УДК 004.056.53
DOI: 10.15587/1729-4061.2021.225646

Розробка методу захисту від атак нульового дня на базі аналітичної моделі зміни станів мережевої пісочниці

С. С. Бучик, О. К. Юдін, І. Д. Бондаренко, Р. В. Зюбіна, О. О. Супрун

Представлено метод захисту від атак нульового дня з використанням технології пісочниць на основі розробленої аналітичної моделі з ймовірнісним ранжуванням станів інформаційної системи. В моделі враховано умови апріорної невизначеності щодо параметрів потоку деструктивного впливу на систему з врахуванням типових процедур мережевої пісочниці.

Запропонована модель станів інформаційної системи дозволяє аналізувати та відслідковувати всі можливі стани та оцінювати рівень безпеки в цих станах, та ймовірності переходів до них. Таким чином, можливо виявити найбільш небезпечні, та відслідкувати активності, що стали причиною відповідних змін. Принципова відмінність даної моделі від стандартних підходів полягає в вагових коефіцієнтах, що характеризують не інтенсивність виникнення випадкових подій, а інтенсивність переходів між станами.

Для безпосередньої реалізації та застосування запропонованої аналітичної моделі використано технології багаторівневих мережевих "пісочниць".

Відмінність від інших популярних антивірусних засобів полягає у використанні апріорної математичної оцінки загроз, що дозволяє виявити впливи, що не розглядаються як загрози класичними системами до моменту нанесення шкоди системі.

Поєднання зі стандартними засобами захисту дозволяє окремо аналізувати файли, які є занадто великими за розміром, чи надходять до системи не через загальний шлюз, що контролюється мережевою "пісочницею", а з зовнішніх носіїв кінцевих користувачів.

Впровадження розробленої аналітичної моделі дозволило покращити рівень захисту корпоративної мережі на 15 *%, відповідно до кількості виявлених загроз. Така різниця пояснюється нездатністю класичних програм виявити нові загрози, якщо вони ще не занесені до бази програми, та їх активність не є тривіальною.*

Ключові слова: атака нульового дня, аналітична модель, ранжування станів, мережева пісочниця, захист інформації.

1. Вступ

Сучасний стан розвитку інформаційного суспільства вимагає захисту інформаційних ресурсів та критичних даних на найвищому рівні. Безпрецедентні вимоги до програмно-апаратних засобів, технологій організації сучасних інфраструктур, тощо характеризуються різким зростанням попиту державних та сус-

пільних відносин в використанні системи надання надійних і якісних ІТ послуг (послуг інформаційних технологій) різних класів.

Зростання кількості та рівня складності різноманітних ІТ послуг, підвищення технологічного рівня кібернетичних атак на державні і суспільні інформаційні ресурси формують нові завдання для системи виявлення і попередження інцидентів.

Клас кібернетичних атак «0 дня» один з найяскравіших прикладів використання розвинених інформаційних технологій з метою порушення властивостей інформаційної системи та втрати відповідних ресурсів.

Антивірусна пісочниця – це рішення для захисту кінцевих пристроїв, яке дозволяє запобігти загрозам і атакам, пов'язаними з використанням критичних даних в інтегрованих інфраструктурах, хмарному середовищі, тощо з умови горизонтального поширенням атаки в інформаційно-комунікаційних мережах [1].

Метод захисту від атак нульового дня за допомогою технології «пісочниця» у корпоративних мережах базується на методах корпоративної (мережної) або антивірусної пісочниці. Антивірусна пісочниця дає змогу емулювати файли великих розмірів на кінцевих станціях не навантажуючи мережевий екран та мережеву пісочницю.

