Технічні науки

УДК 004.491+343.148.6

Колесник Віталій Геннадійович
завідувач відділу комп'ютерно-технічних
та телекомунікаційних досліджень
Харківський науково-дослідний
експертно-криміналістичний центр МВС України
Колесник Виталий Геннадьевич
заведующий отделом компьютерно-технических
и телекоммуникационных исследований
Харьковский научно-исследовательский
экспертно-криминалистический центр МВД Украины
Kolesnyk Vitalii
Head of the Department of Computer and Telecommunication Studies
Kharkiv Scientific Research Forensic Center of the
Ministry of Internal Affairs of Ukraine

Пилипенко Олександр Вадимович
судовий експерт відділу
комп'ютерно-технічних та телекомунікаційних досліджень
Харківський науково-дослідний
експертно-криміналістичний центр МВС України
Пилипенко Александр Вадимович
судебный эксперт отдела компьютерно-технических и
телекоммуникационных исследований
Харьковский научно-исследовательский
экспертно-криминалистический центр МВД Украины

Pilipenko Oleksandr
Forensic Expert of the Department of Computer and Telecommunication Studies
Kharkiv Scientific Research Forensic Center of the
Ministry of Internal Affairs of Ukraine

ОСОБЛИВОСТІ ДОСЛІДЖЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА СЛІДІВ ВІДДАЛЕНОГО ВТРУЧАННЯ В РОБОТУ КОМП'ЮТЕРНОЇ СИСТЕМИ
ОСОБЕННОСТИ ИССЛЕДОВАНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СЛЕДОВ УДАЛЁННОГО ВМЕШАТЕЛЬСТВА В РАБОТУ КОМПЬЮТЕРНОЙ СИСТЕМЫ
FEATURES OF INVESTIGATION OF MALICIOUS SOFTWARE AND TRACES OF REMOTE CONNECTIONS TO COMPUTER SYSTEM

Анотація. *У статті розглянуто практичні аспекти дослідження шкідливого програмного забезпечення та виявлення слідів віддаленого втручання в роботу комп'ютерної системи.*

Ключові слова: *комп'ютерно-технічна експертиза, шкідливе програмне забезпечення, несанкціоноване втручання в роботу системи.*

Аннотация. *В статье рассмотрены практические аспекты исследования вредоносного программного обеспечения и выявления следов удалённого вмешательства в работу компьютерной системы.*

Ключевые слова: *компьютерно-техническая экспертиза, вредоносное программное обеспечение, несанкционированное вмешательство в работу системы*

Summary. *The article discusses the practical aspects of researching malicious software and identifying traces of unauthorized access to computer system.*

Key words: *computer forensics, malicious software, malware, unauthorized access to system.*

На сьогоднішній день, у зв'язку з активним розвитком інформаційних технологій, комп'ютерів, комп'ютерних мереж, мобільних пристроїв все більше людей використовують мережеві технології, зокрема мережу Інтернет у своїй повсякденній діяльності. В умовах сьогодення, сучасна людина постійно користується онлайновими послугами, такими як, наприклад, банківські послуги, замовлення та придбання товарів, керування фінансами та активами, відправлення фінансової звітності, користується електронною поштою, спілкується у онлайн-конференціях, месенджерах. В діяльності державних та приватних установ, організацій та підприємств все зазвичай організовано за допомогою персональних комп'ютерів та комп'ютерних мереж [1]. Ми можемо констатувати, що діджиталізація світу та суспільства є очевидним та вираженим процесом, що відбувається в умовах прогресу, та є невід'ємною часткою розвитку нашої цивілізації.

Очевидно, що такі процеси не могли не привернути увагу сучасних злочинців, які одразу почали використовувати для своїх злочинних дій цей зовсім новий простір – кіберпростір. Світова мережа та її можливості були швидко пристосовані для розповсюдження шкідливого програмного забезпечення (далі – ШПЗ), торгівлі наркотиками, розповсюдження порнографії, викрадення особистих даних про особу та торгівлі ними, атак з метою втручання в роботу фінансових та виборчих установ, кібершпигунства, кіберпропаганди та кібертероризму.

Методи кібератак постійно розвиваються, стають все більш різноманітними та витонченими. Деякі кіберінциденти, особливо пов'язані з політичними та виборчими процесами, обороною, є настільки суттєвими, що мають вплив на геополітичний імідж держави, її економіку та обороноздатність. Фінансові відомості, відомості про рухоме та нерухоме майно громадян, їх особисті дані та електронні платіжні засоби все частіше стають ціллю різноманітних кібератак.

