Шкідливі програми як загроза об'єктам критичної інфраструктури в умовах кібервійни

Міжвідомчий круглий стіл

21 лютого 2023 року м. Київ

УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ СПЕЦІАЛЬНОЇ ТЕХНІКИ ТА СУДОВИХ ЕКСПЕРТИЗ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

УКРАЇНСЬКИЙ ІНСТИТУТ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ПРАЦІВНИКІВ ТЕЛЕБАЧЕННЯ, РАДІОМОВЛЕННЯ І ПРЕСИ

ШКІДЛИВІ ПРОГРАМИ ЯК ЗАГРОЗА ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ КІБЕРВІЙНИ

Збірник матеріалів міжвідомчого круглого столу

21 лютого 2023 року

м. Київ

УДК 004.42.056(477)(06)
Ш66

Рекомендовано до друку
Науково-технічною радою ІСТЕ СБУ
(протокол № 3 від 29 березня 2023 року)

Робочою групою УТРПІ
(протокол № 1 від 24 березня 2023 року)

Ш66 Шкідливі програми як загроза об'єктам критичної інфраструктури в умовах кібервійни : збірник матеріалів міжвідомчого круглого столу, 21 лютого 2023 року. – Київ : ІСТЕ СБУ, 2023. – 204 с.

ISBN 978-617-8013-53-0

Збірник містить матеріали міжвідомчого круглого столу «Шкідливі програми як загроза об'єктам критичної інфраструктури в умовах кібервійни», що відбувся 21 лютого 2023 року у м. Києві (Укрінформ). В тезах доповідей та презентаціях автори розглянули проблемні питання та перспективи кіберзахисту об'єктів критичної інфраструктури від кібератак з використанням шкідливих програмних засобів.

Розраховано на представників суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, а також співробітників судових, правоохоронних органів і спеціальних служб, установ судової експертизи, науковців, викладачів, аспірантів, ад'юнктів та докторантів закладів вищої освіти.

УДК 004.42.056(477)(06)

ЩО НАДХОДЯТЬ НА ЕЛЕКТРОННУ АДРЕСУ
ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 75

ЛАНДЕ Дмитро Володимирович
ВИЯВЛЕННЯ ДЖЕРЕЛ ШКІДЛИВОГО
ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА
ТЕХНОЛОГІЯМИ OSINT..... 77

МЕЛЬНИКОВ Ілля Миколайович
ВАЖЛИВІ ПИТАННЯ ПРОФІЛАКТИКИ ЗЛОЧИННОСТІ
У СФЕРІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ЯК ЗАГРОЗИ
ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 81

НЕДІЛЬКО Артем Олександрович
ЩОДО ПРОТИДІЇ КІБЕРАТАКАМ НА
ІТ-ІНФРАСТРУКТУРУ..... 86

НІЗОВЦЕВ Юрій Юрійович
СУДОВО-ЕКСПЕРТНЕ ТА ТЕХНІКО-КРИМІНАЛІСТИЧНЕ
ЗАБЕЗПЕЧЕННЯ У СФЕРІ ПРОТИДІЇ КІБЕРЗАГРОЗАМ:
НАУКОВІ ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ 88

ОМЕЛЬЯН Олексій Сергійович
ЩОДО РІВНЯ СПЕЦІАЛЬНИХ ЗНАНЬ
ЕКСПЕРТА ПРИ ДОСЛІДЖЕННІ
ШКІДЛИВИХ ПРОГРАМНИХ ЗАСОБІВ 94

ПАКРИШ Олександр Євгенійович
ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ВІД ЗАСТОСУВАННЯ ПРОГРАМ-ВИМАГАЧІВ 97

