## NETWORK AND APPLICATION SECURITY

DOI 10.20535/2411-1031.2021.9.2.249899
УДК 004.056.53:621.391

ІГОР ЯКОВІВ,
АНДРІЙ ТРОХИМЕНКО,
КИРИЛО ГЛУМ

# СПОСІБ ВИЗНАЧЕННЯ КАНАЛУ КЕРУВАННЯ APT-АТАКОЮ

Широкомасштабне застосування проти національної критичної інфраструктури складних кібератак типу APT стало потужним стимулом для розвитку методів проактивного кіберзахисту. Характерними для APT-атак є наступні властивості: атака представляє складний набір взаємозв'язаних за часом і простором дій зловмисника. Окремо ці дії можуть не викликати підозр; цільова акція атаки в кіберсегменті об'єкта готується тривалий час (від декількох місяців до року і більше); сукупність дій зловмисника – це ланцюжок тактик, виконання яких дозволяє досягти мети атаки. Попри різноманітність засобів, що використовуються в APT-атаках, набір більшості тактик та їх сутність залишаються постійними. Основою багатьох APT-атак є використання зловмисником несанкціонованих каналів керування атакою через Інтернет, які дозволяють йому виконувати різні дії в сегменті кіберпростору системи інформаційних технологій жертви. Актуальним є завдання своєчасного визначення таких каналів ще на етапах підготовки цільової акції атаки. Такий підхід відповідає реалізації проактивної стратегії кіберзахисту. За результатами досліджень інформаційних процесів формування та використання несанкціонованого каналу, організації процесів систем проактивного кіберзахисту розроблено спосіб визначення каналу управління APT-атакою. Він може бути використаний в рамках керування інформацією та подіями безпеки SIEM для визначення атаки після її етапу проникнення в систему інформаційних технологій, але ще до реалізації етапу цільової акції. Спосіб розроблено на основі використання кібернетичної моделі APT-атаки із застосування методів формалізованого аналізу інформаційних процесів сучасних систем оперативного кіберзахисту. В рамках досліджень розроблено процедуру формування та використання багатоіндикаторного шаблону каналу керування, що застосовується для комплексного аналізу подій безпеки. Для заповнення шаблону розроблено програмний засіб, що формує інформацію про події безпеки на хостах корпоративної системи. Теоретичні та практичні результати досліджень орієнтовано на застосування у складі SOC корпоративної інформаційної системи для проактивного захисту від APT-атак.

**Ключові слова:** система кіберзахисту, проактивна стратегія, SIEM, SOC, детектування APT, несанкціонований канал керування, backdoor, цільова акція атаки.

**Постановка проблеми.** Аналіз наявних практик захисту корпоративних систем інформаційних технологій (англ. Information Technology System, IT-system, ITS, укр. IT-система) дозволяє виділити дві стратегії протидії кібератакам: реактивний захист і проактивний (превентивний) захист. Загальною основою для цих стратегій є наступні процеси:

1) спостереження в реальному часі (in real time) за подіями в позначеному сегменті кіберпростору;
2) формування за допомогою сенсорів, збір і нормування інформації про події безпеки в єдиному центрі оперативної обробки;
3) аналіз подій і прийняття рішення про наявність кібератаки;
4) прийняття рішення про протидію атаці й реалізація цього рішення за допомогою актуаторів безпеки (виконавчих пристроїв безпеки).

Для *реактивної стратегії* прийняття рішення про виявлення атаки завершується після її закінчення. Заходи протидії можуть запобігти тільки такий же наступній атаці. Для *проактивного (превентивного) захисту* виявлення атаки має відбутися ще до її завершення. В такому випадку залишається час на реалізацію заходів переривання цієї атаки.

Ключовою частиною сучасних систем кіберзахисту корпоративних ІТ-систем є центри операцій кібербезпеки (англ. CyberSecurity Operations Center, CSOC або SOC). Такі центри за допомогою операторів і/або засобів керування інформацією і подіями безпеки (англ. Security of Information and Event Management, SIEM) з різним ступенем автоматизації реалізують перераховані вище процеси 1-4. Якщо загальний час реалізації цих процесів перевищує час проведення атаки, то стратегія кіберзахисту може мати тільки реактивний характер. Значний обсяг атак, для яких наперед відомий критичний ресурс (мета атаки) та послідовність компрометуючих дій, виконуються в автоматичному режимі. У цьому випадку час реакції системи кіберзахисту, як правило, буде перевищувати тривалість зловмисних дій. Впродовж останнього десятиріччя став поширений клас більш складних атак, для яких критичний ресурс, що дозволяє реалізувати шкідливий вплив, заздалегідь невідомий. Після проникнення в ІТ-систему зловмиснику потрібний додатковий час для збору необхідної інформації, прийняття рішення про подальші дії та їх реалізацію. Це може бути складний довготривалий процес, для реалізації якого зловмиснику потрібний канал несанкціонованого доступу до ресурсів ІТ-системи. В рамках протидії таким атакам з'являється можливість реалізації проактивної стратегії.

З 2013 року зафіксоване широкомасштабне застосування проти національної критичної інфраструктури складних кібератак типу APT (англ. Advanced Persistent Threat, вдосконалена стійка загроза або цільова атака). Це стало потужним стимулом для розвитку методів проактивного кіберзахисту на основі детектування каналів керування ще до моменту доступу зловмисника до критичного ресурсу.

**Аналіз останніх досліджень і публікацій.** Аналіз різних інформаційних джерел [1] - [7] дозволяє визначити наступні характерні особливості APT-атак (APTs):

– атака представляє складний набір взаємозв'язаних за часом і простором дій зловмисника. Окремо ці дії можуть не викликати підозр;

– цільова акція атаки в кіберсегменті об'єкта готується тривалий час (від декількох місяців до року і більше);

– сукупність дій зловмисника – це ланцюжок тактик, виконання яких дозволяє досягти мети атаки (цільової акції). Попри різноманітність засобів, що використовуються в APTs, набір більшості тактик і їх сутність залишаються постійними.