Якісне розслідування кіберінцидентів що трапляються, потребує особливого слідчого огляду та фіксації, оскільки спеціаліст (криміналіст) загальної кваліфікації не володіє спеціальними знаннями, необхідними для виконання дій з комп'ютерною інформацією (яка у подальшому стане електронним доказом) та не може використати всі методи та засоби, необхідні для її якісної фіксації [2]. Про це дуже важливо пам'ятати, але темою даної статті є особливості дослідження ШПЗ та фактів втручання до комп'ютерної системи вже на етапі експертного дослідження, тобто, коли ця інформація вже зібрана та надана судовому експерту. Зазвичай, зараження комп'ютерної системи ШПЗ ставить на меті та передує подальшому несанкціонованому втручанню до неї, тому ці процеси часто взаємопов'язані.

Отже, перейдемо до формування загальних етапів [3], на які пропонується умовно розділити процес дослідження:

1. Дослідження загальних характеристик об'єкта.
2. Виявлення шкідливого програмного забезпечення у системі.
3. Виявлення та дослідження шляхів його потрапляння до системи та слідів діяльності.
4. Дослідження функцій виявленого ШПЗ.
5. Виявлення ознак віддаленого керування.
6. Формування висновку.

Зупинимося докладніше на кожному із зазначених етапів.

Дослідження загальних характеристик об'єкта. На даному етапі експертом досліджується наданий об'єкт (електронний носій), створюється файл-образ, підраховується контрольна сума інформації. Всі подальші етапи дослідження експерт виконує вже у вмісті створеного файлу-образа, на даному етапі визначаються відомості про файлові системи носія, операційну систему, облікові записи користувачів, налаштування часу та часового поясу.

Виявлення шкідливого програмного забезпечення у системі. Перед проведенням етапу виявлення рекомендується провести пошук видалених даних, опрацювання та індексацію файлу образу. На даному етапі експертом здійснюється:

1. Перевірка інформації на досліджуваному носії шляхом сканування антивірусними програмними засобами з останніми актуальними оновленнями. Кожне спрацьовування антивірусного засобу з виявленням ШПЗ фіксується та у подальшому перевіряється вручну, шляхом дослідження каталогів у яких виявлені файли, що викликали спрацьовування антивірусного ПЗ. Слід особливо звернути увагу що, відсутність фактів виявлення ШПЗ антивірусною програмою не означає що система не була вражена – ШПЗ може бути унікальним, професійно створеним чи видозміненим та не визначатиметься сканером антивірусу, або просто бути вже видаленим на момент проведення дослідження.

2. Пошук, візуальний аналіз та перевірка каталогів за найбільш типовими шляхами, за якими найчастіше розташовуються файли ШПЗ після враження: C:/Windows/; C:/ProgramData/; C:/Users/%username%/ - каталог користувача та його підкаталоги: /AppData/Local/Temp/, /Desktop/(робочий стіл користувача), /Documents/ (документи), /Downloads/ (Загрузки); C:\ProgramData\Microsoft\Windows\StartMenu\Programs\Startup\; C:\Users\%username%\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\.

Також слід звернути увагу на встановлене на досліджуваній системі антивірусне програмне забезпечення та перевірити його журнали та каталог «карантину», оскільки дуже часто вже після інциденту, але до призначення дослідження, власник системи оновлює антивірусне ПЗ чи встановлює нове, яке в результаті перевірки виявляє файли ШПЗ та видаляє їх, значно ускладнюючи тим самим подальше дослідження.

3. Пошук, візуальний перегляд та перевірка кущів системного реєстру, які відповідають за автозавантаження, служби та контекстне меню:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute\
HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)\
HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions\
HKLM\System\CurrentControlSet\Services\
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers\
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers\
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers\

4. Перевірка бібліотеки запланованих завдань у Планувальнику завдань Windows (Task Sheduler) на наявність в них завдань на запуск підозрілих виконуваних файлів.

Виявлення та дослідження шляхів потрапляння до системи та слідів діяльності. Після виконання попереднього етапу та у разі виявлення файлів, експерт має:

1. Провести дослідження каталогів де вони буди виявлені, зафіксувати атрибути часу, оглянути інші файли що в них розташовані, перевірити наявність недавно видалених файлів у цих каталогах. Особливу

увагу слід звертати на файли типів .exe, .bat, .com, .scr, .vbs, .reg, .js, .rar, .zip.

