УДК 004.056:341.4
КАРЕН ЮРІЙОВИЧ ІСМАЙЛОВ
кандидат юридичних наук, завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ
ВОЛОДИМИР ГЕОРГІЙОВИЧ ПЯДИШЕВ
кандидат технічних наук, доцент, доцент кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ

У світі, керованому соціальними мережами, онлайн-транзакціями, хмарними обчисленнями і автоматизованими процесами, технології розвиваються швидко. Але паралельно з технологічної еволюцією відбувається прогрес кіберзлочинності, яка постійно розвиває нові типи атак, інструменти і методи, що дозволяють злочинцям проникати в більш складні або добре контрольовані середовища, а також збільшувати збитки і навіть залишатися непомітними. Але окрім загального очікування поширення кіберзлочинності, з метою ефективності витрачання ресурсів на боротьбу з нею, необхідно здійснювати більш детальні прогнозування напрямів і масштабів її поширення у різних сферах держаної діяльності, бізнесу, охорони здоров'я тощо. .

Отже, Netwrix – приватна компанія (США) по забезпеченню IT-безпеки, яка пропонує рішення для IT-аудиту для систем і додатків в IT-інфраструктурі, – на підставі аналізу даних 2015 р. визначала напрями, що потребують найбільшої пильності у боротьбі з кіберзлочинністю, таким чином [1]:

1. Злом або шкідливі програми. Шкідливі програми і електронні записи сторонніх осіб залишалися основною причиною порушень даних другий рік поспіль. Зареєстровані випадки сталися через те, що хакери отримали несанкціонований доступ до системи компанії за допомогою атак веб-додатків, шпигунських програм, соціальної інженерії і троянів. Це містить левову частку всіх скомпрометованих даних клієнтів (близько 195 мільйонів записів).

2. Другий найбільш часто зареєстрований тип кіберзлочинності – це несанкціонований доступ до інформації, що зберігається на портативних пристроях, включаючи ноутбуки, смартфони та зовнішні жорсткі диски. Результатом є втрата понад 20 000 конфіденційних даних у 2015 р.

3. Ненавмисне розкриття (людський фактор). Більше 38 000 записів було розкрито через помилки працівників: неправильна адресація електронної пошти та конфіденційної інформації, випадкове розміщення на веб-сайтах компаній.

4. Неправомірна робота інсайдерів (працівників з легальними правами) – порушення цілісності даних:інсайдери заподіяли значної шкоди і скомпрометували більше 600 000 записів клієнтів.

5. Фізичні (неелектронні) втрати даних: втрата або викрадення неелектронних активів з конфіденційною інформацією (паперових документів, карток, канцелярських пристроїв) стали основною причиною витоку даних, що призвело до втрати 1100 записів.

Разом з тим, проведення спеціалізованих досліджень надали можливість встановити важливі кореляції (зв’язки), наприклад, кореляція між видами діяльності і типами атак. Отже, кібер-шпигунство, швидше за все, націлено на уряд, ЗМІ та правоохоронні органи і вельми малоймовірно в інших секторах (роздрібна торгівля, телекомунікації, онлайн-послуги тощо) [2].

Кореляція свідчить також, що, метою кібер-шпигунства, кібервійни і хактівізма швидше за все є державний сектор (уряд, правоохоронні органи, освіта тощо). Проте кібер-злочинність все ж таки націлена на всі сфери бізнесу.

Стосовно динаміки останнього часу щодо поширення проявів кіберзлочинності показові результати лабораторії Malwarebytes Labs, від липня 2018 р. Отже, протягом другого кварталу 2018 р. спостерігалась наступна динаміка проявів кіберзлочинності [3]:

- Cryptomining все ще трималися на високому рівні, але почали знижуватися;
- GandCrab домінували серед програм для вимагання;
- Рекламне програмне забезпечення, що нав’язують, виросло на 19% у порівнянні з попереднім кварталом;
- VPNFilter дебютувало з більш ніж 500.000 виявленнями;
- Експлойти — комп'ютерні програми, що використовують уразливості в програмному забезпеченні та застосовуються для проведення атаки на обчислювальну систему, — демонстрували підйом;
- Шахраї все частіше спрямовували зусилля на PII (особові дані ідентифікації).

Нагадаємо, тут:

- Cryptomining - це вид програми вимагання, яка шифрує всі файли користувача і змінює їх в форматі .KRAB. Вона не блокує використання комп'ютера користуачем, але шифрує практично всі файли на комп'ютері [4].
- GandCrab - це вид програм для здійснення вимагань, які шифрують всі файли користувача і змінюють їх до формату .KRAB, при цьому не блокується використання комп'ютера користувачем, але практично всі файли на комп'ютері шифруються [5];
- VPNFilter — шкідливе програмне забезпечення для зараження маршрутизаторів .
- Експлойти — комп'ютерні програми, що використовують уразливості в програмному забезпеченні та застосовуються для проведення атак на обчислювальну систему;
- PII (personal identification information) — особиста ідентифікаційна інформація.

Висновок.

1. Загальна кількість кібератак у світі розширятиметься.
2. Кібер-шпигунство, кібервійна і хактівізм атакуватимуть у першу чергу державний сектор (уряд, правоохоронні органи, освіта тощо).
3. Основна маса порушень і компрометації даних, як і раніше, здійснюватиметься через використання шкідливих програм, причому

об’єктами злому все частіше будуть портативні пристрої, а також побутові системи типу «розумний будинок», тощо.

4. Значною проблемою у протистоянні кіберзлочинності залишатиметься кримінальна діяльність «інсайдерів».

5. Кіберзлочинці все більше уваги приділятимуть приховуванню слідів своєї злочинності.

Список бібліографічних посилань:

1. Irvine, C.A. Top five cybercrime patterns to watch out for in 2016. *Netwrix, January 5, 2016*. URL : https://www.netwrix.com/ top_five_cybercrime_patterns_for_2016.html [Accessed 25 November, 2018].

2. Bendovschi A. Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, Volume 28, 2015, Pages 24-31* : site. URL : https://www.sciencedirect.com/science/article/pii/ S2212567115010771#! [Accessed 25 November, 2018].

3. Cybercrime tactics & techniques Q2 2018. Malwarebytes Labs. July 23, 2018 : site. URL : https://blog.malwarebytes.com/malwarebytes-news/ctnt-report/2018/07/cybercrime-tactics-techniques-q2-2018/ [Accessed 25 November, 2018].

4. Cryptomining. Malware Wikia : site. URL :. http://malware.wikia.com/ wiki/ Cryptomining

5. GandCrab. Malware Wikia : site. URL : http://malware.wikia.com/wiki/ GandCrab [Accessed 25 November, 2018].

УДК 004[681.518]

ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Комплексний захист інформації ґрунтується на використанні правових, фізичних, організаційних та програмно-апаратних засобів захисту інформації, до яких належить криптографічний захист інформації. Цей вид захисту інформації реалізується шляхом перетворення інформації з використанням ключів на основі математичних методів. Є дві мети використання криптографічних методів – приховування інформації шляхом її шифрування та підтвердження юридичної значимості документів з використанням електронного підпису.

Криптографічні методи вирішують два завдання – забезпечення конфіденційності інформації шляхом позбавлення зловмисника можливості видобути інформацію з каналу зв’язку та забезпечення цілісності інформації шляхом недопущення зміни інформації та внесення в неї неправдивого змісту [1].