УДК 004.056:004.89

МЕТОД АТРИБУЦІЇ КІБЕРАТАК НА ОСНОВІ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ ІЗ ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Сторожко А.В.
Науковий керівник – к.т.н., ст. викл. Адамов О.С.
Харківський національний університет радіоелектроніки, каф. АПОТ,
м.Харків, Україна
тел. +38(099)-931-65-35, e-mail: andrii.storozhko@nure.ua

This work is devoted to the method of attribution of cyberattacks. It is based on the use of compromising indicators of existing Russian hacker groups and the possibility of attributing attacks using artificial intelligence. Thanks to artificial intelligence, attack indicators are compared and, in the future, the involvement of a particular group of hackers is determined. Gathering data on a cyberattack will also allow the identification of new, previously unknown groups of hackers. Determining the totality of attack factors allows us to further diagnose a cyber attack and improve the security of the system.

Вступ. У сучасному світі кіберпростір став невід'ємною частиною буття. Багато людей спілкуються, розважаються та працюють завдяки віртуальному середовищу. Підприємства (у тому числі і державні) Використовують мережу як для керування різними системами так і для збереження важливих даних.

На жаль мережа не так захищена від хакерських атак як хотілось би, та і самі хакери з часом стають куди кмітливіше та винахідливіше. Важливо не тільки запобігати кібер атакам але і знати які самі групи хакерів здійснюють напад. У цьому допомагають компрометуючі індикатори за якими розпізнається та чи інша кібер група.

Мета дослідження – визначення належності груп хакерів до кібератаки за допомогою індикаторів компрометації. Розроблення штучного інтелекту для визначення кібер груп за допомогою порівняння існуючих індикаторів.

Завдання – створення штучного інтелекту, функція якого буде виконувати порівняння хешів, файлів та інших індикаторів кібер атак з існуючими індикаторами хакерських угрупувань.

Зміст дослідження. Атрибуція - це частина великого процесу під назвою Threat Intelligence і буде виглядати так:

- визначення того, ЩО на вас напало – робота з індикаторами компрометації;
- визначення того, ЯК це сталося - визначення тактик, технік та процедур зловмисників;
- визначення того, ВИПАДКОВО це сталося чи є частиною цілої КАМПАНІЇ;

- визначення того, хто стоїть за атакою і ЧОМУ хтось нас атакує.

Також розглянуто модель «Cyber Kill Chain» (ланцюг кібервторгнень). Базова версія моделі включає (передбачає) сім етапів, необхідних для реалізації успішної кібератаки:

1) розвідка;
2) озброєння;
3) доставка;
4) експлуатація;
5) встановлення;
6) командування та контроль;
7) виконання дій.

Зловмисник виконує розвідку, вторгнення, використання вразливостей. Далі слідує отримання та підвищення привілеїв, переміщення для доступу до більш цінних активів. На фінальній стадії робиться спроба приховування своєї активності, і проводиться ексфільтрація (приховане вивантаження) необхідних даних за межі цільового середовища.

Domain	ID		Name	Use
Enterprise	T1134	.001	Access Token Manipulation: Token Impersonation/Theft	APT28 has used CVE-2015-1701 to access the SYSTEM token and copy it into the current process as part of privilege escalation.[25]
Enterprise	T1098	.002	Account Manipulation: Additional Email Delegate Permissions	APT28 has used a Powershell cmdlet to grant the `ApplicationImpersonation` role to a compromised account.[2]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	APT28 registered domains imitating NATO, OSCE security websites, Caucasus information resources, and other organizations.[6][14][26]
		.006	Acquire Infrastructure: Web Services	APT28 has used newly-created Blogspot pages for credential harvesting operations.[26]
Enterprise	T1595	.002	Active Scanning: Vulnerability Scanning	APT28 has performed large-scale scans in an attempt to find vulnerable servers.[27]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Later implants used by APT28, such as CHOPSTICK, use a blend of HTTP, HTTPS, and other legitimate channels for C2, depending on module configuration.[6][2]
		.003	Application Layer Protocol: Mail Protocols	APT28 has used IMAP, POP3, and SMTP for a communication channel in various implants, including using self-registered Google Mail accounts and later

Приклад 1 – використані техніки групи Російських хакерів APT28.

Висновки: Наукова новизна визначається у використанні моделей машиного навчання за для вирішення задач атрибуції кібер атак, що у подальшому може використовуватися для перешкоджання повторних нападів.

Список використаних джерел. 1. Фленов М.В., «Web-сервер глазами хакера»: 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2009. – 320с. 2. Peter Szor., «Art of Computer Virus Research and Defense», Addison-Wesley Professional (February 3, 2005). 3. «Hacking the art of exploitation», Jon Erickson. 4. Інтернет ресурс - https://attack.mitre.org.