Подальший аналіз цих характерних тактик (етапів) [5], [6], [9] дозволяє уточнити суть дій зловмисника в рамках APT атаки. Після визначення корпоративної ІТ-системи і її ресурсу, який критичний для зловмисника (наприклад: база даних, диспетчерський комп'ютер SCADA, вебсайт або інше – об'єкт атаки), він діє таким чином.

Етап 1. Зовнішня розвідка. Здійснюється збір інформації про характеристики ІТ-системи з різноманітних джерел поза нею.

Етап 2. Проникнення в ІТ-систему. На основі інформації зовнішньої розвідки приймається рішення про засоби й способи запуску несанкціонованих процесів на одному із хостів системи. За допомогою комп'ютера зловмисника здійснюється реалізація рішення шляхом направлення через Інтернет необхідних даних. На основі прийнятих повідомлень запускаються процеси, які встановлюють прихований канал віддаленого керування хостом (англ. backdoor, BD).

Етап 3. Доставка засобів впливу. Отримана зловмисником інформація про встановлений прихований канал керування запускає процес доставки набору несанкціонованих програмних засобів, що дозволяють здійснити внутрішню розвідку в межах корпоративної комп'ютерної мережі.

Етап 4. Внутрішня розвідка. Шляхом запуску несанкціонованих і штатних процесів здійснюється збір даних про компоненти мережі. Зібрана інформація надсилається по прихованому каналу зловмисникові. Після її оцінки приймається і реалізується рішення про просування від одного вузла мережі до іншого до моменту виявлення критичного ресурсу.

Етап 5. Цільовий вплив (цільова акція атаки). На основі отриманих даних про знаходження критичного ресурсу зловмисником приймається рішення про засоби й способи реалізації цільового впливу. За допомогою BD до критичного хоста доставляються необхідні програмні засоби. Запускаються несанкціоновані процеси, які реалізують компрометацію цільового ресурсу (отримання доступу до критичної інформації й передача зловмисникові, отримання доступу до управління технологічним процесом і переведення його в потрібний стан, порушення процесів обробки інформації).

Етап 6. Приховування слідів атаки. За допомогою несанкціонованих процесів на всіх хостах стираються дані, які були пов’язані з атакою.

Проведений аналіз дозволяє стверджувати, що формування BD та його застосування є основними процесами, які дозволяють зловмиснику в рамках APT-атаки отримувати інформацію про стан IT-системи, визначати, доставляти та застосовувати необхідні програмні засоби для проведення несанкціонованих дій.

Отже, актуальним стає завдання своєчасного визначення (детектування) BD ще на етапі підготовки цільової акції. Встановлення оперативного контролю над BD дозволяє приймати своєчасні рішення про припинення атаки, або про проведення додаткових заходів зниження збитків від цієї атаки у випадку неможливості її припинення. Такий підхід відповідає реалізації проактивної стратегії кіберзахисту, метою якої є переривання APT-атаки ще до початку етапу цільової акції [8], [11].

**Метою статті є** розробка способу визначення каналу керування APT-атакою, який дозволяє формувати механізми проактивного кіберзахисту.

**Виклад основного матеріалу досліджень.** У рамках досліджень виконані наступні часткові завдання:

- аналіз інформаційних процесів формування та застосування BD в рамках APT-атаки;
- вибір моделі APT-атаки;
- розробка моделі поведінки BD;
- визначення відповідності процедур управління в рамках BD та елементарних бітових подій IT-системи (трафіків, файлів, обчислювальних процесів);
- розробка структури шаблону BD;
- програмний засіб для формування інформації про події безпеки на хостах корпоративної IT-системи.

**1. Аналіз інформаційних процесів формування та застосування каналів управління.** Результат аналізу різних доступних джерел [1] - [10] про механізми проведення APT-атак та відповідні заходи захисту дозволяє стверджувати, що:

1) BD дозволяє зловмиснику реалізовувати план проведення атаки шляхом впровадження програм-агентів та віддаленого управління ними;

2) BD є базовим засобом реалізації APT-атаки;

3) переривання BD засобами захисту IT-системи може спровокувати запуск механізмів знищення інформаційних ресурсів, що пов’язано зі значним збитками;

4) детектування BD протягом часу перед цільовою акцією атаки та встановлення оперативного контролю за командами зловмисника дозволяє значно знизити відповідні ризики безпеки;

5) основою сучасних підходів проактивного захисту від APT-атак є застосування автоматизованих засобів SIEM, які визначають несанкціоновані дії шляхом збору інформації з журналів подій різних сенсорів безпеки IT-системи та порівнюють цю інформацію із шаблонами атак;

6) шаблон APT-атаки – це набір індикаторів (сигнатур) подій в системі, що визначені на основі закономірностей, які притаманні атаці. Закономірності визначаються на основі моделей APT;

7) більшість APT-атак – це атаки *0-day*, для яких характерна постійна зміна засобів і тактик. BD є постійною складовою більшості атак. Шаблон для BD може дозволити детектувати різні атаки.

**2. Вибір моделі APT-атаки.** Проведений аналіз різних моделей APT-атак на предмет їх використання для формування BD-шаблону показує, що більшість з них представлено у вигляді вербального опису цілей етапів атаки та загального сенсу механізмів їх досягнення [1] - [4]. Переваги таких моделей – вони виділяють загальні закономірності для різних атак. Загальний недолік – неможливість прямого застосування в SIEM через відсутність логічного зв'язку між описом подій в рамках етапів та відповідних індикаторів компрометації, які необхідно представляти у бітовому форматі.

Інша група моделей [5] - [7] описує атаку за допомогою різних математичних конструкцій (графи, логічні елементи, мурашиний алгоритм оптимізації, приховані Марківські процеси, піраміда атаки та інші). Переваги таких моделей – дозволяють уявити масштабні дії зловмисника у вигляді одного складного процесу. Загальний недолік – складно зв'язуються з технологічними процесами в корпоративному кіберсегменті [7].

