SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 42, FEBRUARY 2018

DEFENSE THE COMPUTER RESOURCES OF THE GOVERNMENT AGENCIES, PRIVATE ORGANIZATIONS AND ACADEMIC INSTITUTIONS AGAINST THE WANNACRY (WANACRYPT0R 2.0) RANSOMWARE CYBER-ATTACK

Abstract: In this paper a summarized defense the computer resources of the government agencies, private organizations and academic institutions against the wannacry (wanacrypt0r 2.0) ransomware cyber-attack is made. Most of the network system administrators, security professionals, network architects and IT specialists must create security defense mechanisms against all types of modern encryption computer viruses in the computer networks of government agencies and private organizations.

Keywords: Cyber-attacks, Computer resources, Government, Enumeration, Defense, LAN, Ransomware, Security, Vulnerability, WAN, Wanacrypt0r 2.0.

Authors information:

Petar Boyanov
Chief Assistant Professor, PhD,
Lecturer in Department
"Communication and Computer Technologies"
at Konstantin Preslavsky University of Shumen
✉ peshoaikido@abv.bg
Bulgaria

Hristo Hristov
Associate Professor, PhD,
Lecturer in Department
"Management of Security Systems"
at Konstantin Preslavsky University of Shumen
✉ hristov63@abv.bg
Bulgaria

1. Въведение

Компютърните вируси представляват самокопиращи се софтуерни програми, които копират своя код в други изпълними файлове като (".exe", ".bat", ".com", ".vbs" и др.) компютърни зареждащи сектори или документи [20]. Вирусите главно се пренасят чрез сваляне на файлове, отваряне на заразени твърди дискове или USB флаш памети [25], [27], както и прикачвания в електронните съобщения. Типовете компютърни вируси са следните [1], [2], [3], [4], [8], [13], [15], [16], [17], [23], [26], [28]:

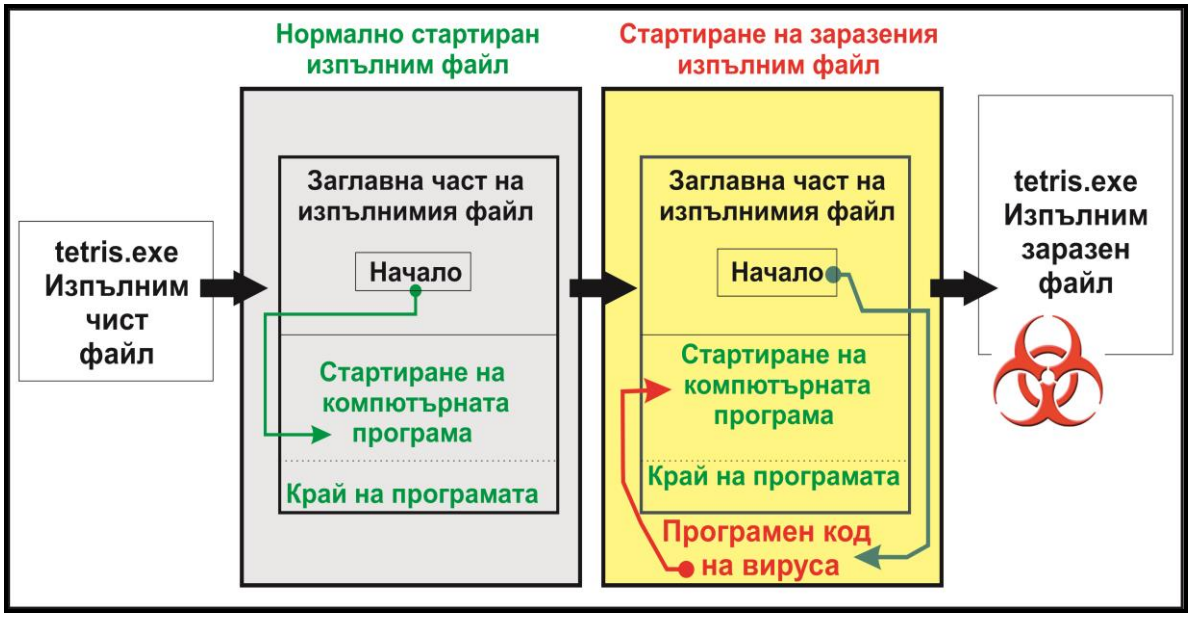
- системни зареждащи вируси;
- файлови вируси;
- макро вируси за различни видове програми от офис пакета на Microsoft;
- скрити вируси в услуги;
- криптиращи вируси;
- полиморфни вируси;
- метаморфни вируси;
- вируси, използващи празното място в файловете;
- вируси с файлови разширения;
- вируси, използващи помощни уеб инструменти в браузерите като "Add-on";
- вируси, развалящи директно кода на програма;
- резидентни вируси в оперативната памет.

