УДК 621.39

ВИКОРИСТАННЯ ЦИФРОВОЇ СТЕГАНОГРАФІЇ В СУЧАСНОМУ КІБЕРПРОСТОРІ

Фокін Д.Г., Євдокименко М.О.
Харківський національний університет радіоелектроніки, Україна
E-mail: denys.fokin@nure.ua, maryna.yevdokymenko@ieee.org

APPLICATION OF DIGITAL STEGANOGRAPHY IN MODERN CYBERSPACE

This paper reviews recent documented cyber incidents involving the use of digital steganography in images, audio, video, and network traffic. The analysis shows that steganographic techniques can be effective in circumventing threat detection systems during cyberattacks. However, real-world use cases remain rare and poorly documented due to the complexity of both the implementation and the detection process.

В роботі розглядаються останні задокументовані кіберінциденти, пов'язані із застосуванням цифрової стеганографії у зображеннях, аудіо-, відеофайлах та мережному трафіку. Аналіз показує, що стеганографічні методи можуть бути ефективними для обходу систем виявлення загроз під час кібератак. Водночас реальні випадки їхнього використання залишаються рідкісними та недостатньо задокументованими через складність як самої реалізації, так і процесу виявлення.

Стеганографія теоретично є значним ризиком для кібербезпеки, але її задокументоване використання в реальному світі, особливо публічно повідомлене, є відносно рідкісним.

Стеганографія зображень. Зловмисники часто приховують зловмисний код або дані у файлах зображень (JPEG, PNG, BMP), оскільки зображення є найбільш поширеними мультимедійними даними. Вбудовуючи шкідливе програмне забезпечення (ПЗ) в зображення, зловмисники можуть проскочити повз антивірусні сканери та брандмауери. Пізніше приховане корисне навантаження вилучається та виконується супутнім скриптом або завантажувачем шкідливого ПЗ у цільовій системі [1].

"GO#WEBBFUSCATOR" (2022) – кампанія по розповсюдженню шкідливого ПЗ приховала зашифроване корисне навантаження всередині зображення JPEG космічного телескопа Джеймса Вебба. При звичайному перегляді зображення було фотографією галактики, опублікованою NASA, але в текстовому редакторі воно показало замаскований блок сертифіката, який містить шкідливе ПЗ, закодоване Base64. Це дозволило початковому зараженню через фішинговий документ завантажити те, що виглядало як зображення, минаючи сканери, а потім декодувати його у виконуваний файл на комп'ютері жертви [2].

Аудіо стеганографія. При належному виконанні ця методика дозволяє аудіофайлу відтворюватися без помітних змін у якості звуку, незважаючи на приховане корисне навантаження. Як стеганографія зображень, ця тактика

може бути корисною для прихованої доставки шкідливого ПЗ.

"Криптомайнери в музиці" (2019) – кампанія з розповсюдження шкідливого ПЗ, яка приховує шкідливе ПЗ у файлах WAV для встановлення криптомайнерів Monero і бекдорів. Зловмисники поєднали музику у WAV форматі із, в одному випадку, XMRig-криптомайнером, в іншому – виконуваним кодом Metasploit для налаштування віддаленого доступу який завантажувач міг вилучити з аудіофайла в пам'ять комп'ютера. В одному випадку файл WAV містив XMRig криптомайнер, в іншому – виконуваний код Metasploit для створення зворотної оболонки. Для приховування корисного навантаження зловмисники використовували LSB-заміну і псевдовипадкове кодування. Особливістю є те, що прихований код шкідливого ПЗ ніколи не з'являвся у файловій системі – він був декодований і виконувався безпосередньо в пам'яті, що значно ускладнювало виявлення. Дослідники відзначили, що це був лише другий задокументований приклад використання аудіостеганографії для впровадження шкідливого ПЗ у реальних умовах, підкресливши, що аудіостеганографія є життєздатною технікою, хоча і рідкісною [3].

Відео стеганографія. Відеофайли мають значну ємність, і ймовірність їхнього сканування на прихований вміст є навіть нижчою, ніж у випадку зображень або аудіофайлів.

