5. Salam Khanji, Farkhund Iqbal, Raja Jabir, Andrew Marrington. Forensic analysis of Xbox one and Playstation 4 gaming consoles. URL: https://www.researchgate.net/publication/312560894_Forensic_analysis_of_xbox_one_and_playstation_4_gaming_consoles (дата звернення: 09.10.2018).

6. Sasa Mrdovic, Alvin Huseinovic, Ernedin Zajko. Combining Static and Live Digital Forensic Analysis in Virtual Environment. URL: http://people.etf.unsa.ba/~smrdovic/publications/ICAT2009-Mrdovic_Huseinovic_Zajko.pdf (дата звернення: 10.10.2018).

7. Matthew Davies, Huw Read, Konstantinos Xynos, Iain Sutherland. Forensic analysis of a Sony PlayStation 4: A first look. URL: https://www.researchgate.net/publication/273261827_Forensic_analysis_of_a_Sony_PlayStation_4_A_first_look (дата звернення:11.10.2018).

Одержано 22.10.2018

УДК 004.492.3

Богдан Володимирович ЛИТВИНЕНКО,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»;
Михайло Віталійович ЦУРАНОВ,
старший викладач кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

МОНІТОРИНГ КОМП'ЮТЕРНИХ МЕРЕЖ ЯК ЗАСІБ ВИЯВЛЕННЯ КІБЕРЗЛОЧИНЦІВ

Останнім часом масштабні кіберзлочини на території України стали досить частим явищем. Як повідомив начальник кіберполіції Сергій Демедюк в інтерв'ю виданню «Економічна правда» в січні 2018 року, в Україні кількість виявлених злочинів у сфері кібербезпеки збільшується в середньому на 2,5 тисячі щорічно[1], що свідчить не тільки про зростання їх кількості, але й про збільшення ефективності роботи підрозділів кіберполіції з фіксації злочинів. Об'єктами зловмисників все частіше стають державні установи, акаунти держслужбовців у різних соціальних мережах.

До найбільших кібератак за останні 5 років можна віднести:

1) грудень 2015 року – кібератака віруса BlackEnergy на «Укренерго», в результаті чого в Прикарпатті, Київській та Чернівецькій областях без електроенергії залишились близько 220 тис. споживачів[2]. В результаті розслідування було виявлено, що атака почалась ще у травні 2014 року з розсилки на поштові скриньки робітників електронного листа, який містив файл з троянською програмою, що збирала інформацію про систему та відправляла її зловмисникам. З червня 2014 по жовтень 2015 року продовжились розсилки і 23 грудня 2015 року зловмисниками була проведена скоординована кібератака на інфраструктуру українських обленерго. Після внесення змін до режиму роботи розподільчих станцій програма

за допомогою модуля KillDisk знищувала файли в зараженій системі. В січні 2016 року була здійснена нова розсилка по підприємствам, що мають відношення до енергетики України, але тепер поширювався Excel-документ нібито з внутрішньою інформацією по Укренерго[3];

2) березень 2016 року – атака трояна-шифрувальника під назвою Petya[4]. Розповсюджувалась програма за допомогою спам-розсилки до HR-менеджерів «прикидаючись» листом з резюме, наприклад, «Резюме Senior Java Developer». Лист містив гіперпосилання на сервіс зберігання даних Dropbox. При подальшому переході за посиланням, зловмисна програма ініціювала перезавантаження комп'ютера, вносячи зміни в операційну систему. Програма блокувала доступ до операційної системи [5];

3) травень 2017 року – масова кібератака вірусу WannaCry, що заблокував не менше 200 тис. комп'ютерів в 150 країнах світу, в тому числі й в Україні[6]. Українці отримували електронні листи нібито від «Приват Банку» та інших відомих українських компаній, після відкриття яких, на комп'ютер встановлюється програма-блокувальник [7]. Вірус-вимагач, блокував комп'ютер і вимагав суму в $300 в біткоінах. Якщо протягом трьох днів оплата не відбувалась, ціна викупу подвоювалась, а через 7 днів від початку зараження без виплати викупу всі файли видалялись [8];

4) жовтень 2018 року – кібератака типу відмова в обслуговуванні на Державну фіскальну службу України, а саме на «Електронний кабінет» та «Офіційний веб-портал ДФС України» [9].