Захист від цілеспрямованих атак невизначеного класу залишається одним із найбільш актуальних питань у сфері інформаційної безпеки. Протягом останнього року кількість кібератак в Україні збільшилася в десять разів. Майже кожен знайомий з такими виразами: «таргетована (цільова) атака», «вразливість нульового дня», «0-day» або навіть Advanced Persistant Threats (ATP). Дані теми можна сміливо назвати головним трендом в сфері інформаційної безпеки. Добре відомі атаки з шифруванням є одним з підвидів перерахованих загроз. «Пісочниці» (SandBox) – це єдині засоби, які дозволяють боротися з вище згаданими загрозами [2].

Такі засоби захисту проводять динамічний і статистичний аналіз файлів у віртуальному середовищі і блокують різноманітні атаки при необхідності [3, 4].

Це дозволяє оцінити поведінку підозрілих файлів і наслідки запуску таких файлів. При цьому головна мета не на виявлення шкідливого коду за допомогою сигнатур, а на оцінку дій, які виконуються кодом, безпеку і коректність в даному середовищі.

На даний момент ринок рішень по виявленню і протидії цільовим атакам знаходиться лише на стадії становлення. Виробники пропонують широкий спектр засобів захисту, але часто такі товари робляться задля маркетингу і не відображають реальної ефективності рішень. Проте, серед існуючих на ринку засобів захисту одним з найефективніших рішень є «пісочниці» (SandBox).

Атаки нульового дня є серйозною загрозою безпеки інфраструктури практично кожної організації. Традиційний набір засобів захисту інформації не здатний протистояти не визначеним класам загроз. Технологія «пісочниця» є найефективнішим механізмом виявлення загроз нульового дня.

2. Аналіз літературних даних та постановка проблеми

Забезпечення захищеності даних в комп'ютерних системах різних масштабів, та належного рівня функціонування таких систем загалом, є одним з найголовніших питань в сфері ІТ. Проте, зі стрімким ростом галузі, також змінюються і підходи та інструменти до отримання несанкціонованого доступу, основні інструменти показано та проаналізовано в роботі [5]. Це вимагає постійне вдосконалення наявних методів захисту та створення нових підходів. Одним з найяскравіших прикладів нових методів є створення антивірусної системи, що імітує імунну систему живих організмів. Така система розроблена та описана в [6], вона дозволяє виявляти нетривіальні загрози та усувати їх, але потребує значних затрат ресурсів.

Слід зазначити, що в сфері захисту даних та інформаційних систем в цілому, недостатньо лише реагувати на наявні загрози, але необхідно їх попереджати. Це ускладнюється тим, що віруси досить часто адаптуються до наявних систем, тому і системи захисту повинні без втручання людини виявляти нові загрози. Один з перших підходів до створення адаптивної системи продемонстровано в [7], проте описаний підхід все ж не здатний розпізнати спеціалізовані замасковані атаки. Також, разом зі стрімким розвитком інформаційного суспільства та збільшенням кількості даних, що необхідно перевіряти, зростають і вимоги до апаратних компонентів систем захисту, аналіз основних загроз проведено в [8]. Одним з варіантів вирішення проблеми нестачі ресурсів та часу при забезпеченні безпеки є використання методів штучного інтелекту, наприклад нейронних мереж, що було вперше запропоновано ще в минулому столітті. В статті [9] представлено розроблений метод, проте вказано такі недоліки, як залежність від якості процесу навчання мережі та мала ефективність з використанням непідготовлених даних.

В той же час, разом з ростом складності інформаційних систем, змінюється і поняття порушника в даному контексті. Це ставить нові вимоги перед існуючими системами. Наприклад, ціллю зловмисника все частіше стає не руйнування системи чи заподіяння прямої шкоди, а отримання доступу до персональних чи статистичних даних. Це може бути несуттєвим на перший погляд, але може мати значні наслідки. В [10] показано, як використання інформації з соціальних мереж може нанести значної шкоди, та запропоновано метод захисту. Недоліком згаданого методу є повільність його роботи. Також порівняно новим є поняття «0 дня», але проблема, описана в [11], є однією з найактуальніших на даний момент. Виявлення таких атак вимагає впровадження інноваційних методологій, наприклад системи пасток, описаної в [12], чи технології "горщиків меду". В [13] описано роботу такого методу, він є досить ефективним при наявності інформації про майбутні атаки, але неактуальний при повній невизначеності.

