ХАРАКТЕРИСТИКА НА СЪВРЕМЕННИТЕ ВИДОВЕ ШПИОНСКИ ИНФОРМАЦИОННИ ПРОГРАМИ

Христо ХРИСТОВ*

In this paper a characteristic of the modern types of spyware information programs is made.

Въведение

Информационните системни кибератаки представляват съвкупност от специални злонамерени софтуерни програми, които се използват за осигуряване на неоторизиран достъп до ресурсите на машината жертва на служителя от държавната или частната организация [1; 2: 249 – 259; 3: 36 – 47; 5: 414; 7: 34 – 41; 8: 114 – 124].

Успешното извършване на определена кибератака към машината жертва на служителя от дадена организация е свързано с изпълнението на основните фази на кибератаките.

Кибератаки, записващи всеки натиснат клавиш от клавиатурата (keylogger)

Тези кибератаки се разделят главно на хардуерни шпионски инструменти и устройства и софтуерни шпионски програми [1; 2: 249 – 259; 3: 36 – 47; 4: 178 – 183; 7: 34 – 41; 9: 18 – 23]. Хардуерните шпионски инструменти, които се използват от киберпрестъпниците, са устройства, вградени в дънната платка или BIOS-а на компютърната машина, клавиатура, в която има вградени електронни платки за записване на всеки натиснат клавиш, Bluetooth

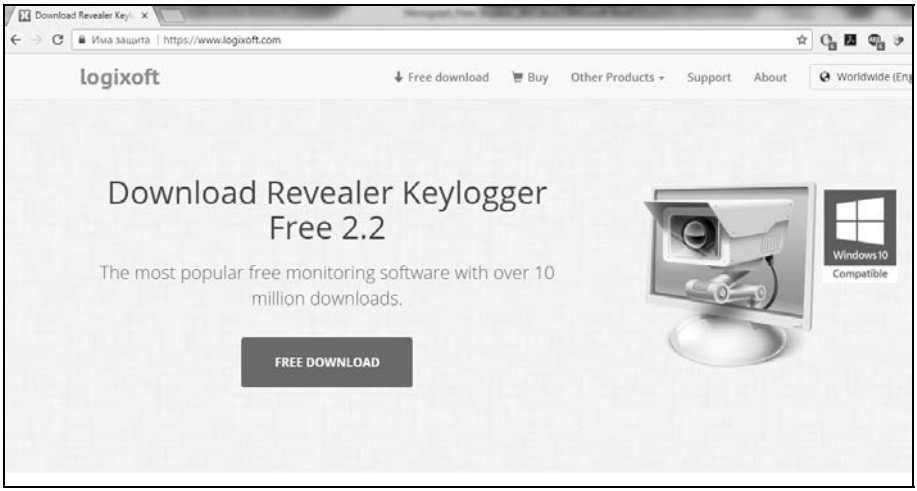
* Авторът е доцент, доктор, инженер в Шуменски университет „Епископ Константин Преславски“.

кийлогър, Wi-Fi кийлогър, USB флаш кийлогър, VGA, HDMI, DVI кийлогър и др.

Трябва да се знае, че софтуерните програми, записващи всеки натиснат клавиш от клавиатурата, записват още всички текущи съобщения, заснемат снимки (скрийншотове), следят използването на ресурсите на машината жертва за всяка стартирана програма, изпращат отчети със записаните данни по електронната поща, отдалечено управление и споделени сървъри с файлове (FTP), записват звуците от микрофона, генерират уеб-HTML отчети, управляват, наблюдават потребителските акаунти и спират работата на софтуерни програми, които имат задача да намерят програми, които записват всеки натиснат клавиш [6: 465; 10: 58 – 64; 11: 1 – 22, 1 – 52; 14: 302; 15: 13 – 21].

На *Фигура 1* е показана официалната уебстраница на един от използваните кийлогъри (Keylogger).

Фигура 1. ***Официален уебсайт на програмата Revealer Keylogger***



КИБЕРАТАКИ, ИЗПОЛЗВАЩИ ШПИОНСКИ ПРОГРАМИ ОТ ТИПА „SPYWARE“

Злонамерените извършители [1; 2: 249 – 259; 3: 36 – 47; 7: 34 – 41; 14: 302; 15: 13 – 21; 16: 359] използват уязвимости в уеббраузърите, като Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari и др., с цел инсталирането на агент, който да следи всички

дейности на машината жертва на служителя от организацията. След инсталирането на специалните злонамерени софтуерни агенти без знанието на служителя от организацията всички записани данни се предават през интернет до машината на киберпрестъпника. Тези кибератаки се разделят на:

- мултимедийни кибератаки на звук и видео;
- кибератаки на работния плот на операционната система;
- кибератаки, използващи глобалната система за позициониране GPS;
- кибератаки, използващи буфера на принтера;
- кибератаки, използващи буфера на факса;
- кибератаки, използващи флаш памети;
- кибератаки, използващи клавиша за заснемане на текущото състояние на прозореца;
- кибератаки, използващи уязвимости в съвременните смарт телефони.