ПЕПА Юрій Володимирович
ЗАСОБИ ПРОНИКНЕННЯ В АВТОМАТИЗОВАНУ СИСТЕМУ
ТА РАННЄ ЇХ ВИЯВЛЕННЯ..... 100

ПЛАХОТНІК Олег Віталійович
НЕБЕЗПЕКА РОЗГОЛОШЕННЯ ОКРЕМИХ ВІДОМОСТЕЙ
У ТЕКСТАХ СУДОВИХ РІШЕНЬ 110

ПРОКОПОВ Сергій Олександрович
ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕРМІНАЛІВ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ВІД ШКІДЛИВИХ ПРОГРАМ..... 115

РИБАЛЬЧЕНКО Людмила Володимирівна,

ЛАНДЕ Дмитро Володимирович,
доктор технічних наук, професор,
керівник наукового центру ІІБП НАПрН України,
завідувач кафедри інформаційної безпеки
КПІ ім. Ігоря Сікорського

ВИЯВЛЕННЯ ДЖЕРЕЛ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА ТЕХНОЛОГІЯМИ OSINT

Відкриті інформаційні ресурси мережі Інтернет містять неявні експертні оцінки, що вносяться користувачами. Невід'ємна складова інформаційної і кібернетичної безпеки – методологія і стек технологій розвідки у відкритих джерелах (OSINT) полягає у виявленні та екстрагуванні цих прихованих знань, їх узагальненні, а також подальшій аналітичній обробці. В роботі представлено методику екстрагування понять із текстів документів із мережевих джерел, що стосуються кібербезпеки, а саме злочинних хакерських угрупувань, зокрема, російських і білоруських, що є учасниками сучасної кібервійни, а також відповідного шкідливого програмного забезпечення.

Постановка проблеми

Фахівцям, що працюють у галузі інформаційної і кібернетичної безпеки, зазвичай відомі її основні поняття та об'єкти. Проте, з плином часу виникають нові поняття та нові об'єкти. У сфері кібербезпеки такими об'єктами можуть бути хакерські угрупування, шкідливе програмне забезпечення, види кібератак, уразливості, так звані бекдори тощо. Змістовні зв'язки між такими об'єктами можуть динамічно з'являтися і зникати. Таким чином, виникає завдання постійного моніторингу інформації у межах цієї предметної галузі. До такої інформації може бути застосована технологія розвідки у відкритих джерелах (Open Source INTelligence, OSINT) [1,2,3]. Моніторинг і аналіз відкритих джерел інформації з метою пошуку цільового контенту приводить до необхідності застосування технологій Big Data, які успішно розвиваються на цей час.

Мета роботи

Мета цієї роботи – представлення методики визначення об'єктів кібербезпеки і зв'язків між ними на базі аналізу змістовної складової інтернет-простору. Для досягнення цієї мети вирішується низка завдань, зокрема, цільового збору інформації, її обробки, витягу із неї необхідних сутностей, встановлення зв'язків між ними, тобто формування мережі, кластерний аналіз мережі об'єктів, виявлення центрів цих кластерів тощо.

Опис методики

Пропонується до розгляду методика, сутність якої полягає у виконанні таких технологічних операцій, як: 1) добування інформації; 2) екстрагування понять – об'єктів кібербезпеки; 3) фільтрація понять із залученням експертів (або засобів штучного інтелекту); 4) формування мережі об'єктів кібербезпеки;

5) аналіз (у тому числі кластеризація) і візуалізація цієї мережі; 6) візуалізація динаміки появи понять у часі.

На 1-му етапі формується тематичний інформаційний масив, для чого мають використовуватись наявні інформаційно-пошукові системи, як загальнодоступні, так і корпоративні системи контент-моніторингу, наприклад систем контент-моніторингу Cyber Aggregator, Attack Index і InfoStream [2, 3], які дозволяють збирати інформацію із веб-сайтів і 12 соціальних мереж.