Також відносно новими є методи "пісочниць", реалізовані в більшості відомих антивірусних програм, наприклад, це Check Point для антивірусів ESET та AvastSandbox для систем AVAST. Подібна технологія являє собою сукупність двох ключових компонентів: SandBlast та Threat Emulation – компоненти, які є новим видом організації «пісочниці» [14, 15], що дозволяють емулювати ймовірні атаки та відповідно прогнозувати захист системи.

Виявлення атак здійснюється на двох рівнях архітектури: рівні операційної системи (OS level) – як і у традиційних «пісочниць», і на рівні центрального процесора (CPU level) [16]; SandBlast Threat Extraction – компонент, що дозволяє проаналізувати файли, які передаються по мережі, видалити з них весь небезпечний вміст, реконструювати файли і надати ці файли користувачеві вже чистими.

Наприклад, ESET Dynamic Threat Defence (EDTD) [17] забезпечує ще один рівень безпеки, використовуючи перехідні технології ESET для виявлення нових загроз [14]. Якщо антивірус розпізнає шкідливий код, він запобігає подальшій активності загроз, тим самим утримуючи в карантинній зоні. За аналогічним принципом працюють і інші антивірусні системи, такі як Avast чи NOD32.

Саме через неможливість впровадження єдиних стандартів та еталонів щодо великого різноманіття існуючих інформаційних систем, необхідно створити загальну модель, що здатна адаптуватися до реального стану. Це досягається впровадженням математичного базису виявлення загроз. На основі моделі і буде впроваджено метод захисту.

3. Мета і задачі дослідження

Метою дослідження є створення методу захисту інформаційної системи від атак «0 дня», що буде використовувати ймовірнісні ранжування станів даної системи в умовах невизначеності.

Для досягнення мети були поставлені наступні завдання:

– розробити аналітичну модель станів системи з ймовірнісним ранжуванням переходів в умовах апріорної невизначеності до параметрів потоку деструктивного впливу, та врахуванням динамічних змін функціоналу системи в часі;

– розробити схему реалізації аналітичної моделі з використанням синтезованої мережевої та антивірусної пісочниці;

– провести тестування запропонованої схеми реалізації моделі з використанням пісочниць.

4. Матеріали та методи дослідження

Враховуючи характерні відмінності атак «0 дня», а також з метою синтезу нового методу виявлення загроз цього класу на тлі мережевої пісочниці, необхідно сформувати математичну модель методу на базі багатоальтернативного підходу до кількості можливих типів атак. Зазначений підхід характеризується тим що сторона, яка є ціллю атаки, не має апріорних даних про тип, параметри та час здійснення атаки на критичні дані власника інформаційних ресурсів.

В даному випадку процес визначення класу атаки повинен проходити в умовах апріорної нестатистичної невизначеності щодо параметрів та станів деструктивного впливу на інформаційну систему з урахуванням типових процедур мережевої пісочниці. Аналітична модель повинна формуватись в контексти відсутності попередніх ймовірностей про тип і стан функції впливу, а також апріорної невизначеності станів стосовно самої системи на яку спрямований деструктивні впливи.

Таким чином, загальний підхід до моделювання загрози на інформаційні ресурси [17] будемо розглядати в контексті побудованої моделі аналітичного ряду. При цьому слід враховувати дискретні стани та безперервний час імовірнісного ранжування вхідних потоків з метою розрахунку необхідних параметрів та характеристик функції впливу (загрози). З метою коректності та спрощення аналітичного представлення, використаємо функціональний ряд з врахуванням динамічної послідовності випадкових станів (потік подій), що виникають у системі з урахуванням вразливостей інформаційних ресурсів. Враховуючи особливості класу атак «нульового дня», оберемо експонентний розподіл часу нагнітання частоти загроз процедури здійснення атаки через вразливості системи [18].