За основу досліджень цієї роботи була прийнята кібернетична модель APT-атаки [8], [10]. В основі моделі є представлення дій зловмисника у вигляді кібернетичної системи (CyberSystem of APT, CSoA), об'єктом управління котрої є хост (хост – комп'ютер IP-мережі) зі складу IT-системи жертви, а суб'єктом управління – віддалений хост зловмисника. Поведінка CSoA може бути представлена послідовністю циклів управління (рис. 1).

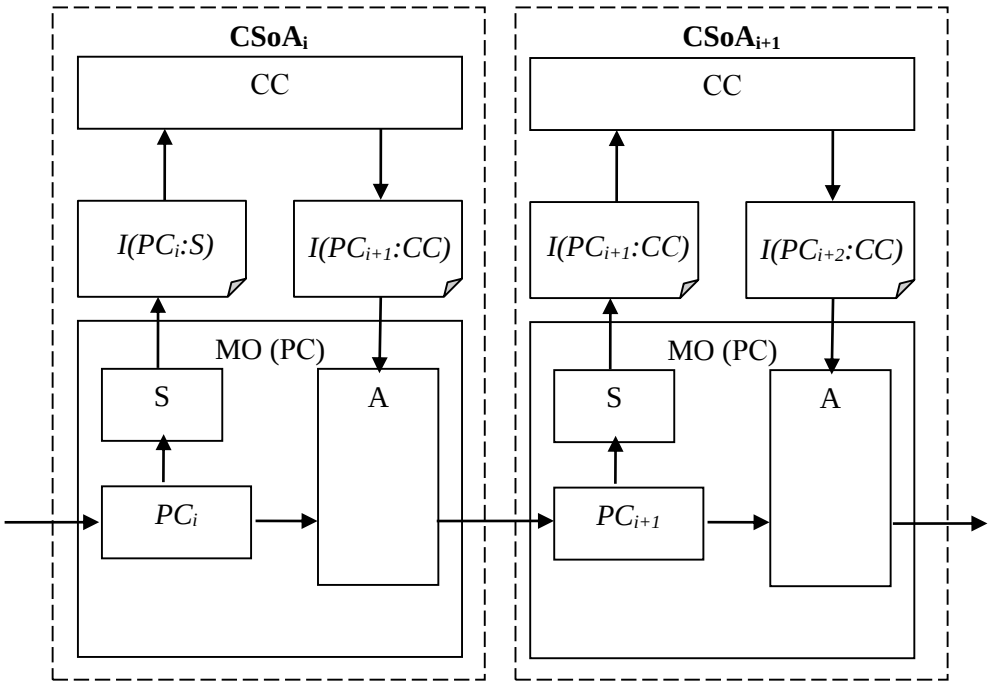


Рисунок 1 – Графічна модель кібернетичної системи APT-атаки

Персональний комп'ютер (PC), що входить до складу корпоративної мережі, виступає в ролі об'єкта управління (MO). Зловмисник і його комп'ютер представлені як центр керування (CC). $I(PC_i:S)$ – це інформація про стан $PC_i$ персонального комп'ютера в рамках актуальної (поточної) фази $CSoA_i$. Дана інформація сформована і направлена до CC сенсором S. На основі прийнятої інформації центр керування CC приймає рішення про переведення об'єкта керування MO в наступний стан $PC_{i+1}$ і оформлює це рішення в вигляді інформації

$I(PC_{i+1}:CC)$. Далі ця інформація пересилається до МО, де прийняте рішення реалізується за допомогою актуатора А: об'єкт управління переходить в наступний стан $PC_{i+1}$. Кожний $i$-й цикл управління $CSoA_{i+1}$ закінчується переходом в цикл $CSoA_{i+1}$ на основі виконання актуатором А команди $I(PC_{i+1}:CC)$.

Процес керування в рамках *CSoA* і поведінку самої *CSoA* (перехід з одного циклу в інший) може бути описаний наступною системою рівнянь:

$$\begin{cases} I(PC_{i+1}:CC)=F_{cc}[I(PC_i:S)]; \\ PC_{i+1}=F_A[PC_i, I(PC_{i+1}:CC)]. \end{cases} \quad (1)$$

де $PC_{i+1}$, $I(PC_i:S)$, $I(PC_{i+1}:CC)$, $PC_i$ – це кінцеві бітові множини;

$F_{cc}$ [.] – оператор відображення, який на основі прийнятої інформації і по заданому правилу прийняття рішення формує команду про перехід в інший стан;

$F_A$ [.] – це оператор відображення, який на підставі прийнятої команди переводить об'єкт керування з одного стану в інший.

Вся APT-атака за допомогою CSoA може бути представлена у вигляді наступної множини:

$$\boldsymbol{APT} = \{CSoA_i\},\ I = 1,\ldots,\ I. \quad (2)$$

де ***APT*** – це кінцева множина, що складається з кінцевих підмножин $CSoA_i$ (відповідних циклів управління кібернетичної системи атаки);

$CSoA_i = \{PC_i, I(PC_i:S), I(PC_{i+1}:CC)\}$ – підмножина, що складається з кінцевих бітових наборів (множин). Ці набори двох суміжних циклів *CSoA*, що пов'язані між собою системою рівнянь (1);

$i = 1,\ldots,I$ – номер поточного циклу *CSA*;

$I$ – кількість циклів атаки.

За допомогою такої формалізації вдалося представити APT-атаку у вигляді послідовності фаз кібернетичної системи атаки. Кожна фаза – це послідовність регулярно повторюваних дій, які можна назвати *процедурами атаки*. Часові межі кожної фази визначаються моментами встановлення нового стану об'єкта керування. Під новим станом слід розуміти або зміни в керованому комп'ютері, або перехід до іншого комп'ютера в мережі. Візуальним поясненням запропонованої моделі може бути структура на рис. 2.