2. Изложение

Фазите на живот на един компютърен вирус са:

1. Създаване на компютърния вирус на специален компютърен език за програмиране като python, perl, c, c++, javascript, bash scripting и др.
2. Копиране на компютърния вирус за точно определено време в компютърната машина на служителя от организацията.
3. Активирането (стартирането) на вируса се извършва след стартирането на заразената компютърна програма.
4. Разкриване и изтриване на компютърния вирус чрез антивирусни програми.

Трябва да се знае, че не всички антивирусни програми са способни да изтрият компютърните вируси, поради което се налага цялостно форматиране на твърдите дискове и наново инсталиране на операционната система. На фиг. 1. е показан начинът за заразяване на изпълним файл на компютърната игра - "tetris.exe".



Фиг. 1. Изпълнение на изпълним заразен файл

Киберпрестъпниците създават компютърните вируси с цел:

- Причиняване на физически повреди и щети на компютърната машина жертва на служителя.
- Получаване на финансови облаги и ползи.
- Получаване на важна конфиденциална информация за изследователски или фирмени проекти.
- Извършване на вандалски действия.
- Извършване на кибертероризъм.
- Разпространение на политически съобщения и новини.
- Заплашване на компютърната машина жертва на служителя за удоволствие и игра.

Признаците, по които може да се установи, че компютърната машина жертва на служителя е заразена с компютърен вирус, са [2], [5], [6], [7], [8], [9], [86], [12], [17], [21], [23]:

- Наличие на неразпознати файлове от операционната система.
- Компютърната машина издава нетипични звуци и сигнали.
- Появяване на странни геометрични фигури по екрана на монитора.
- Оперативната памет е винаги запълнена догоре, което довежда до пълен срив на компютърната машина.
- Изключително дълго зареждане на софтуерните програми.
- Твърдият хард диск е винаги пълен и няма повече свободно място.

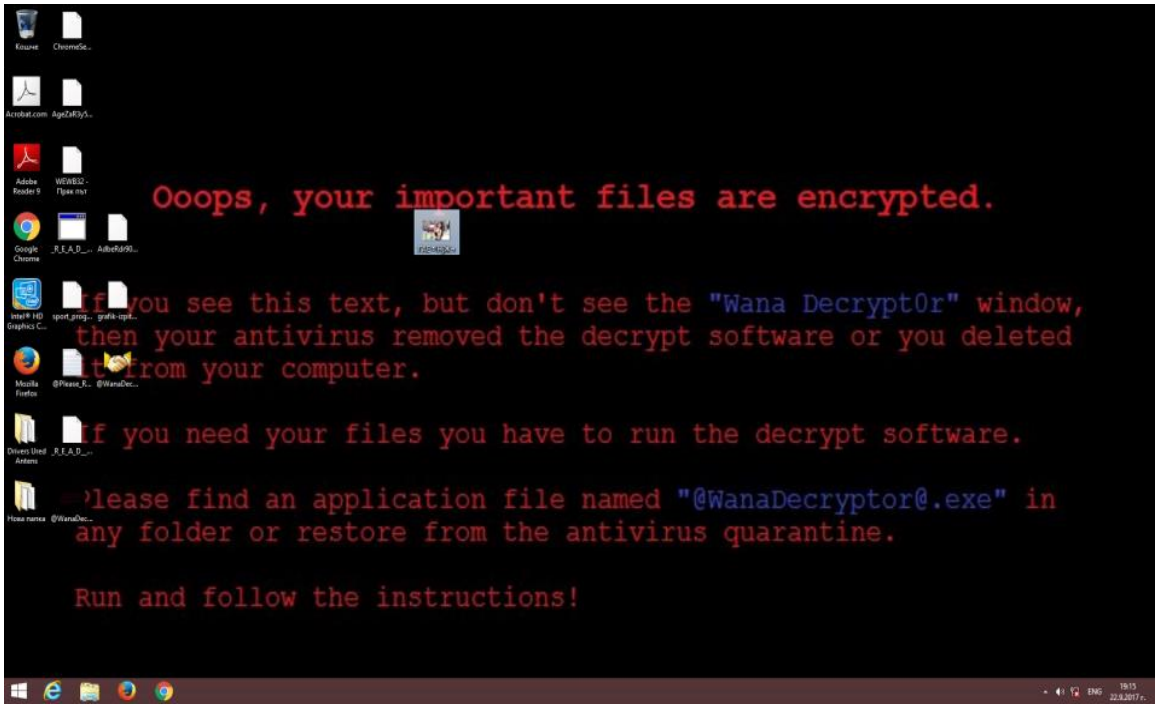
Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), служителите по развитие и експлоатация на (АИС/М), администраторът по сигурността, както и потребителите на АИС/М могат да бъдат заразени от компютърни вируси чрез [1], [5], [6], [7], [25], [26], [27], [28]:

- Инсталиране на пиратски софтуерни програми.
- Отваряне на заразени прикачени файлове (компютърни архиви с разширения ".zip", ".rar", ".7z", ".tar") от електронната поща.
- Изтегляне и стартиране на изпълними файлове или снимкови файлови без специално сканиране с антивирусна програма.
- Ненавременно обновяване на уеб добавки и програми към даден уеб браузер.
- Необновяване на най-новите дефиниции на антивирусните програми и др.
- Безразборно поставяне на различни USB флаш памети без проверка с антивирусна програма.

В компютърното пространство най-разпространените софтуерни програми, които се използват за създаване на компютърни вируси, са:

- CB Mutate - example VBS poly engine.
- TeraBIT_Virus_Maker_3.0_SE.
- JPS White Shell.
- Zed's Word Macro Virus Constructor.

В началото на месец май 2017 г. се появи един от най-страшните компютърно криптиращи вируси, създавани до момента. Неговото име е WannaCrypt или WanaCrypt0r 2.0, чиято цел е да криптира всички изпълними или неизпълними файлове на операционната система. За да бъдат декриптирани файловете на жертвата, е необходимо тя да си плати чрез виртуалната парична валута - bitcoin. Поради тази цел е направен специален научен експеримент в безжична локална мрежа WLAN (Wireless Local Area Network) от 3 хоста в компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски”. Всеки хост използва безжичен USB адаптер 150Mbps Wireless N USB Adapter TL-WN721N. В компютърната лаборатория се използва безжичен рутер 150Mbps Wireless N Router TL-WR741ND, на който е активиран протоколът DHCP (Dynamic Host Configuration Protocol) с цел автоматично раздаване на IP (Internet Protocol) адреси на всеки хост, който се опита да се свърже с рутера. Безжичната локална мрежа използва двадесет и четири битова мрежова маска и номерът на мрежата е 192.168.254.0, т.е. 192.168.254.0/24. Операционната система, върху която ще бъде инсталиран криптиращия вирус WannaCry, е Microsoft Windows 8.1 x64. На фиг. 2. е показан първоначалният екран, който се появява след изпълнението на криптиращия вирус.

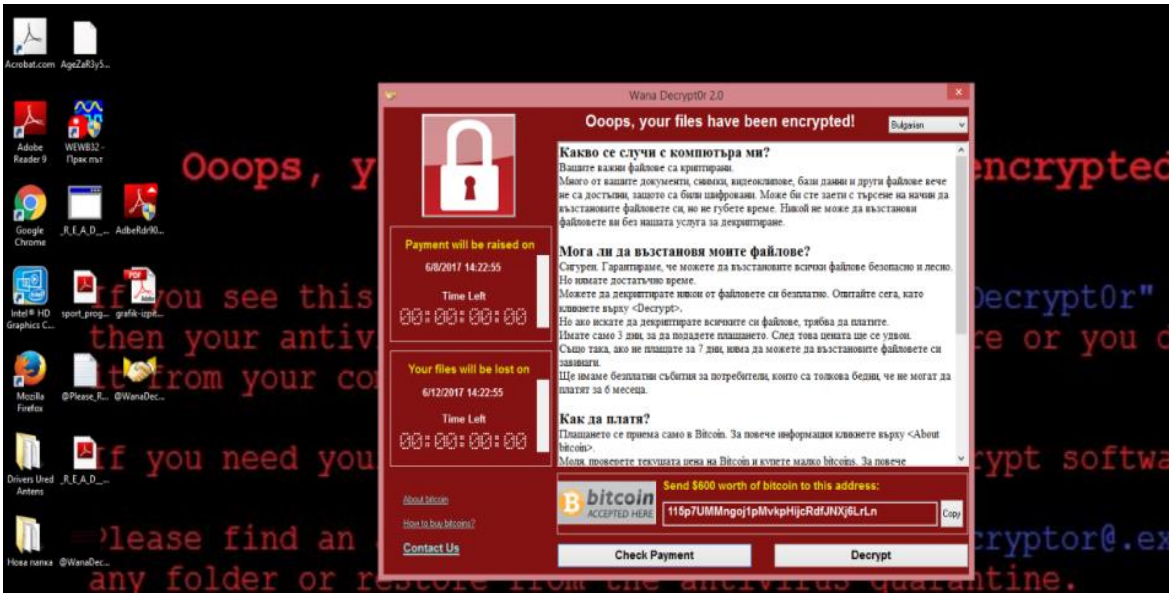


Фиг. 2. Първоначалният екран, който се появява след изпълнението на криптиращия вирус

На фиг. 3. е показана диалоговата кутия с надпис "Wana Decrypt0r 2.0" и съдържащ следната информация:

- "Какво се случи с компютъра ми?".
- "Мога ли да възстановя моите файлове".
- "Как да платя".
- "Контакт".