Оскільки моделюється серія загроз, в формуванні аналітичної моделі доцільно враховувати послідовність вразливостей інформаційної системи (або ресурсів), які використовуються порушником. Відмінність проблематики формування моделі для атак «нульового дня» полягає в тому, що в аналітичній моделі ряду не буде враховуватись кореляційний взаємозв'язок між загрозою та відповідною вразливістю. Зазначені обмеження обґрунтовані ще тим, що розроблювана модель буде додатково ускладнена набором взаємозв'язків вразливостей критичних даних до невизначеного класу атак. Таким чином, встановлено відмінність від типових критеріїв опису загроз – апріорно невідомі тип та параметри атаки, не відомо на яку вразливість буде спрямована загроза за динамікою часу. Також треба врахувати, що апріорно інформаційна система вважається захищенню з визначеним рівнем гарантій та ризик вразливості ресурсів зведений до мінімуму.

Введемо обґрунтоване припущення, що інцидент створюється двома класами відповідних параметрів несанкціонованого впливу на інформаційну систему. Ці параметри наступні: за інтенсивністю впливу загроз різного класу за часом, а також на основі помилок реалізації програмних засобів при виявленні інцидентів й усуненні вразливостей. Згідно визначеного підходу можна сформувати аналітичну модель системної функції визначення процедури виявлення інцидентів будь-якої складності.

Для безпосередньо реалізації методу захисту та імплементації запропонованої моделі, використано технологію "пісочниць "

5. Аналітична модель станів інформаційної системи з врахуванням ймовірнісного бінарного ранжування переходів

Стан системи, яка підпадає під несанкціонований вплив загроз, позначимо через S_{ij}, де i та j – вразливості i-го та j-го типу. Потік загроз з несанкціонованим впливом на стаціонарний стан системи надходить на вхід аналітичної моделі з інтенсивністю Q. Введемо реалістичне припущення, що переходи між станами в аналітичній моделі здійснюються миттєво за часом, що характерно для атак «0 дня» та сучасної швидкодії обробки даних в інформаційних системах. Імовірнісне бінарне ранжування потоку несанкціонованих впливів приводить до утворення змін станів інформаційної системи. Тобто, враховується динаміка зміни стану в залежності від інтенсивності потоку впливу за одиницю часу. Враховуючи можливі переходи стаціонарного стану системи введемо бінарне ранжування ймовірностей переходу P_{ij} системи в кожний стан S_{ij}. Тобто,

P_{ij} розподіляється між станами системи S_{ij}, подія може наступити у випадковий момент часу, коли система знаходиться в одному з можливих станів. Переходи між станами в аналітичній моделі ранжування здійснюються безінертно (миттєво). Ймовірнісне ранжування потоку впливів призводить до утворення потоку подій в системі та на виході. В такому випадку, введемо ранжування станів моделі системи, а саме:

– S_{00} – система знаходиться в стаціонарному режимі забезпечення операційних процесів;

– S_{01} – зміна стаціонарного стану при великій інтенсивності зовнішнього впливу параметрів атаки «0 дня» на вразливість системи за часом (стан – відмова системи захисту на базі штучно створеного інтенсивного впливу за часом);

– S_{10} – зміна стаціонарного стану при зовнішньому впливі атаки «0 дня» на вразливість програмного забезпечення (стан – відмова системи захисту на базі вразливості програмного забезпечення);

– S_{11} – зміна стаціонарного стану при зовнішньому інтенсивному впливі атаки «0 дня» на вразливість системи та програмного забезпечення (стан – відмова системи захисту на базі змішаного впливу двох класів) [19].

При побудові аналітичної моделі ймовірність P_{ij} знаходження системи в будь-якому стані у вихідній моделі ймовірнісного ранжування інтерпретується як кількісний показник відповідності перебування системи у відповідному стані [20]. При цьому множина станів вважається дискретною, а час неперервним.