У разі виявлення графічних файлів знімків екрану або журналів кейлоггера (прихований засіб для перехоплення та записування натискань клавіш клавіатури) необхідно провести їх окреме дослідження, аналіз атрибутів та опис у висновку.

2. Провести аудит журналів подій операційної системи (файли .EVT та .EVTX в каталогах %SystemRoot%\System32\Config\; %SystemRoot%\System32\winevt\Logs\), у журналах Application.evtx, Security.evtx, System.evtx зберігається багато важливих записів щодо подій що відбувалися у системі: часи вмикання/вимикання, запити програмних продуктів на ескалацію (підвищення) привілеїв, активність облікових записів, критичні помилки.

Вищевказані журнали та спеціальні журнали подій операційних систем (що маються у системах, новіших за Microsoft Windows 7): «Microsoft-Windows-TerminalServices-RemoteConnectionManager/Opertional.evtx», «Microsoft-Windows-TerminalServices-LocalSessionManager/Operational.evtx», «Microsoft-Windows-TerminalServices-RDPClient/Operational.evtx» зберігають окремі записи подій щодо віддаленого під'єднання до операційної системи облікових записів а також подій віддаленого керування нею з використанням протоколу Remote Desktop Protocol – RDP (записи подій 21, 22, 23, 24, 4624, 4625, 4634, 1149). Досліджуючи та співставляючи виявлені записи та їх мітки часу, експерт може відтворити хронологію про успішні та невдалі реєстрації облікових записів користувачів в системі, автентифікацію користувачів при під'єднанні до віддаленого робочого столу досліджуваної системи за необхідний період.

Дуже часто зловмисник після здійснення віддаленого втручання намагається «вичистити» сліди своїх дій у системі видаляючи як файли

самого ШПЗ, так і інші створені ним файли, а також записи у системних журналах подій, у зв'язку з чим експерту необхідно ретельно перевірити область видалених даних, у тому числі на видалені записи с журналів подій. Пошук та відновлення видалених записів проводиться з використанням спеціального ПЗ що має відповідний функціонал для опрацювання такого типу даних: Bulk Extractor with Record Carving, EvtxECmd, EVTXtract, Magnet AXIOM.

3. Провести дослідження каталогу та файлів попередньої вибірки (Prefetch, SuperFetch), записів Recent Applications, Recent Docs, Jump Lists, Open File History, Shell File History, SMB Events, Apps Compatibility Settings, правил та журналу брандмауера (Firewall rules and logs), записів Amcache (\%SystemRoot%\AppCompat\Programs\Amcache.hve) та Shimcache у системному реєстрі (HKLM\SYSTEM\CurrentControlSet\Control\ SessionManager\AppCompatCache\AppCompatCache).

Дослідження функцій виявленого ШПЗ. Дослідження функції проводиться одним з двох або обома методами – статичним та/або динамічним. Статичний аналіз є складним, оскільки являє собою дослідження вихідного коду, що вимагає від фахівця значної кваліфікації та навичок з реверс-інжинірингу (OllyDbg, IDA Pro, x64dbg), дизасемблювання та деобфускації, оскільки сучасні ШПЗ, зазвичай, мають обфускований та захищений від читання код [4]. До переваг статичного аналізу можна віднести отримання на виході дуже докладного результату з відображенням усіх явних та прихованих функцій. До недоліків – цей аналіз буде потребувати значного часу.

Найбільш ефективним методом дослідження функцій ШПЗ вбачається динамічний аналіз, що виконується шляхом спостереження за поведінкою ШПЗ в реальних умовах, із використанням віртуальної машини та т.з. «пісочниць» (віртуальних систем, налаштованих на фіксацію та аналіз дій програмного забезпечення). До частин динамічного

аналізу також слід віднести створення образу оперативної пам'яті враженої системи та збереження для подальшого дослідження файлу підкачки (pagefile.sys) та файлу гібернації (hyberfil.sys).