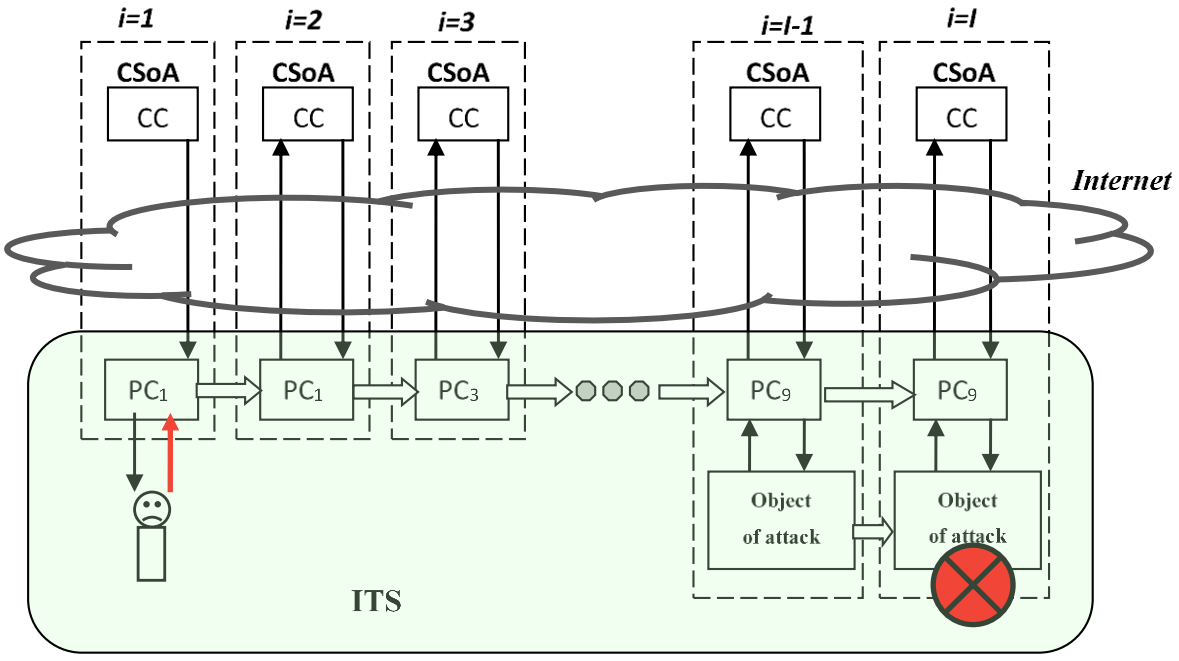


Рисунок 2 – Графічне представлення кібернетичної моделі APT-атаки

Кібернетична модель APT-атаки дозволяє:

– кожний етап вербальної моделі атаки представити у вигляді одного або декількох циклів кібернетичної системи;

– кожний цикл представити у вигляді конкретних інформаційних процесів (процедур атаки);

– кожній процедурі атаки поставити у відповідність бінарні набори, які відображають елементарні події в комп'ютерному середовищі. Ці події можуть бути зафіксовані комп'ютерними пристроями корпоративної IT-системи та представлені на обробку в SIEM;

– в рамках SIEM порівняти набори елементарних подій з шаблонами індикаторів компрометації. Ці шаблони формуються на основі характеристик IT-систем (склад, організація, топологія, інші) та визначеної політики безпеки.

**3. Розробка моделі поведінки BD.** В загальному випадку BD складається із наступних частин, що відповідають розглянутим процедурам CSoA:

1) програма-агент, що збирає та передає дані про стан хоста-жертви (англ. Sensor BD, SBD);

2) прямий канал BD (англ. Forward Link BD, FLBD), за допомогою якого повідомлення про стан хоста-жертви доставляється до хоста-зловмисника;

3) програма хоста-зловмисника, що приймає та представляє зловмиснику інформацію про стан хоста-жертви (англ. Control Center BD, CCBD);

4) зворотний канал BD (англ. Return Link BD, RLBD), за допомогою якого команди та повідомлення від зловмисника доставляються до хоста-жертви;

5) програма-агент, що приймає та виконує команди від хоста-зловмисника (англ. Actuator BD, ABD).

За допомогою вказаних складових можливо визначити структуру та модель поведінки BD (рис. 3).