Переходи між станами мають вагові коефіцієнти g інтенсивності реагування на потоки впливу та переходи станів в системі. Принципова відмінність даної моделі від стандартних підходів полягає в тому, що вагові коефіцієнти характеризуються не інтенсивністю виникнення випадкових подій в системі, а інтенсивною переходів між станами. Тобто, наскільки значний коефіцієнт інтенсивності g для переводу системи в інший стан. Зазначені вагові коефіцієнти визначаються рівнем спроможності програмного забезпечення або оператора безпеки реагувати на потік несанкціонованого впливу у реальному часі та спроможністю системи на відновлення процесів. З метою забезпечення коректності цього перетворення, врахуємо вагові коефіцієнти в побудові моделі ймовірного бінарного ранжування вхідних та вихідних потоків в системі.

На базі опису ймовірнісного бінарного ранжування станів системи та вхідних і вихідних потоків, інтенсивність виникнення в системі реальної загрози атаки може бути представлено аналітичним рядом у вигляді:

$$Q = \sum_{S_i \in S_{(R+1)}} P_{S_i Q_{S_i S_R}}, \qquad (1)$$

де $S_{(R)}$ – множина станів системи, що характеризуються стаціонарністю процесів та відсутністю в ній реальної загрози атаки «0 дня».

В кожному з станів, система може знаходиться з імовірністю $P_{S(R+1)}$, де $S_{(R+1)}$ – стан системи, що знаходиться під загрозою реальної атаки. Перехід в стан $S_{(R+1)}$ з $S_{(R)}$ в системі здійснюється з інтенсивністю $P_{S(R+1),S(R)}$. Для бінарного

ранжування ймовірності переходів, формула для визначення інтенсивності потоку переходів станів буде визначена, як:

$$Q_d = P_{10}Q_2 + P_{01}Q_1, \tag{2}$$

$$P_{S_{R+1}} = 1 - P_{0d},$$

де P_{0d} ймовірність спроможності системи залишатися в стаціонарному режимі з забезпечення встановлених операційних процесів по відношенню до інтенсивності вхідного потоку класу d не санкціонованих впливів.

В стаціонарному режимі функціонування системи з врахуванням впливу реальної загрози з інтенсивністю $Q_{S(R+1),S(R)}$, стан системи без втрат (вхідний потік не змінює стан системи), це потік подій Q_d. Таким чином, стає можливим розрахувати інтенсивність усунення реальних загроз атак на тлі введення вагових коефіцієнтів:

$$q_d = \frac{Q_d}{1 - P_{0d}}. \tag{3}$$

Для найпростішого бінарного ранжування ймовірності переходів, формула для ваги q_a прийме вигляд:

$$q_d = \frac{P_{10}Q_2 + P_{01}Q_1}{P_{11}}.$$

Імовірність готовності інформаційної системи до безпечної (щодо загрози атаки) експлуатації можна визначити наступним чином:

$$P_{0d} = P_{00} + P_{10} + P_{01} = \frac{q_1 q_2 + Q\mu_2 + Q_2 q_1}{(Q_1 + q_1)(Q_2 + q_2)}. \tag{4}$$

Зрозуміло, що кількість можливих випадкових станів системи повинно бути кінцевим та може бути визначена у відповідності до порядкових номерів. Такий випадковий процес будемо називати процесом з дискретними станами [14].

Адекватність представленої аналітичної моделі забезпечується виконанням наступних обмежень, що стосуються розглянутої проблеми моделювання загрози атаки «0 дня», а саме:

– модель станів системи, що є дискретними, з безперервним часом коректна в загальному випадку, якщо з кожного стану системи при випадковому процесі несанкціонованих впливів, виходять всі N вхідних потоків подій з інтенсивністю Q_i, i=1,…, N ;

– у загальному випадку, для моделювання станів системи при загрозах атак «0 дня» повинно використовуватися розрахунки на базі моделі ряду з нескінченним числом дискретних станами і безперервним часом.