Атаки, перелічені вище, були успішними, бо потрапляючи на комп'ютер через мережу Інтернет, розповсюджувались через корпоративні мережі. Мінімізувати наслідки чи запобігти зараженню зловмисною програмою можна було б використовуючи програмні чи апаратні засоби забезпечення кібербезпеки. Щоб вберегтись від сучасних мережевих загроз недостатньо використовувати лише традиційні засоби захисту як, наприклад, антивірусні програми чи брандмауери. Для вирішення проблеми використовуються системи виявлення вторгнень (IDS) або системи запобігання вторгнень (IPS). IDS/IPS часто виступає як наступний рівень безпеки після обминання зловмисником брандмауеру. Системи виявлення вторгнень в залежності від виконуваних функцій підрозділяються на [10]:

1. Пасивні IDS – програмне (або апаратне) забезпечення, призначене для виявлення фактів несанкціонованого доступу в комп'ютерну систему чи мережу або несанкціонованого управління ними.

2. Активні IDS (частіше їх називають IPS) – програмне (або апаратне) забезпечення, призначене для забезпечення системної чи мережевої безпеки шляхом виявлення вторгнень чи порушень безпеки і автоматичного їх усунення.

Найчастіше системи типу IPS використовуються системними адміністраторами для захисту найбільш критичних систем, в яких

необхідно в режимі реального часу реагувати на вторгнення. Системи типу IDS використовуються для моніторингу вторгнень в менш критичних системах.

IDS/IPS-системи можуть відрізнятися також за місцем проведення моніторингу: комп'ютер чи корпоративна мережа. Отже можна виділити 2 види IDS/IPS-систем[11]:

1. Host-based (HIDS/HIPS) – виявляють атаки, що направлені на конкретний вузол мережі, аналізують роботу операційної системи для виявлення вторгнень.

2. Network-based (NIDS/NIPS) – виявляють атаки, що направлені на сегмент мережі чи мережу взагалі, аналізують мережеві пакети.

В залежності від способу роботи IDS/IPS-системи можна розділити на [11]:

1. Статичні IDS/IPS-системи – роблять так звані «знімки» (англ. – «snapshot») системи та аналізують їх, шукаючи помилки в конфігураціях системи тощо.

2. Динамічні IDS/IPS-системи – виконують моніторинг в режимі реального часу всіх дій в системі, перевіряють системні файли та мережеві пакети за певний проміжок часу.

Загальна кількість кібератак на території України є настільки великою, що використання засобів захисту інформації в системах та мережах є не рекомендованим, а навіть обов'язковим для нормального функціонування країни. Саме тому дуже важливо звернути увагу на системи виявлення/запобігання вторгнень, що представляють собою потужний інструмент моніторингу мережі, оповіщення про несанкціоновані зловмисні дії та якнайшвидшого усунення атак. Виходячи з реалій побудови обчислювальних мереж, в державному та корпоративному секторі, найбільш доцільно використовувати апаратні IDS/IPS-системи розташовані на центральному комунікаційному шлюзі або в межах ДМЗ.

Список бібліографічних посилань

1. Кількість кіберзлочинів в Україні збільшується на 2,5 тисячі на рік. URL: https://dt.ua/UKRAINE/kilkist-kiberzlochiniv-v-ukrayini-zbilshuyetsya-na-2-5-tisyachi-na-rik-266179_.html (дата звернення: 08.10.2018).

2. Как происходила атака на украинские электростанции – расследование Wired. URL: https://ain.ua/2016/03/07/kak-proisxodila-ataka-na-ukrainskie-elektrostancii-rassledovanie-wired/ (дата звернення: 08.10.2018).