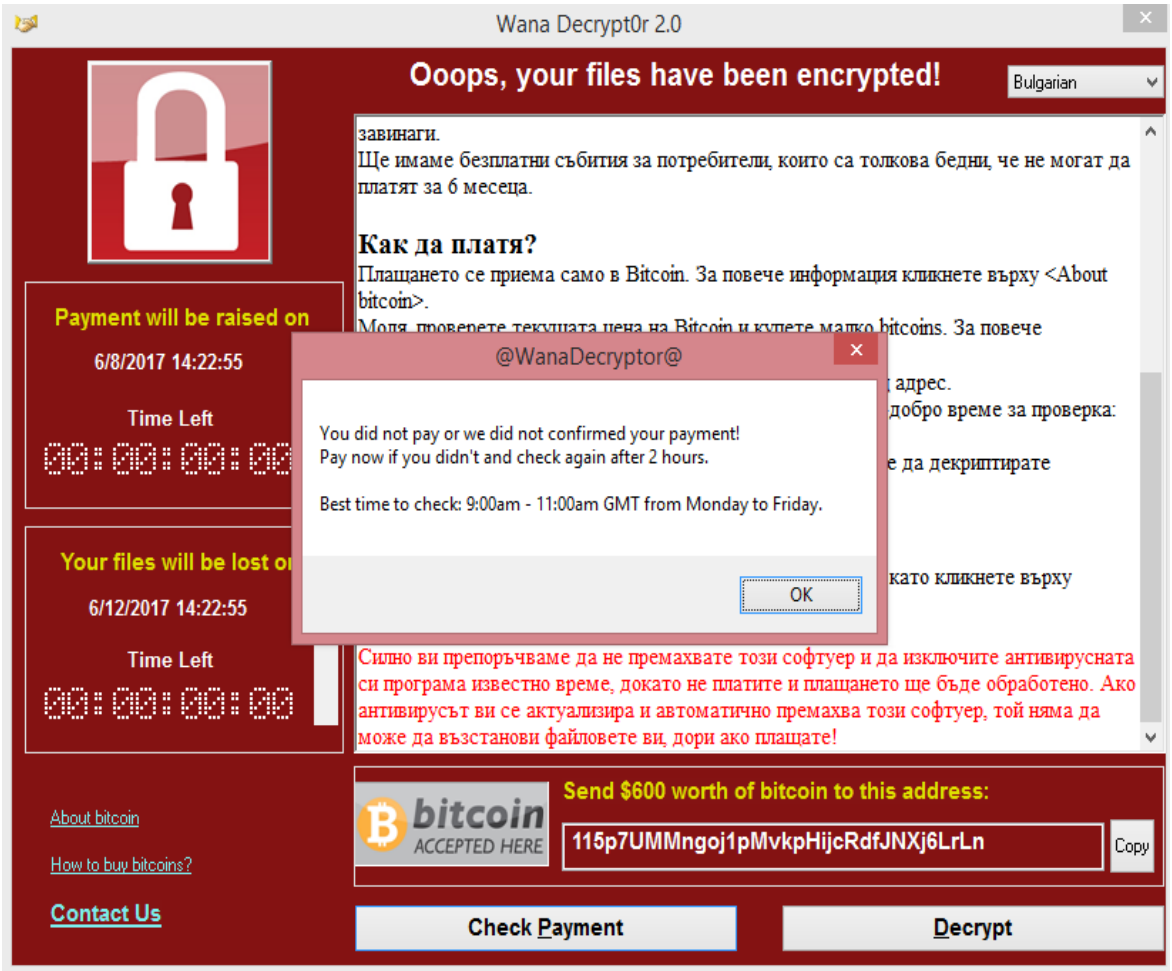
На фиг. 4. е показана цялата диалогова кутия в пълен размер на криптиращия вирус "Wanna Cry".



Фиг. 3. Диалоговата кутия с надпис "Wana Decrypt0r 2.0"

Фиг. 4. Цялата диалогова кутия в пълен размер на криптиращия вирус "Wanna Cry"

На фиг. 5. е показано предупреждение относно кога е удобно жертвата да си плати.