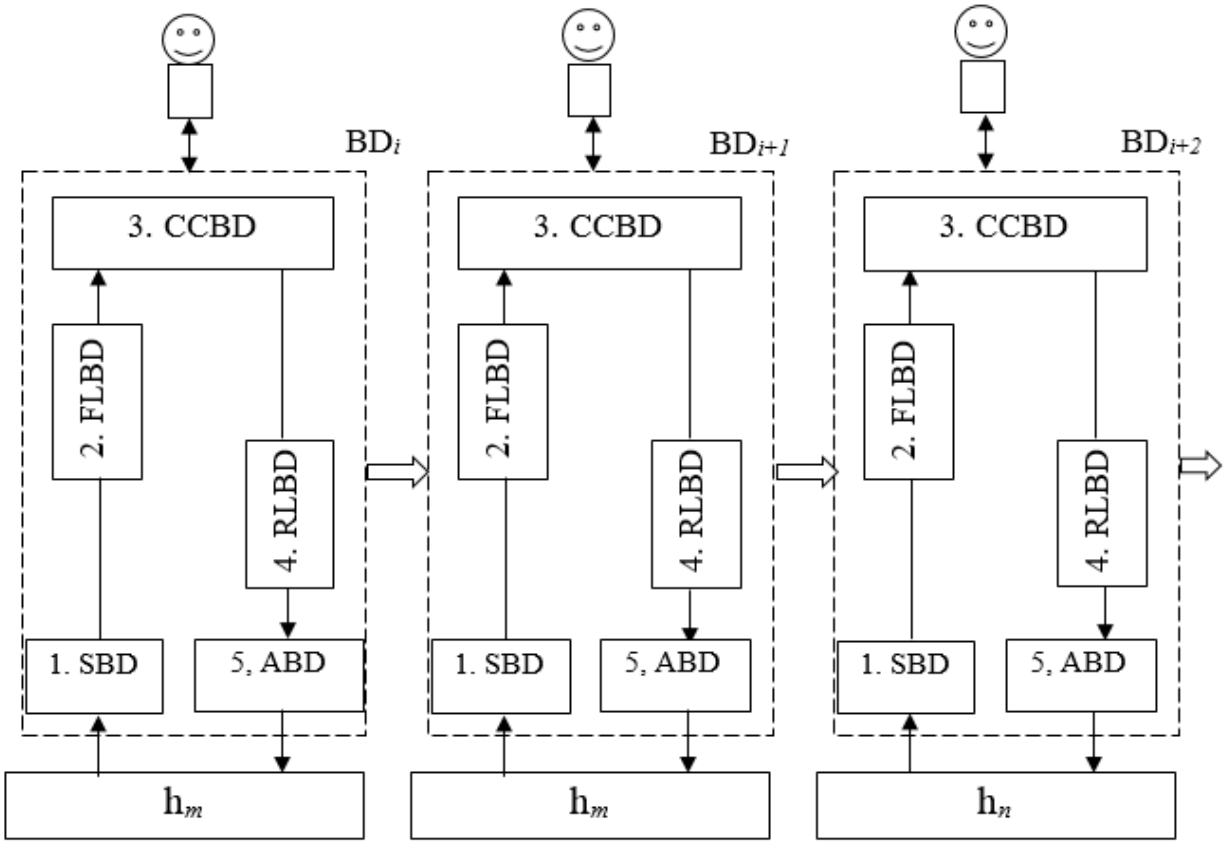


Рисунок 3 – Структура та модель поведінки BD в рамках APT-атаки

У рамках розробленої моделі поведінка BD в просторі корпоративного кіберсегменту реалізується у вигляді послідовності циклів з наступних процедур:

- формування сенсором SBD повідомлення зловмиснику про стан хоста (1);
- передача повідомлення через прямий канал FLBD (2);
- прийняття повідомлення CCBD, його аналіз зловмисником та прийняття рішення про подальші дії, формування CCBD команди для актуатора ABD (3);
- передача команди через зворотний канал RLBD (4);
- прийом команди актуатором ABD та її реалізація.

**4. Визначення відповідності процедур управління в рамках BD та елементарних подій ITS.** Процедури (англ. *procedure, Pr*) (1) - (5) виконуються циклічно в рамках визначеної послідовності, але з різною протяжністю відповідного часового періоду (період циклу, $T_i$). Закінчення періоду циклу визначається моментом часу, що відповідає припиненню виконання останньої команди від зловмисника. Кожний цикл $BD_i$ пов'язаний із конкретним хостом (англ. *host, h*) корпоративної IT-системи. Зловмисник може виконувати один або декілька циклів на одному хості, а потім продовжувати використовувати BD відносно іншого хосту. Якщо кожну процедуру циклу *Pr* пов'язати з якоюсь бітовою послідовність (сигнатура, англ. *signature, Sign*), то з'являється можливість відстежувати за допомогою засобів SIEM за часом та кіберпростором IT-системи. Можливо розглядати наступні види елементарних подій (об'єктів) в корпоративному кіберсегменті:

1) обчислювальні процеси на хостах (процес, англ. *process, Prs*);
2) послідовність даних, якими обмінюються обчислювальні процеси різних хостів за допомогою мережі (трафік, англ. *traffic, Trc*);
3) файли даних, які формуються процесами та зберігаються на носіях.

З одного боку кожна елементарна подія пов'язана із набором індивідуальних характеристик конкретного хоста корпоративної комп'ютерної мережі. Наприклад, кожний трафік пов'язаний із просторовими характеристиками мережі: IP-адреса, MAC-адреса, *domen name*. Також трафік пов'язаний із видом транспортного протоколу (TCP або UDP) і конкретним обчислювальним процесом (через номер IP-порта). Кожний обчислювальний процес також пов'язаний із рядом характеристик: образ виконуваного машинного коду; пам'ять (зазвичай деяка область віртуальної пам'яті) і її стан; стан стеку викликів; дескриптори ресурсів операційної системи; файлові дескриптори; набір повноважень процесу (допустимі операції); стан процесору (контекст процесору) та інші характеристики. Операційна система зберігає більшу частину інформації про процеси в таблиці процесів.

Структура та модель поведінки BD (рис. 3) дозволяє кожній процедурі (1) - (5) поставити у відповідність наступні елементарні події (табл. 1), що можуть бути детектуванні сенсорами безпеки IT-системи.

Таблиця 1 – Відповідність процедур циклу BD, елементарних подій ITS та індикаторів компрометації для BD

| Компонента моделі BD | Процедура циклу, *Pr* | Елементарна подія ITS | Назва індикатору компрометації, IoC | Змінне значення IoC |
|---|---|---|---|---|
| SBD | *Pr1* | 1) вихідний трафік хоста, $Trc_1$<br>2) процес хоста, $Prs_1$ | $Sign(Trc_1)$<br>$Sign(Prs_1)$ | $x_{1\text{-}1}$<br>$x_{1\text{-}2}$ |
| FLBD | *Pr2* | вихідний трафік ITS, $Trc_2$ | $Sign(Trc_2)$ | $x_2$ |
| CCBD | *Pr3* | вихідний трафік хоста зловмисника, $Trc_3$ | $Sign(Trc_3)$ | $x_3$ |
| RLBD | *Pr4* | вхідний трафік ITS, $Trc_4$ | $Sign(Trc_4)$ | $x_4$ |
| ABD | *Pr5* | 1) вхідний трафік хоста, $Trc_5$<br>2) процес хоста, $Prs_5$ | $Sign(Trc_5)$<br>$Sign(Prs_5)$ | $x_5$ |
| h | *Pr6* | процес хоста, що активований BD, $Prs_6$ | $Sign(Prs_6)$ | $x_6$ |
| … | | … | … | … |

Табл. 1 може бути розширена за допомогою додаткових знань про політику застосування BD. Наприклад, за допомогою BD зловмисник доставляє шкідливу програму, а потім на її основі активує шкідливий процес $Prs_6$. Ця процедура не є циклічною (в табл.1 – *Pr6*). Якщо за допомогою SIEM в рамках циклу $BD_i$ буде визначено зв'язок між цими подіями, то для наступного циклу $BD_{i+1}$ можливо сформувати додаткові індикатори компрометації (IoC): $Sign(Prs_6)$, $Sign(Trc_5)$.