Одним із останніх задокументованих випадків використання було використання відео для вилучення даних із скомпрометованої мережі. У 2014 році одна з найбільших компаній зі списку Fortune 500 зазнала витоку конфіденційної інформації через відеофайли. Дані спочатку були зашифровані, а потім вбудовані у відеофайли за допомогою загальнодоступного інструменту стеганографії, ймовірно OpenPuff, після чого зловмисники завантажили їх в загальнодоступний хмарний сервіс для обміну відео. Завдяки цьому передавання відеофайлів виглядало як звичайне завантаження користувачами легітимного контенту, що унеможливило виявлення несанкціонованого вивантаження інформації традиційними засобами безпеки [4].

Мережна стеганографія. Мережна стеганографія стосується приховування інформації в мережних протоколах без створення нових файлів що значно ускладнює її виявлення традиційними засобами аналізу трафіку. Це можна зробити, маніпулюючи корисним навантаженням пакетів, їхньою послідовністю, часовими параметрами, полями заголовка протоколу [5]. Метою є створення прихованого каналу зв'язку, який буде непомітно інтегруватися в легітимний трафік, дозволяючи зловмисникам передавати конфіденційну інформацію або управляти шкідливим ПЗ.

Одним із останніх прикладів є Pingback – шкідливе ПЗ для Windows, виявлене у 2021 році, яке використовує ICMP-тунелювання для комунікації з

Command-and-Contol (C2) сервером. Замість використання HTTP або TCP Pingback здійснював надсилання та отримання команд через ICMP-пакети запиту та відповіді, використовуючи протокол, що зазвичай застосовується для діагностики мереж (утиліта ping). Використання ICMP як каналу зв’язку дає зловмисникам переваги: ICMP-трафік не має портів і рідко перевіряється брандмауерами чи засобами типу netstat. Інструменти, як Pingback, приховано передають C2-команди в корисному навантаженні ICMP-пакетів, утворюючи непомітний двосторонній канал зв'язку з зараженими пристроями. Виявити мережну стеганографію важко, адже вона використовує дозволений трафік (ICMP або DNS), який зазвичай не аналізується глибоко, що дає змогу обходити засоби виявлення загроз і ексфільтрувати дані [6].

Підсумовуючи, сучасна цифрова стеганографія залишається складним, але ефективним інструментом. В останніх задокументованих випадках вона використовувалася переважно для прихованої доставки шкідливого ПЗ, керування зараженими системами та викрадення даних. Випадки її виявлення залишаються рідкісними, що пояснюється кількома факторами. По-перше, ця техніка є складною у реалізації, і її застосовують лише кваліфіковані зловмисники в спеціалізованих сценаріях. По-друге, методи виявлення стеганографії є недостатньо розвиненими, що ускладнює автоматизацію їхнього виявлення. По-третє, дослідження подібних атак вимагає тривалого аналізу, через брак публічних звітів залишається маловідомим. Як наслідок, хоча задокументовані випадки використання стеганографії є відносно застарілими, це не виключає її використання у складних і цільових атаках.

Література

1. The Hacker News. Steganography explained: how xworm hides inside images. The Hacker News. URL: https://thehackernews.com/2025/03/steganography-explained-how-xworm-hides.html (date of access: 16.03.2025).
2. Toulas B. Hackers hide malware in James Webb telescope images. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/hackers-hide-malware-in-james-webb-telescope-images/ (date of access: 16.03.2025).
3. Gatlan S. Attackers hide backdoors and cryptominers in WAV audio files. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/attackers-hide-backdoors-and-cryptominers-in-wav-audio-files/ (date of access: 16.03.2025).
4. Paganini P. Hackers used data exfiltration based on video steganography. Security Affairs. URL: https://securityaffairs.com/30624/cyber-crime/hackers-used-data-exfiltration-based-video-steganography.html (date of access: 16.03.2025).
5. Team Nuspire. Steganography in cybersecurity: a growing attack vector. Security Boulevard. URL: https://securityboulevard.com/2022/05/steganography-in-cybersecurity-a-growing-attack-vector/ (date of access: 16.03.2025).
6. Sharma A. New Windows 'Pingback' malware uses ICMP for covert communication. Bleeping Computer. URL: https://www.bleepingcomputer.com/news/security/new-windows-pingback-malware-uses-icmp-for-covert-communication/ (date of access: 16.03.2025).