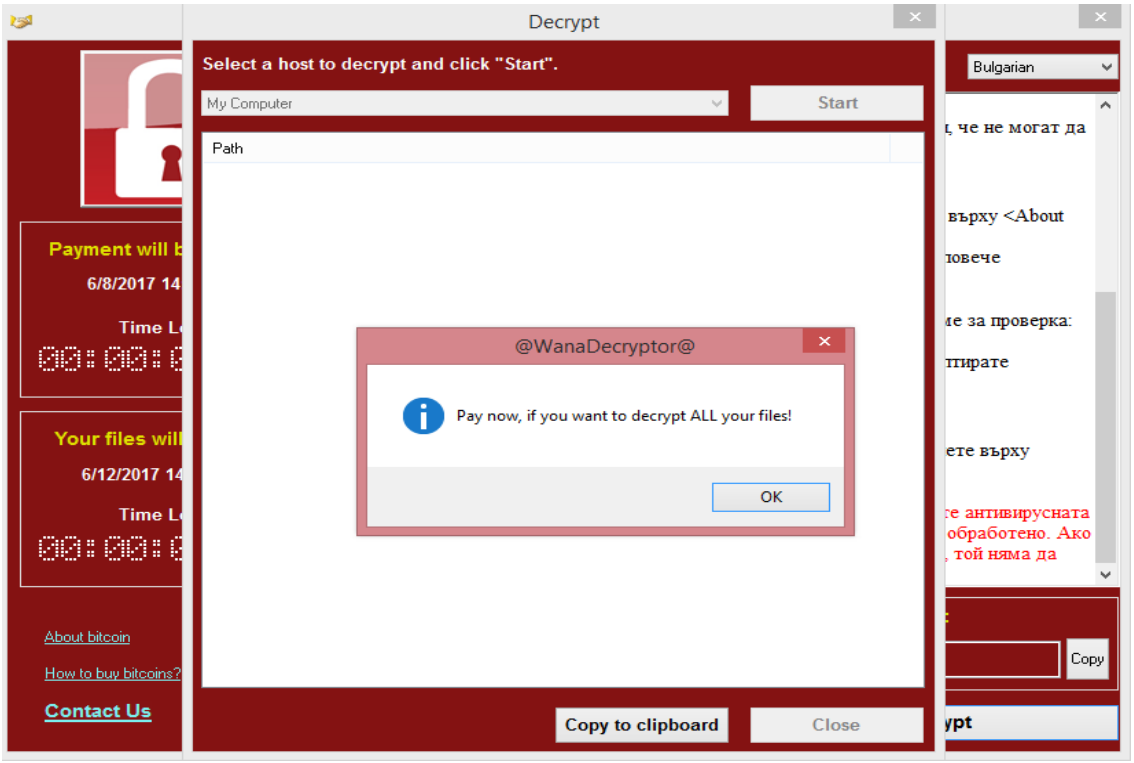


Фиг. 5. Предупреждение относно кога е удобно жертвата да си плати

На фиг. 6. е показан начинът, по който могат да се декриптират файловете. Трябва да се знае, че дори и да си плати жертвата, киберпрестъпниците може и да не пратят декриптиращите ключове.

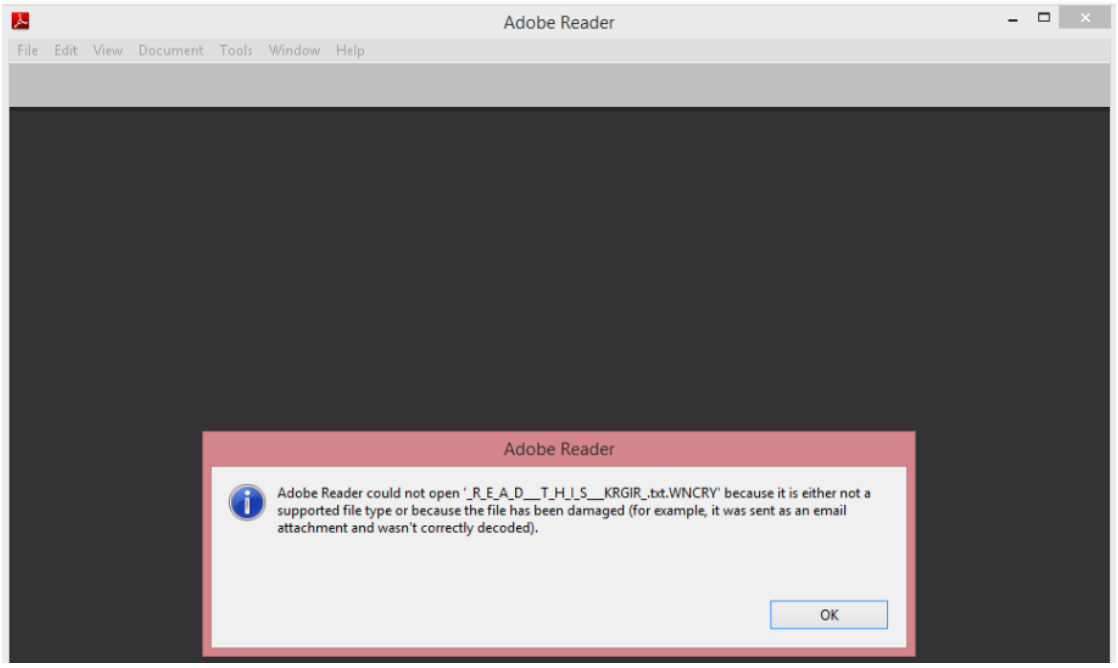
На фиг. 7. е показана системна грешка при опит за отваряне на файл с разширение .pdf. Името на файла е "_R_E_A_D___T_H_I_S___KRGIR_.txt.WNCRY". Както се вижда разширението на криптиращия вирус е ".WNCRY". Установи се, че нито един не може да бъде отворен повече.