Як приклад розглядається дослідження є аналіз активності російських/білоруських хакерських угрупувань впродовж 2022 і початку 2023 року. Для отримання інформаційного масиву публікацій щодо кібербезпеки необхідно визначити та опрацювати тематичний запит , наприклад такий:

хакер|(вредоносн-программн)|(шкідл-програмн)|
(кибер-атак)|кібератак|(кібер-атак)|кібератак

Зазначимо, що в рамках методики, що пропонується, запит формується саме у кирилиці, для спрощення подальшого екстрагування об’єктів. В результаті опрацювання подібного запиту отримується масив релевантних документів, який підлягає подальшій обробці.

На 2-му етапі на основі лінгвістичного і статистичного аналізу здійснюється екстрагування понять із предметної області, що містяться в документах отриманого тематичного інформаційного масиву.

Основна ідея розпізнавання іменних сутностей – об’єктів кібербезпеки полягає у тому, що на цей час більшість іменних сутностей об’єктів кібербезпеки, таких як хакерські угрупування, назви шкідливого програмного забезпечення, тощо, в документах. наведених не у латинському кодуванні, переважно позначаються латиницею, або кириличними літерами, але в лапках. Це значно спрощує задачу екстрагування. У цих випадках достатньо виявляти короткі слова або словосполучення у латинському кодуванні або у лапках. Крім того, для екстрагування вже відомих іменних сутностей також застосовується словник відомих іменних сутностей об’єктів кібербезпеки, які відшукуються в інформаційному масиві.

На 3-му етапі здійснюється сортування відібраних понять за частотою та фільтрація цих понять фахівцем-експертом (Рис. 1).

На 4-му етапі здійснюється формування мережі відібраних понять. Для цього визначаються неспрямовані зв’язки між поняттями. Зв’язки можуть встановлюватись на базі різних підходів, зокрема, два поняття можуть вважатися зв’язаними, якщо вони входять в той самий сегмент документу (речення, абзац, окіл у N слів, або цілий документ) із відібраного інформаційного масиву.

Ранг	Хакерське угрупування	Знайдено документів
1	KillNet	3058
2	RaHDIt	1842
3	Armageddon	1082
4	Sandworm	864
5	UNC1151	823
6	APT28	481
7	Trickbot	365
8	APT29	361
9	UAC-0056	326
10	Xaknet	281
11	DarkSide	247
12	Turla	153
13	ColdRiver	142
14	UAC-0041	142
15	Callisto	140
16	FIN7	78
17	Nobelium	73
18	Berserk Bear	33
19	CyberArmyofRussia_Reborn	31
20	Z-Team	23
21	Venomous Bear	20
22	Pawn Storm	16

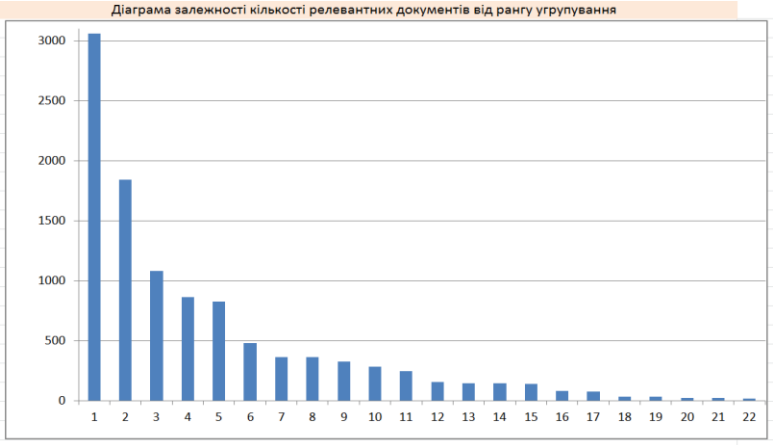

Рисунок 1. Перелік найчастіше згадуваних хакерських угрупувань із росії/білорусії

На 5-му етапі здійснюється кластерний аналіз відібраної мережі та знаходження об'єктів – центрів кластерів за алгоритмом модулярності, а також візуалізація сформованої мережі із застосуванням системи Gephi (Рис.2).

