейни. Имплементиране в mail сървъра на организацията на централизиран, редовно актуализиращ се антивирусен софтуер, сканиращ всяко e-mail съобщение за известните към момента злонамерени кодове.

• Изграждане на навици у обикновения потребител

Честа грешка е инсталиране на неизвестен софтуер или даване на администраторски права. Препоръчително е избягването на посещенията на съмнителни сайтове.

5 Заключение

В този доклад става ясно, че броят на засегнатите потребители и щетите от ransomware атаки ще нараства. Посочените по-горе подходи за превенция на атаките са добра отправна точка в борбата с тези кибер заплахи. Спазването им значително ще ограничи риска и ще гарантира цялостност и сигурност на данните на всеки потребител и организация.

Повечето атаки от този вид засягат потребителите на Windows, но хората не са имунизирани при използването на други платформи, включително мобилни устройства.

ЛИТЕРАТУРА:

[1] Христов, Хр., Сигурност на фирмата и противодействие на посегателствата срещу нея. Университетско издателство „Епископ Константин Преславски“, монография, Шумен (2014). ISBN: 978-954-577-981-7.

[2] Zhelezov, S., Paraskevov, H., Hristov, H., Boyanov, P., Uzunova, B., An architecture of steganological subsystem for information protection. Proceedings of 10-th International Conference ICBBM, Liepaya, Latvia, (2014), 123-128.

[3] Железов, С., Оценка на ефективността на системи за защита на информацията в компютърните системи. Университетско издателство „Епископ Константин Преславски“, дисертация, Шумен (2014).

[4] Станев, С., Железов, С., Компютърна и мрежова сигурност. Университетско издателство „Епископ Константин Преславски”, Шумен (2005). ISBN 954-577-306-5.

[5] Kadir, A. F., Stakhanova, N., Ghorbani, A. A., Understanding Android Financial Malware Attacks: Taxonomy, Characterization, and Challenges. University of New Brunswick (2018).

[6] Asamoah-Okyere, E., The changing face of cybercrime: How mobile devices have changed the approach to committing cybercrime, MSc, University of Strathclyde (2014).

[7] Agrawal, M., Singh, H., Gour, N., Kumar, A., Evaluation on Malware Analysis. International Journal of Computer Science and Information Technologies, 5 (3) (2014), 3381-3383.

[8] Vijayalakshmi, Y., Natarajan, N., Manimegalai, P., Babu, S. S., Study on Emerging Trends in Malware Variants. International Journal of Pure and Applied Mathematics, 116 (22) (2017), 479-489.

[9] Brenner, B., 2018 Malware Forecast: ransomware hits hard, continues to evolve. Sophos, 11 февруари 2017. <https://news.sophos.com/en-us/2017/11/02/2018-malware-forecast-ransomware-hits-hard-crosses-platforms/> (10.07.2018).

[10] Fruhlinger, J., What is ransomware? How it works and how to remove it. CSO, 13 ноември 2017. <https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html> (15.07.2018).

[11] Seals, T., One Year After WannaCry: A Fundamentally Changed Threat Landscape. Threatpost, 17 май 2018. <https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/> (16.07.2018).

[12] Fruhlinger, J., Petya ransomware and NotPetya malware: What you need to know now. CSO, 17 октомври 2017. <https://www.csoonline.com/article/3233210/ ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html> (17.07.2018).

[13] Fox-Brewster, T., Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry. Forbes, 27 юни 2017. <https://www.forbes.com/sites/ thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/#c556f3d532e9> (17.07.2018).

[14] Ragan, S., BadRabbit ransomware attacks multiple media outlets. CSO, 24 октромври 2017. <https://www.csoonline.com/article/3234691/security/badrabbit-ransomware-attacks-multiple-media-outlets.html> (20.07.2018).

[15] Kordov, K., Modified pseudo-random bit generation scheme based on two circle maps and XOR function. Applied Mathematical Sciences, 9 (3) (2015), 129-135.

[16] Kordov, K., Signature Attractor Based Pseudorandom Generation Algorithm. Advanced Studies in Theoretical Physics, 9 (6) (2015), 287 – 293.

Теодора Тихомирова Стоянова
Шуменски университет „Еп. Константин Преславски“
E-mail: t.stoyanova@shu.bg

Виктория Росенова Янакиева
Шуменски университет „Еп. Константин Преславски“
E-mail: v.yanakieva@shu.bg