На фиг. 8. е показан отвореният текстовия файл с име "@Please_Read_Me@". Този файл се генерира след изпълнението на криптиращия вирус с цел даване на информация за своята жертва на английски език.

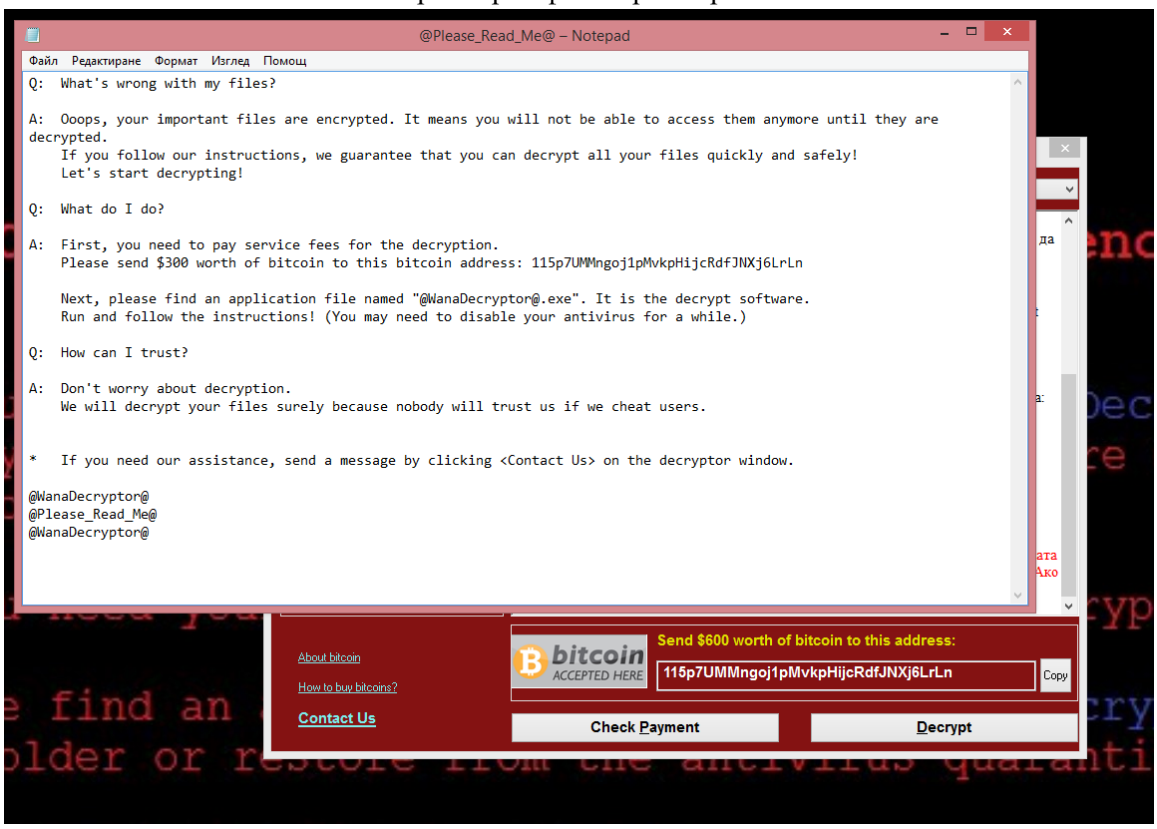


Фиг. 6. Начинът, по който могат да се декриптират файловете

Трябва да се знае също така, че има и определено фиксирано време за пращане на съответната сума за декриптиране на файловете. И отделно има допълнителна дата - 6/12/2017 г. и час 14:22:55 ч., на която всички криптирани файлове ще бъдат изтрити завинаги от операционната система. Финансовите щети след заразяване с такъв криптиращ вирус могат да достигнат милиони или милиарди долари [27], [28].