3. Расследование кибератаки на Украину: как вирус сломал облэнерго. URL: https://biz.liga.net/all/it/article/rassledovanie-kiber-ataki-na-ukrainu-kak-virus-slomal-oblenergo (дата звернення: 09.10.2018).

4. Ransom.Petya // Symantec Security Center. URL: https://www.symantec.com/security-center/writeup/2016-032913-4222-99 (дата звернення: 10.10.2018).

5. Компьютеры украинцев атаковал вымогатель Petya. URL: https://www.rbc.ua/rus/lnews/kompyutery-ukraintsev-atakoval-vymogatel-1462889440.html (дата звернення: 10.10.2018).

6. Украинцев предупредили об атаке вируса WannaCry. URL: https://korrespondent.net/ukraine/3851006-ukrayntsev-predupredyly-ob-atake-vyrusa-WannaCry (дата звернення: 11.10.2018).

7. Украинцев накрыл спам с вирусами от поддельного «ПриватБанка». Сколько это могло стоить. URL: https://ain.ua/2017/03/03/ukraincy-poluchili-spam-s-virusami-ot-poddelnogo-privatbanka/ (дата звернення: 11.10.2018).

8. Массовая кибератака затронула 74 страны, заражены тысячи компьютеров. Но вы сами в этом виноваты. URL: https://ain.ua/2017/05/13/massovaya-kiberataka-zatronula-74-strany-zarazheny-tysyachi-kompyuterov-no-vy-sami-v-etom-vinovaty/ (дата звернення: 11.10.2018).

9. Державна фіскальна служба заявляє про кібератаки на свої ресурси. URL: https://www.radiosvoboda.org/a/news-dfs-kiberataka/29534547.html (дата звернення: 09.10.2018).

10. Бирюков А. А. Информационная безопасность. Защита и нападение. М. : ДМК Пресс, 2017. 434 с.

11. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). М. : Гор. линия-Телеком, 2013. 220 с.

Одержано 16.10.2018

УДК 343.98

Олександр Олександрович МОЖАЄВ,
доктор технічних наук, професор,
професор кафедри інформаційних технологій факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-1412-2696;
Михайло Олександрович МОЖАЄВ,
кандидат технічних наук,
завідувач лабораторії комп'ютерно-технічних, телекомунікаційних
досліджень та досліджень відео-, звукозапису
Харківського НДІ судових експертиз ім. Засл. проф. М. С. Бокаріуса;
Михайло Олександрович ЛОГВИНЕНКО,
завідувач сектору лабораторії комп'ютерно-технічних, телекомунікаційних
досліджень та досліджень відео-, звукозапису
Харківського НДІ судових експертиз ім. Засл. проф. М. С. Бокаріуса
Сергій В'ячеславович ЧОРНИЙ,
кандидат технічних наук, доцент,
провідний науковий співробітник лабораторії комп'ютерно-технічних,
телекомунікаційних досліджень та досліджень відео-, звукозапису
Харківського НДІ судових експертиз ім. Засл. проф. М. С. Бокаріуса

АВТОМАТИЗОВАНА СИСТЕМА НАКОПИЧЕННЯ ЕМПІРИЧНИХ ДАНИХ У СФЕРІ КОМП'ЮТЕРНО-ТЕХНІЧНИХ ЕКСПЕРТИЗ

Комп'ютерно-технічна та телекомунікаційна судові експертизи мають особливості, що важко піддаються документуванню засобами класичного збереження офіційної інформації. Така ситуація зумовлена надто великим зростанням кількості та різноманітності пристроїв на світовому ринку, що можуть зберігати цифрову інформацію свого власника чи будь-яку іншу.

Враховуючи наведене вище, судово-експерта система потребує динамічної, швидко наповняємої, простої в експлуатації та легкодоступної системи, здатної накопичувати зазначену вище інформацію у великих обсягах та надавати доступ до неї. Враховуючи