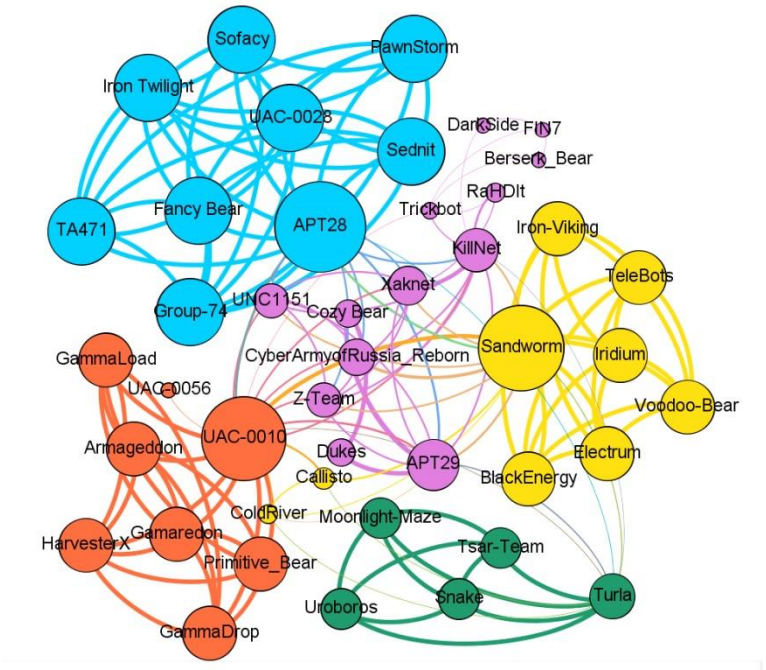

Рисунок 2. Мережа основних хакерських угрупувань із росії/білорусії

Для кластеризації обчислюється модульність окремих вузлів – іменних сутностей, відповідають хакерським угрупуванням, на основі якої здійснюється виявлення клік в цій мережі (кластерів).

Висновки

Запропоновано методику виявлення іменних сутностей об'єктів кібербезпеки із документів, а також аналізу взаємозв'язків і динаміки об'єктів предметної області. Методика враховує приховані знання, внесені експертним мережевим середовищем.

Результати контент-моніторингу Інтернет-ресурсів вказують на переважну приналежність розглянутих хакерських угрупувань до спецслужб рф і білорусії, а саме:

- ФСБ рф (Gamaredon, Primitive_Bear, UAC-0010).
- ГУ ГШ ЗС рф (ГРУ) (Sandworm, BlackEnergy, Electrum, Iridium, Iron-Viking, TeleBots, Voodoo-Bear, APT28, UAC-0028, TA471, Fancy Bear, PawnStorm, Sednit, Sofacy, Iron Twilight, Group-74).
- СЗР рф (APT29, Cozy Bear, Dukes, UAC-0029).
- Міністерство оборони рб (UNC1151, GhostWriter, UAC-0051).
- Проросійські угрупування (Xaknet, KillNet, RaHDIt, Z-Team, UAC-0106, UAC-0108, UAC-0109, UAC-0107).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ATP 2-22.9. Army Techniques Publication No. 2-22.9 (FMI 2-22.9). Open-Source Intelligence. Headquarters Department of the Army Washington, DC, 10 July 2012.
2. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system. Theoretical and Applied Cybersecurity, 2019. – Iss. 1. – pp. 103-108.
3. D. Lande, O. Puchkov, I. Subach, M. Boliukh, D. Nahornyi OSINT investigation to detect and prevent cyber attacks and cyber security incidents // Information Technology and Security, 2021. Vol 9 (2). – pp. 209-218. DOI: doi.org/10.20535/2411-1031.2021.9.2.249921.
4. Cherven K. Mastering Gephi Network Visualization. – Packt Publishing, 2015. – 378 p. ISBN 78-1-78398-734-4.