Фиг. 7. Криптиран файл с разширение ".WNCRY"



Фиг. 8. Отворен текстов файл с име "@Please_Read_Me@"

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста. Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без

разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева." // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).

3. Заключение

Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), както и администраторът по сигурността трябва използват специални антивирусни програми.

Изследванията и анализите в този монографичен труд са реализирани с помощта на антивирусни програми, показващи добри резултати при откриване на злонамерени заплахи и уязвимости. Един от най-добрите институти за тестване на антивирусни програми е институтът AV-TEST. Щаб-квартирата на този институт се намира в град Магдебург, Германия [9], [10], [11], [13]. Този институт сравнява и тества всяка една антивирусна програма със следните показатели:

- Протекция.
- Производителност.
- Използваемост.

Протекцията се характеризира с това, че открива злонамерени инфекции като вируси, червеи и троянски коне. Протекцията включва още защита срещу кибератаките от "нулев ден". Тези кибератаки най-често се проявяват като уеб или e-mail заплаха [20], [21], [22], [23], [24], [25], [26].

Производителността се характеризира със средното влияние на антивирусната програма върху скоростта на компютърната система при делничните дни. Докато сканира антивирусната програма, компютърната система се натоварва с теглене на софтуер, инсталиране и изпълнение на програми, копиране на данни, както и посещение на уеб страници [11], [12], [17], [18], [19], [27], [28]. Използваемостта се характеризира с:

- Грешни предупреждения или блокировки при посещения на уеб страници.
- Разпознаване на легитимния софтуер като фалшива злонамерена програма.

Поради тази причина всички налични в момента на пазара платени и безплатни антивирусни програми са тестване от този независим институт [13], [14], [15], [16]. Тестваните антивирусни програми са:

- AhnLabAhnLab V3 Internet Security 9.0
- AvastAvast Free AntiVirus 17.5
- AVGAVG Internet Security 17.5
- AviraAvira Antivirus Pro 15.0
- BitdefenderBitdefender Internet Security 21.0 & 22.0
- BullGuardBullGuard Internet Security 17.1
- ComodoComodo Internet Security Premium 10.0
- ESETESET Internet Security 10.1
- F-SecureF-Secure Safe 14 & 17 certified
- G DataG Data InternetSecurity 25.4
- K7 ComputingK7 Computing Total Security 15.1
- Kaspersky LabKaspersky Lab Internet Security 17.0 & 18.0
- McAfeeMcAfee Internet Security 20.0
- MicrosoftMicrosoft Security Essentials 4.10
- MicroWorldMicroWorld eScan Internet Security Suite 14.0
- NortonNorton Norton Security 22.10
- ThreatTrackThreatTrack VIPRE Internet Security Pro 9.3
- Trend MicroTrend Micro Internet Security 11.1

References:

1. Ameen S. Y., Ahmed I. M., Design and Implementation of e-Laboratory for Information Security Training, IEEE Fourth International Conference on e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity", 2013, Manama, pp. 310 – 317.
2. Awad A. I., Hassanien A. E., Baba K., Advances in Security of Information and Communication Networks, First International Conference, SecNet 2013, Cairo, Egypt, September 3-5, 2013. Proceedings, Springer, 2013, ISBN 978-3-642-40596-9, pp. 260.
3. Bayuk J. L., Healey J., Rohmeyer P., Sachs M. H., Schmidt J., Weiss J., Cyber Security Policy Guidebook, John Wiley & Sons, 2012, ISBN: 978-1-118-02780-6, pp. 288.
4. Barry B. I., Chan H. A., Intrusion detection systems, Handbook of Information and Communication Security, Springer Berlin Heidelberg, ISBN: 978-3-642-04117-4, pp. 193 – 205.
5. Beale J., Foster J. C., Snort 2.0 Intrusion Detection, Syngress Publishing, 2003, ISBN: 1-931836-74-4, pp. 650.
6. Bejtlich R., The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013, ISBN-13: 978-1593275099, pp.376.
7. Boyanov P., Vulnerability penetration testing the computer and network resources of windows based operating systems, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, vol. 5, 2014, pp. 85 – 92.
8. Boyanov P. K., "A taxonomy of the cyber attacks", a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, Vol.3, 2013, pp. 114 – 124.
9. Boyanov P., Zhaneta T., "An unauthorized penetration into computer system with activated firewall and antivirus software", Anniversary Scientific International Conference 45 Years Computer Sciences and Engineering Department 30 Years Computer Systems and Technologies Speciality, 27-28 September, 2013, ISSN 1312-3335, Varna, Bulgaria, Section 1 Computer systems and Networks, pp.41 – 46.
10. Boyanov P. Kr., Finding a modern security approach and defence mechanism against various cyber-attacks, Proceedings of the 10th International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics (ICBBM 2014), Liepaya, Latvia, ISBN 978-9934-10-573-9, Volume 10, June 2-7, 2014, pp. 113 – 116.
11. Boyanov P., Using a specialized software for comprehensive monitoring the suspicious states in computer networks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, vol. 6, 2014, pp. 148 – 154.
12. Boyanov P., Analysis and assessment the security vulnerability in communication processes in a given computer network, JOURNAL SCIENCE EDUCATION INNOVATION, ISSN 1314-9784, VOL. 2. 2014, pp. 39 – 44.
13. Boyanov P., Building Secure mechanisms with the software program Avast Free Antivirus, JOURNAL SCIENCE EDUCATION INNOVATION, ISSN 1314-9784, vol.3, 64-71.
14. Blunden B., The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System 2nd Edition, Jones & Bartlett Learning; 2 edition, 2012, ISBN-13: 978-1449626365, pp. 784.
15. Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal With Impact Factor, Issue 36, August 2017, ISSN 2367-5721, www.sociobrains.com.
16. Dimanova D, Kuzmanov Z, "Measuring and assessing risk". International Scientific Refereed Online Journal With Impact Factor, Issue 32, april 2017, ISSN 2367-5721, www.sociobrains.com.
17. Myers C., Powers S., Faissol D., Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. Lawrence Livermore National Laboratory, April 2009, vol.7, pp. 1 – 22.

18. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Informatsionnые tehnologii i bezopasnosty, Zhurnal Akad. nauk Ukrainы., Spets. vыpusk, Kiev, 2013, Str. 79-86
19. Nasr K., El Kalam A. A., and Fraboul., Generating Representative Attack Test Cases for Evaluating and Testing Wireless Intrusion Detection Systems, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012, pp. 1 – 19.
20. Oram A., Viega J., Beautiful Security, O'Reilly Media, 2009, ISBN: 978-0-596-52748-8, pp. 302.
21. Perla E., Oldani M., A guide to kernel exploitation: attacking the core, Syngress Elsevier, ISBN 978-1-59749-486-1, 2011, p. 465.
22. Prowell S., Kraus R., Borkin M., Seven Deadliest Network Attacks, Syngress Elsevier, ISBN: 978-1-59749-549-3, 2010, p. 145.
23. Sharma A., Kalbarczyk Z., Iyer R., Barlow J., Analysis of credential stealing attacks in an open networked environment, In Proc. of the Fourth International Conference on Network and System Security. Washington, 2010, DC, USA: IEEE Computer Society, pp. 144 – 151.
24. Simmons C., Shiva S., Dasgupta D., Wu Q., AVOIDIT: A cyber attack taxonomy, University of Memphis, Proceedings of the 9th Annual Symposium on Information Assurance (ASIA '14), Albany, NY, USA, June 3-4, 2014, pp. 1 – 12.
25. Stanev S, Hristov H, Dimanova D, "Aproaches for stego defense of sensitive information", Proceedings of the 10th International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics (ICBBM 2014), Liepaya, Latvia, ISBN 978-9934-10-573-9, Volume 10, June 2 - 7, 2014, pp. 117 – 122.
26. Stanev St., Szczypiorski Krzysztof., Steganography Training: a Case Study from University of Shumen in Bulgaria, Intl Journal Of Electronics And Telecommunications, 2016, Vol. 62, No. 3, Pp. 315-318, Manuscript received September 7, 2016; revised September, 2016, DOI: 10.1515/eletel-2016-0043.
27. Tasheva, Z. N., Tasheva, A. T. Combining cryptography and steganography in software system for hiding confidential information, International Journal of Science, Education and Innovation, Volume 1, 2013. ISSN 1314-9784, Association Scientific and Applied Research, pp. 84-92.
28. Zhelezov St. K., Paraskevov Hr. Iv., Hristov Hr. At., Boyanov P. Kr., Uzunova B. Hr., An architecture of steganological subsystem for information protection, Proceedings of the 10th International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics (ICBBM 2014), Liepaya, Latvia, ISBN 978-9934-10-573-9, Volume 10, June 2-7, 2014, pp. 123 – 128.