**5. Розроблення способу формування шаблону для визначення BD атаки.** Запропонована модель BD та підхід до відповідності процедур циклу BD елементарним подіям в IT-системі (табл. 1) дозволяють розробити наступну структуру шаблону для детектування BD (табл. 2). Структура розроблялася для IT-системи, що має локальну корпоративну мережу з підключенням до ресурсів Інтернет через роутер периметру *R* та фаєрвол нового покоління *NGFW*.

Таблиця 2 – Структура шаблону для детектування BD

| Компонента IT-системи | Цикли BD | | | | | | |
|---|---|---|---|---|---|---|---|
| | $BD_{i=1}$ | | $BD_{i=2}$ | | | $BD_{i=I}$ | |
| | $IoC_{i=1}$ | Мітка про детектування (МД) | $IoC_{i=2}$ | МД | | $IoC_{i=I}$ | МД |
| *NGFW* | $Sign(Trc_{3,\,inp})$<br>$Sign(Trc_{3,\,out})$ | + | $Sign(Trc_{3,\,inp})$<br>$Sign(Trc_{3,\,out})$ | +<br>+ | | $Sign(Trc_{3,\,inp})$<br>$Sign(Trc_{3,\,out})$ | +<br>+ |
| $h_{m=1}$ | $Sign(Trc_1)$ | + | $Sign(Trc_1)$ | | … | $Sign(Trc_1)$ | |
| | $Sign(Prs_1)$ | + | $Sign(Prs_1)$ | | | $Sign(Prs_1)$ | |
| | $Sign(Trc_5)$ | + | $Sign(Trc_5)$ | | | $Sign(Trc_5)$ | |
| | $Sign(Prs_5)$ | + | $Sign(Prs_5)$ | | | $Sign(Prs_5)$ | |
| | | | $Sign(Prs_6)$ | | | $Sign(Prs_6)$ | |
| | … | | | | | | |
| $h_{m=2}$ | $Sign(Trc_1)$ | | $Sign(Trc_1)$ | + | | $Sign(Trc_1)$ | |
| | $Sign(Prs_1)$ | | $Sign(Prs_1)$ | + | | $Sign(Prs_1)$ | |
| | $Sign(Trc_5)$ | | $Sign(Trc_5)$ | + | | $Sign(Trc_5)$ | |
| | $Sign(Prs_5)$ | | $Sign(Prs_5)$ | + | | $Sign(Prs_5)$ | |
| | | | $Sign(Prs_6)$ | | | $Sign(Prs_6)$ | |
| | … | | | | | | |
| … | | | | | … | | |
| $h_{m=M}$ | $Sign(Trc_1)$ | | $Sign(Trc_1)$ | | | $Sign(Trc_1)$ | + |
| | $Sign(Prs_1)$ | | $Sign(Prs_1)$ | | | $Sign(Prs_1)$ | + |
| | $Sign(Trc_5)$ | | $Sign(Trc_5)$ | | | $Sign(Trc_5)$ | + |
| | $Sign(Prs_5)$ | | $Sign(Prs_5)$ | | | $Sign(Prs_5)$ | + |
| | | | | | | $Sign(Prs_5)$ | |
| | … | | | | | | |

Ця структура шаблону (СШ) об'єднує індикатори компрометації таким чином, що дозволяє відслідковувати поведінку BD за часом (номер циклу процедур управління $I = 1, \ldots, I$) та простором ITS (фаєрвол *NGFW* та хости $h_m$, $m = 1, \ldots, M$). СШ дозволяє використовувати різни політики детектування BD (ПД). Розглянемо одну з цих ПД (ПД-1):

1) *NGFW* фіксує вхідний трафік $Trc_{3,\,inp}$ та вихідний трафік $Trc_{3,\,out}$;
2) формується припущення, що це перший цикл керування $BD_{i=1}$;
3) формуються наступні значення IoC:

$$Sign(Trc_{3,inp}) = (IP\text{-}адреса,\ IP\text{-}порт);$$

4) на $h_m$, що визначений за *IP-адресою* $Sign(Trc_{3,inp})$, визначається новий $Prs_1$, що пов'язаний з обміном даних через *IP-портом* $Sign(Trc_{3,inp})$;

5) сформовані $Sign(Trc_{3,inp})$, $Sign(Trc_{3,out})$, $Sign(Prs_1)$ використовуються для визначення наступних циклів керування (на цьому, або іншому хості);

6) за мітками детектування відстежується траєкторія поведінки BD.

Для ситуації коли СШ пов'язується з декількома траєкторіями BD (одна – істинна, а інші – помилкові), то рішення приймається на основі порівняння ваг цих траєкторій.

**6. Основні етапи способу визначення каналу керування.** Розроблені модель поведінки BD та спосіб формування шаблону дозволяють сформувати основні етапи визначення каналу керування APT-атакою.

6.1. Формування структури шаблону для IT-системи. За результатами ідентифікації корпоративних апаратних та програмних засобів, зовнішніх IP-трафіків (функція "Ідентифікація ризиків кібербезпеки", категорії ID.AM, ID.BE, ID.GV [12]) визначається розмірність та структура шаблону.

6.2. Визначення індикаторів BD. На основі прийнятої політики кібербезпеки визначаються ознаки пар IP-трафіків (пара – вхідний трафік + вихідний трафік з однаковими сокетами) та обчислювальних процесів, що не відповідають її правилам.

6.3. Налаштування мережевих та хостових IDS. Для всіх IDS на основі індикаторів BD формуються правила визначення подій безпеки.

6.4. Збір інформації про події безпеки. При визначені подій безпеки (п. 6.2) корпоративні IDS формують та направляють інформацію про ці події на хост, де розміщений шаблон BD. Інформація про подію зберігається у комірці шаблону відповідної IDS. Наступна інформація, що пов'язана з іншим хостом, зберігається у новому рядку шаблону (зміна циклу $BD_i$).

6.5. Формування гіпотези про BD. За результатами аналізу шаблону з інформацією про події безпеки формується гіпотеза про наявність BD, що має відповідну зовнішню IP-адресу (адреси).