Спайуерът (Spyware) представлява компютърна софтуерна наблюдаваща програма, която се инсталира като скрит допълнителен компонент наред с безплатна или платена програма, която е изтеглена от интернет. Тъй като повечето програми изискват администраторски права за инсталация, тогава скритото инсталиране на такъв шпиониращ софтуер остава незабелязано от служителя във фирмата или организацията. След това откриване на този шпиониращ софтуер е почти невъзможно, защото злонамереният софтуер се маскира под определен системен процес като svchost.exe в операционната система Microsoft Windows. Вредите, които може да последват след инсталирането на такъв шпиониращ софтуер в машината на служителя, са [1; 2: 249 – 259; 3: 36 – 47; 6: 465; 7: 34 – 41; 11: 1 – 22, 1 – 52; 12: 1 – 22; 13]:

- постоянно наблюдение на цялата онлайн уебактивност в интернет;
- откradване на потребителски имена и пароли на служителите и изпращането им след това на отдалечен сървър на киберпрестъпника;
- намаляване на производителността и бързината на операционната система;
- автоматично пренасочване на уеббраузъра към порнографски сайтове;

• поставяне на преки пътища на работния плот на различни злонамерени и шпиониращи уебсайтове;

• намаляване на политиките на системната сигурност на операционната система;

• пренасочване към уебстраници, съдържащи нежелани реклами и продукти;

• изключване на защитната стена;

• намаляване на бързодействието на уеббраузъра с цел много бавно зареждане на всяка една уебстраница.

Кибератаки, използващи шпионски програми от типа „Rootkit“

Руткитът **(Rootkit)** представлява програма, която се използва за придобиване на администраторски права за Windows базирани операционни системи или суперпотребителски права за Linux базирани операционни системи, без да бъдат забелязани и открити от антивирусните програми. Тези злонамерени програми се закачват или обвиват в специални софтуерни пакети за компютърни игри. След като киберпрестъпникът инсталира тези злонамерени програми, тогава той ще може да управлява всички ресурси на операционната система чрез отдалечен достъп с агент, тип „Задна врата“, да изтрива всички свои направени следи, да компрометира и замаскира злонамерените процеси като нормални системни процеси от операционната система, да събира и анализира конфиденциална информация, използвана от служителя на организацията. Тези кибератаки се разделят на [1; 2: 249 – 259; 3: 36 – 47; 13; 14: 302; 15: 13 – 21; 16: 359; 17: 1 – 22]:

• кибератаки, използващи твърдо кодиран код в хардуера;

• кибератаки, използващи ядрото на операционната система [7: 34 – 41];

• кибератаки, използващи приложни софтуерни програми;

• кибератаки, използващи инициализиращата програма (Boot Loader) за зареждане на операционната система.

Едни от най-известните шпионски програми от типа „Rootkit“ са Fu за операционна система Windows, KBeast за операционна система Linux, Hacker Defender (hxdef) и др.

Друг начин шпионските програми от типа „Rootkit“ да бъдат прикачени към даден изпълним или неизпълним файл е използването на Alternate Data Streams (ADS). Алтернативните потоци от

данни служат за допълнително описание на даден файл от операционната система. Например, ако даден служител от организацията реши да добави още съдържание към даден текстов файл, тогава се използват алтернативните потоци от данни. По този начин киберпрестъпникът може да добави злонамерен файл или код към даден текстов файл и след това да го изпрати на машината на служителя [2: 249 – 259; 3: 36 – 47]. След отварянето на този файл от служителя киберизвършителят ще получи неоторизиран достъп до машината на своята жертва. Едни от програмите за извършване на манипулации с файлове са NTFS-Streams ADS manipulation tool и GMER.

Кибератаки с „Троянски кон“ или „Задна врата“

Тези „Троянски коне“ или „Задни врати“ са синонимни компютърни понятия и представляват софтуерни програми, съдържащи вреден код, вкаран в изпълним файл с разширение, завършващо на „exe“, „bat“, „com“, „vbs“, „pl“, „rar“, „zip“ или др. „Троянските коне“ се активират единствено след стартиране на даден изпълним файл, незнайно или знайно от служителя в организацията. Целта на тези кибератаки е да изтрият или заменят критични файлове на операционната система на служителя от фирмата или компанията, да създадат задна врата, играеща ролята на агент за отдалечен достъп до машината жертва, да записват аудио- и видеоинформация за служителя, да инсталират допълнително софтуерни шпионски програми, да използват компютърната машина на служителя като робот (зомби), който да извършва разпределени атаки с отказ на услуги Distributed Denial of Service (DDoS) [1; 2: 249 – 259; 3: 36 – 47; 6: 465; 7: 34 – 41; 10: 58 – 64; 11: 1 – 22; 12: 1 – 22; 17: 1 – 12] към други машини жертви, да използват жертвата за изпращане на фалшиви електронни съобщения, да блокират работата на защитните стени и антивирусните програми и др.

Забележка: *Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки, катедра „Управление на системите за сигурност“ при Шуменския университет „Епископ Константин Преславски“. Всичко илюстрирано и обяснено в тази статия е с научноизследователска 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.).