В «ручному» режимі динамічний аналіз проводиться, шляхом експериментального зараження операційної системи на віртуальній машині експерта з подальшим дослідженням процесів що виникли, та змін що відбулися в системі – тобто створенням власної «пісочниці». Рекомендується застосування програмного забезпечення: віртуальні машини - VMware або VirtualBox, дослідження процесів – набори програмних продуктів Sysinternals (Autoruns, ProcessMonitor, ProcessExplorer, TCPView, PortMon, LoadOrder та ін.) та Nirsoft (CurrProcess, WhatInStartup, WinPrefetchView, ServiWin та ін.), дослідження реєстру – RegShot, RegistryChangesView, YARU, створення образу оперативної пам'яті – AccessData FTK Imager, BelkaRamCapturer, MagnetRAMCapture, дослідження мережевої активності – NetworkMiner, WireShark. Крім того, сучасні програмні засоби дозволяють запускати та досліджувати копію враженої операційної системи у віртуальній машині, використовуючи її файл-образ (Virtual Forensic Computing, Disk Adapter For VMware Workstation, OpenLV).

В «автоматичному» режимі дослідження проводиться з використанням онлайн-«пісочниць», таких як Hybrid-Analysis, Any.Run, VirusTotal, joesandbox, sandbox.anlyz.io. В результаті опрацювання відправленого файлу видається докладний звіт, у якому відображаються всі виконувані ШПЗ дії та вказуються маркери шкідливості. Отримана інформація дозволяє підтвердити та деталізувати результати «ручного» режиму аналізу, а також допомагає виявляти деякі приховані та упущені шкідливі функції досліджуваного програмного забезпечення.

Виявлення ознак віддаленого керування. На даному етапі [6] експертом здійснюється:

1. Дослідження облікових записів, їх рівня привілеїв. Виявлення фактів створення нових облікових записів, видалення облікових записів, змін привілеїв.

2. Дослідження журналів подій операційної системи, зокрема з метою виявлення підключень по RDP.

3. Виявлення явних, видалених та прихованих чи навмисно модифікованих примірників програмного забезпечення для віддаленого керування (найбільш розповсюдженими є: TeamViewer, Radmin, TektonIt RMS, Ammy, AnyDesk, RemoteControl, Microsoft Remote Desktop, Supremo Remote Desktop, AeroAdmin, RemotePC, Splashtop, UltraVnc, TightVNC, RealVNC), їх файлів та слідів функціонування (журнали). Рекомендується застосовувати пошук за ключовими словами, пошук по таблицям відомих контрольних сум. Крім того, також доцільно перевірити перелік встановлених програм, служб, процесів.

Формування висновку. В результаті дослідження виявленої в ході дослідження інформації, зведення та співставлення виявлених фактів, відтворення хронології подій в системі, експерт доходить до висновку про наявність чи відсутність шкідливого програмного забезпечення та фактів віддаленого керування в досліджуваній системі.

Таким чином, підсумовуючи вищезазначене, зауважимо, що комп'ютерно-технічне дослідження шкідливого програмного забезпечення та виявлення слідів віддаленого втручання в роботу комп'ютерної системи є достатньо складним та кропітким процесом, час якого застосовується значна кількість спеціалізованого програмного забезпечення, та який потребує від експерта досвіду, знань, кваліфікації та вміння аналізувати значний обсяг даних. Сучасний стан рівня кіберзлочинності та швидкість її розвитку, вимагають адекватної відповіді від правоохоронних органів, тому роль таких досліджень при формуванні доказової бази у розслідуванні складно переоцінити.

Література

1. Кібенко О.Р. Діджиталізація як нова ера розвитку корпоративного права. // Судебно-юридическая газета: сайт: 16.07.2019. URL: https://sud.ua/ru/news/blog/145948-didzhitalizatsiya-yak-nova-era-rozvitku-korporativnogo-prava (дата звернення: 22.09.2020).
2. Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку // Науковий вісник Національної академії внутрішніх справ, 2020, № 2 (115) с. 58–68.
3. Harlan Carvey. Windows Forensic Analysis DVD Toolkit 2E. // © 2009 by Elsevier, Inc. ISBN 978-1-59749-422-9.
4. Сикорски Майкл, Хониг Эндрю Вскрытие покажет! Практический анализ вредоносного ПО. СПб.: Питер, 2018. 768 с.: ил. (Серия «Для профессионалов»). ISBN 978-5-4461-0641-7.
5. О. П. Войтович, В. О. Вітюк, В. А. Каплун. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів. ISSN 1999-9941 // Інформаційні технології та комп'ютерна інженерія. 2013. №3. С. 4–5.
6. Paresh Kerai. Remote Access Forensics for VNC and RDP on Windows Platform: Forensic Analysis of Remote Protocols Paperback / Edith Cowan University. ISBN 978-3659194290.
7. Monappa K.A. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware // 2018 Packt Publishing. ISBN 978-1788392501.