6.6. Підтвердження гіпотези. Подальший збір інформації про наступні події безпеки з попередньо зафіксованими значеннями параметрів дозволяє підтвердити гіпотезу та відстежувати траєкторію поведінки BD.

Працездатність запропонованого способу було перевірено за допомогою обладнання навчального ситуаційного центру з кібербезпеки Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського". До складу макету корпоративної IT-системи було включено: фізичний роутер периметру; фізичний фаєрвол FortiGate 60E; фізичний комутатор; чотири корпоративні віртуальні хости. З віртуального хоста зловмисника засобами ОС Kali Linux шляхом впровадження Reverse Shell через було встановлено канал керування корпоративним хостом. В якості сенсорів безпеки використовувались FortiGate 60E (мережевий IDS) та розроблене програмне забезпечення (ПЗ), що дозволяє визначати події безпеки на хостах корпоративної IT-системи (хостові IDS). Збір даних проводився в автоматизованому режимі. Аналіз інформації шаблону проводився оператором.

**Висновки.** Основою багатьох APT-атак є використання зловмисником несанкціонованих каналів керування атакою через Інтернет, що дозволяють йому виконувати різні дії в корпоративному сегменті кіберпростору. Актуальним стає завдання своєчасного визначення BD ще на етапі підготовки цільової акції атаки. Такий підхід відповідає реалізації проактивної стратегії кіберзахисту.

За результатами досліджень інформаційних процесів формування та використання каналу керування атакою, організації процесів систем проактивного кіберзахисту в рамках досліджень було розроблено спосіб визначення каналу керування APT-атакою. В основі способу:

– раніше розроблена кібернетична моделі APT-атаки [8], що дозволяє представити поведінку зловмисника у вигляді циклічних цифрових подій комп'ютерної системи. Кожна така подія може бути детектована комп'ютерними засобами;

– розроблена в рамках досліджень кібернетична модель BD, що дозволяє представити дії зловмисника по використанню цього каналу керування атакою у вигляді повторюваних циклів з п’яти процедур. Більшість цих процедур можливо фіксувати за допомогою мережевих та хостових IDS;

– розроблена структура багатоіндикаторного шаблону, що дозволяє в рамках SIEM фіксувати та аналізувати інформацію про події безпеки за простором та часом корпоративної інформаційної системи.

Розроблений спосіб складається з наступних основних етапів:

1) формування структури багатоіндикаторного шаблону на основі конкретних характеристик корпоративної IT-системи;
2) визначення індикаторів каналу керування;
3) налаштування мережевих і хостових IDS відповідно до структури шаблону та визначених індикаторів;
4) збір інформації про події безпеки за простором та часом IT-системи;
5) аналіз інформації щаблону та формування гіпотези про наявність каналу керування;
6) подальший збір та аналіз інформації в рамках підтвердження гіпотези;
7) в разі підтвердження гіпотези – відслідковування поведінки зловмисника.

Для перевірки способу розроблено програмний засіб, що на основі аналізу хостових трафіків детектував події безпеки (функції хостового IDS). Працездатність способу перевірено за допомогою комп’ютерного макету: фізичний роутер периметру (файєрвол FortiGate 60E, функції мережевого IDS), чотири віртуальні хости інформаційної системи із хостовими IDS, віртуальний хост зловмисника з засобами ОС Kali Linux, канал керування на основі Reverse Shell. Збір даних проводився в автоматизованому режимі. Аналіз інформації шаблону проводився оператором.

Теоретичні та практичні результати досліджень орієнтовані на застосування у складі SOC корпоративної IT-системи в рамках проактивного захисту від APT-атак.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] P. Chen, L. Desmet, and C. Huygens, “A study on Advanced Persistent Threats”, in *Proc. 15th IFIP TC 6/TC 11 International on Conference Communications and Multimedia Security*, Aveiro, Portugal, 2014, pp. 63-72, doi: https://doi.org/10.1007/978-3-662-44885-4_5.

[2] E. M. Hutchins, M. J. Clopperty, and R. M. Amin, Intelligence-Driven Computer Network Defense. Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2009. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed on: Aug. 10, 2021.

[3] Mandiant M-Trends: The Advanced Persistent Threat. Mandiant, 2010. [Online]. Available: https://wikileaks.org/hbgary-emails//fileid/27714/8307. Accessed on: Aug. 10, 2021.

[4] J. Navarro, et al. ICube. HuMa: A multi-layer framework for threat analysis in a heterogeneous log environment, Université de Strasbourg, France, ECAM Strasbourg-Europe, Schiltigheim, France, 2015. [Online]. Available: http://fps2017.loria.fr/wp-content/uploads/2017/10/08.pdf. Accessed on: Aug. 10, 2021.

[5] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, “Time-dependent analysis of attacks”. *Principles of Security and Trust, Lecture Notes in Computer Scienc*e, vol. 8414, pp. 285-305, doi: https://doi.org/10.1007/978-3-642-54792-8_16.

[6] S. Camtepe, and B. Yener, “Modeling and detection of complex attacks”, in Proc. *Third International Conference on Security and Privacy in Communications Networks and the Workshops – SecureComm 2007*, Nice, France, 2007, pp. 234-243, doi: https://doi.org/10.1109/SECCOM.2007.4550338.

[7] O. Flåten, and M. S. Lund, “How good are attack trees for modelling advanced cyber threats?”, in *Proc. Norwegian Information Security Conference*, Fredrikstad, Norway, 2014. [Online]. Available: http://ojs.bibsys.no/index.php/NISK/article/view/105. Accessed on: Aug. 10, 2021.

[8] І. Яковів, "Кібернетична модель APT атаки", *Information Technology and Security*, vol. 6, iss. 1, pp. 46-58, January – June 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.1.153140.

[9] D. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", in *Proc. 70th Annual Conference for Protective Relay Engineers*. 2017. [Online]. Available: https://doi.org/10.1109/CPRE.2017.8090056. Accessed on: Aug. 10, 2021.