Заключение

Служителите по сигурността на автоматизираните информационни системи и мрежи АИС/М, както и администраторът по сигурността, трябва да предприемат и направят следните защитни действия:

- откриване на алтернативните потоци от данни (ADS), съдържащи злонамерен код;
- премахване на шпионски програми от типа „Spyware“ чрез използване на специални софтуерни програми;
- прилагане на строги правила за разпознаване на фалшивите електронни писма от страна на служителите в организацията;
- винаги след приключване на работния ден служителят е длъжен да заключи вратата на своя кабинет;
- служителят и системният администратор трябва да проверяват редовно компютърните машини с цел откриване на прикрепени устройства към клавиатурата на компютъра;
- на всеки 20 дена да се сменят потребителските имена и пароли на служителите в организацията;
- да се използват отново скенери за откриване на аномалии и уязвимости на компютърните машини на служителите;
- задължително сканиране на всеки свален файл от интернет с антивирусна програма;
- използване на виртуална софтуерна клавиатура от операционната система с цел избягване на програми, които следят всеки натиснат клавиш от клавиатурата;
- редовно сканиране за съмнителни и злонамерени файлове и директории с антивирусна програма;
- редовно сканиране за злонамерени програми, които се стартират със самата операционна система на служителя;
- редовно сканиране за съмнителни мрежови действия и активности.

Литература

1. **Боянов,** П. Кибератаки и противодействие. Монография. Шумен: Епископ Константин Преславски, 2017, 210 с. ISBN 978-619-201-206-9.

2. **Савов,** И. Относно някои аспекти от процедурите по използване на трафичните данни в Република България и някои европейски страни. – В: *Международна* конференция „Противодействие на радикализацията и тероризма“, Академия на МВР, април 2017 г. ISBN 978-954-348-145-3.

3. **Савов,** И. Един поглед върху същността на киберпрестъпленията. – В: *Политика* и сигурност, ВУСИ, 2017. ISSN 2535-0358.

4. **Ташева,** Ж. Н., П. Кр. Боянов. Сравнителен анализ на злонамерени уеббазирани атаки. – В: *Научна* конференция на тема „Защитата на личните данни в контекста на информационната сигурност“. Факултет „Артилерия, ПВО и КИС“ при Националния военен университет „Васил Левски“, Шумен, 6 – 7 юни 2013. ISBN 978-954-9681-49-9.

5. **Allen,** L. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Birmingham, UK: Packt Publishing, 2012. ISBN 978-1-84951-774-4.

6. **Bodmer,** S., M. Kilger, Gr. Carpenter, J. Jones. Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw-Hill Education, 2012. ISBN 978-0-07-177250-1.

7. **Boyanov,** P. Educational exploiting the information resources and invading the security mechanisms of the operating system Windows 7 with the exploit Eternalblue and Backdoor Doublepulsar. – In: *Scientific* and Applied Research, Konstantin Preslavsky University Press, Vol. 14, 2018. ISSN 1314-6289. [online]. *http://www.rst-tto.com/publication.html.*

8. **Boyanov,** P. A taxonomy of the cyber attacks. – In: *Scientific* and Applied Research, Konstantin Preslavsky University Press, Vol. 3, 2013. ISSN 1314-6289. [online]. *http://www.rst-tto.com/publication.html.*

9. **Kahya-Özyirmidokuz,** E., A. Gezer, C. Ciflikli. Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application. – In: *Data* Analytics, The First International Conference on Data Analytics, September, 2012. ISBN 978-1-61208-242-4.

10. **Kaur,** R., G. Singh. Analysing, Port Scanning Tools and Security Techniques. – In: *International* Journal of Electrical Electronics & Computer Science Engineering, Vol. 1, Issue 5, October 2014. ISSN 2348 2273.

11. **Meyers,** C., S. Powers, D. Faissol. Probabilistic Characterization of Adversary Behavior in Cyber Security. No. LLNL-TR-419023. – In: *Lawrence* Livermore National Laboratory (LLNL), Livermore, CA, 2009.

12. **Meyers,** C., S. Powers, D. Faissol. Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. – In: *Lawrence* Livermore National Laboratory, April 2009, Vol. 7.

13. **Nachev,** A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. – In: *Information* Technology and Security, No. 1(3), 2013.

14. **Oram,** A., J. Viega. Beautiful Security. – In: *O'Reilly* Media, 2009. ISBN 978-0-596-52748-8.

15. **Savov,** I. The collision of national Security and Privacy in the age of information technologies. – In: *European* Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017. ISSN 2443-7883.

16. **Shimeall,** T. J., J. M. Spring. Introduction to Information Security: A Strategic-Based Approach. Syngress, 2014. ISBN 978-1-59749-969-9.

17. **Simmons,** C., S. Shiva, D. Dasgupta, Q. Wu. AVOIDIT: A cyber attack taxonomy. University of Memphis. – In: *Proceedings* of the 9th Annual Symposium on Information Assurance (ASIA '14), Albany, NY, USA, June 3 – 4, 2014.