[10] И. Яковив, "Базовая модель информационных процессов управления и критерии безопасности кибернетической системы", *Information Technology and Security*, vol. 3, iss.1, pp. 68-74, January – June 2015, doi: https://doi.org/10.20535/2411-1031.2015.3.1.57735.

[11] I. Yakoviv. "Basic model of information processes and behavior of a cyber defense system", *Information technology and security*, vol. 7, iss. 2, pp. 183-196, July – December 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190568.

[12] Cybersecurity Framework Version 1.1. (April 2018). [Online]. Available: https://www.nist.gov/cyberframework/framework. Accessed on: Aug. 10, 2021.

Стаття надійшла до редакції 06.09.2021.

## REFERENCE

[1] P. Chen, L. Desmet, and C. Huygens, "A study on Advanced Persistent Threats", in *Proc. 15th IFIP TC 6/TC 11 International on Conference Communications and Multimedia Security*, Aveiro, Portugal, 2014, pp. 63-72, doi: https://doi.org/10.1007/978-3-662-44885-4_5.

[2] E. M. Hutchins, M. J. Clopperty, and R. M. Amin, Intelligence-Driven Computer Network Defense. Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2009. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed on: Aug. 10, 2021.

[3] Mandiant M-Trends: The Advanced Persistent Threat. Mandiant, 2010. [Online]. Available: https://wikileaks.org/hbgary-emails//fileid/27714/8307. Accessed on: Aug. 10, 2021.

[4] J. Navarro, et al. ICube. HuMa: A multi-layer framework for threat analysis in a heterogeneous log environment, Université de Strasbourg, France, ECAM Strasbourg-Europe, Schiltigheim, France, 2015. [Online]. Available: http://fps2017.loria.fr/wp-content/uploads/2017/10/08.pdf. Accessed on: Aug. 10, 2021.

[5] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, "Time-dependent analysis of attacks". *Principles of Security and Trust, Lecture Notes in Computer Scienc*e, vol. 8414, pp. 285-305, doi: https://doi.org/10.1007/978-3-642-54792-8_16.

[6] S. Camtepe, and B. Yener, "Modeling and detection of complex attacks", in Proc. *Third International Conference on Security and Privacy in Communications Networks and the Workshops – SecureComm 2007*, Nice, France, 2007, pp. 234-243, doi: https://doi.org/10.1109/SECCOM.2007.4550338.

[7] O. Flåten, and M. S. Lund, "How good are attack trees for modelling advanced cyber threats?", in *Proc. Norwegian Information Security Conference*, Fredrikstad, Norway, 2014. [Online]. Available: http://ojs.bibsys.no/index.php/NISK/article/view/105. Accessed on: Aug. 10, 2021.

[8] I. Yakoviv, "Cybernetic model of the Advanced Persistent Threat", *Information Technology and Security*, vol. 6, iss. 1, pp. 46-58, January – June 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.1.153140.

[9] D. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", in *Proc. 70th Annual Conference for Protective Relay Engineers*. 2017. [Online]. Available: https://doi.org/10.1109/CPRE.2017.8090056. Accessed on: Aug. 10, 2021.

[10] I. Yakoviv, “The base model of informational processes of management and safety criteria for cybernetic systems”, *Information Technology and Security*, vol. 3, iss.1, pp. 68-74, January – June 2015, doi: https://doi.org/10.20535/2411-1031.2015.3.1.57735.
[11] I. Yakoviv. “Basic model of information processes and behavior of a cyber defense system”, *Information technology and security*, vol. 7, iss. 2, pp. 183-196, July – December 2019, doi: https://doi.org/10.20535/2411-1031.2019.7.2.190568.
[12] Cybersecurity Framework Version 1.1. (April 2018). [Online]. Available: https://www.nist.gov/cyberframework/framework. Accessed on: Aug. 10, 2021.

IHOR YAKOVIV,
ANDRIY TROKHYMENKO,
KYRYLO GLUM

**WAY OF DETERMINING APT CONTROL CHANNEL**

The widespread use of sophisticated cyber attacks against the national critical infrastructure of the APT type has been a powerful stimulus for the development of proactive cyber defense techniques. APTs are characterized by the following features: an attack is a complex set of time and space-related actions of an attacker. Separately, these actions may not arouse suspicion; the target attack action in the cyber segment of the object is prepared for a long time (from several months to a year or more); the set of actions of the attacker is a chain of tactics, the implementation of which allows to achieve the goal of the attack. Despite the variety of tools used in ARTs, the set of most tactics and their nature remain constant. The basis of many APTs is that the attacker uses unauthorized channels to control the attack via the Internet, which allows him to perform various actions in the cyberspace segment of the victim's information technology system. The task of timely identification of such channels at the stages of preparation of the target action of attack is urgent. This approach is in line with the implementation of a proactive cybersecurity strategy. Based on the results of research of information processes of formation and use of unauthorized channel, organization of processes of proactive cyber defense systems, a method of determining the control channel of APT has been developed. It can be used in the management of information and security events SIEM to determine the attack after its stage of penetration into the information technology system, but before the implementation of the stage of the target action. The method is developed on the basis of using the cybernetic model of APT using the methods of formalized analysis of information processes of modern operational cyber defense systems. As part of the research, a procedure for the formation and use of a multi-indicator template of the control channel, which is used for a comprehensive analysis of security events, was developed. To fill in the template, a software has been developed that generates information about security events on the hosts of the corporate system. Theoretical and practical results of research are focused on the use of corporate information system for proactive protection against APTs.

**Key words:** cyber defense system, proactive strategy, SIEM, SOC, APT detection, unauthorized channel, backdoor, target attack action.

**Яковів Ігор Богданович**, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування автоматизованих інформаційних систем і технологій, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0000-0001-7432-898X, iyakov52@gmail.com.

**Трохименко Андрій Олександрович**, магістрант, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0000-0001-8175-096X, trohimuch11@gmail.com.

**Глум Кирило Дмитрович**, бакалавр, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-8658-5366, glum.kiril@gmail.com.

**Yakoviv Ihor**, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

**Trokhimenko Andriy,** master's student, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

**Hlum Kyrylo,** bachelor's student, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.