В рамках визначених обмежень така модель станів та переходів між ними може бути застосована для оцінки надійності засобів безпеки інформаційних систем та виявлення загроз. Запропонована модель характеризується можливістю одночасного виникнення в системі двох і більше несанкціонованих зовнішніх впливів. Модель ймовірнісного ранжування станів системи використана як основа для методу виявлення атак «0 дня» з врахуванням інтенсивності потоків впливу [21, 22].

Оскільки при моделюванні використовується достатня кількість можливих наборів атак або потоків впливу, можна обґрунтовано використати нормальний закон розподілу випадкових подій впливів на систему [23]. Враховуючи характеристики атак «0 дня», необхідно врахувати ймовірність виникнення в системі одночасно кількох несанкціонованих подій. Тобто, одночасний вплив кількох подій на вразливості одного типу на фіксованому інтервалі часу. Для аналітичного моделювання таких станів введемо коефіцієнт навантаження системи в залежності від інтенсивності потоку впливів. Використовуючи коефіцієнт навантаження, як $z=Q/g$, можна визначити необхідну ймовірність одночасної появи в системі n подій з урахуванням нормального (закон Гауса) закону розподілу $P_n(z)$. Для кожного типу загрози, з урахуванням заданих вимог до точності моделювання, за допомогою розрахунку значень ймовірностей $P_n(z)$ визначається число max. Також визначається число загроз, які реалізуються через вразливості відповідного типу. Всі стани $S_{i>\max(ij)}$ та переходи між ними, виключаються з моделі ряду станів системи випадкового процесу (присвоюється нульова ймовірність утворюючи штучно кінцеву послідовність), в результаті чого отримана шукана кінцева модель з можливістю прогнозування ймовірностей атак.

Таким чином, модель дозволяє відслідковувати всі можливі стани системи S_{ij}, що є зліченими згідно з відповідним обмеженням, та оцінити відповідні ймовірності знаходження в цих станах $P_{S(R+1)}$. Відповідно, за допомогою Q – інтенсивності виникнення в системі реальної загрози (1) можливо оцінити P_{0d} – ймовірність готовності системи до безпечної експлуатації (4). Використовуючи емуляцію станів за допомогою мережевої “пісочниці”, є можливим виявити найбільш небезпечні стани системи та чинники, що стали причиною переходів на ці стани, а відповідно відслідкувати можливі загрози.

Запропонована аналітична модель станів системи (1)–(4) з врахуванням особливостей атак типу «0 дня» дозволяє об’єктивно оцінити базові параметри, ймовірність та характеристики загрози. Для цього використовуються статистичні дані про виникнення і усунення вразливостей в автоматизованому режимі [24, 25].

6. Розробка схеми реалізації аналітичної моделі з використанням синтезованої мережевої та антивірусної пісочниці

Метод захисту від атак нульового дня базується на поєднанні розробленої моделі бінарного ранжування станів інформаційної системи та методів мережевої і антивірусної пісочниць. Апаратне рішення, яке включає у себе мережеву

пісочницю, встановлюється на периметрі мережі і виконує роль шлюзу. Отриманий трафік розшифровується, підозрілі файли відправляються для аналізу у хмару. Під час аналізу файл конвертуватиметься у формат PDF та відправлятиметься користувачеві з можливістю отримання оригіналу.

На кінцевих пристроях встановлюється програмне забезпечення, яке включає в себе технологію антивірусної пісочниці на основі повної віртуалізації у хмарному сервісі. Дане рішення дозволяє запобігти загрозам і атакам, пов'язаними з підключенням до зовнішньої мереж. Наприклад, підключення до Wi-Fi та хмарних додатків, які не підлягають розшифровуванню шлюзом на периметрі, підключенням до ПК зовнішніх носіїв і горизонтальним поширенням атаки в мережі. Антивірусна пісочниця дає змогу емулювати файли великих розмірів, не створюючи високого навантаження на шлюз (рис. 1).

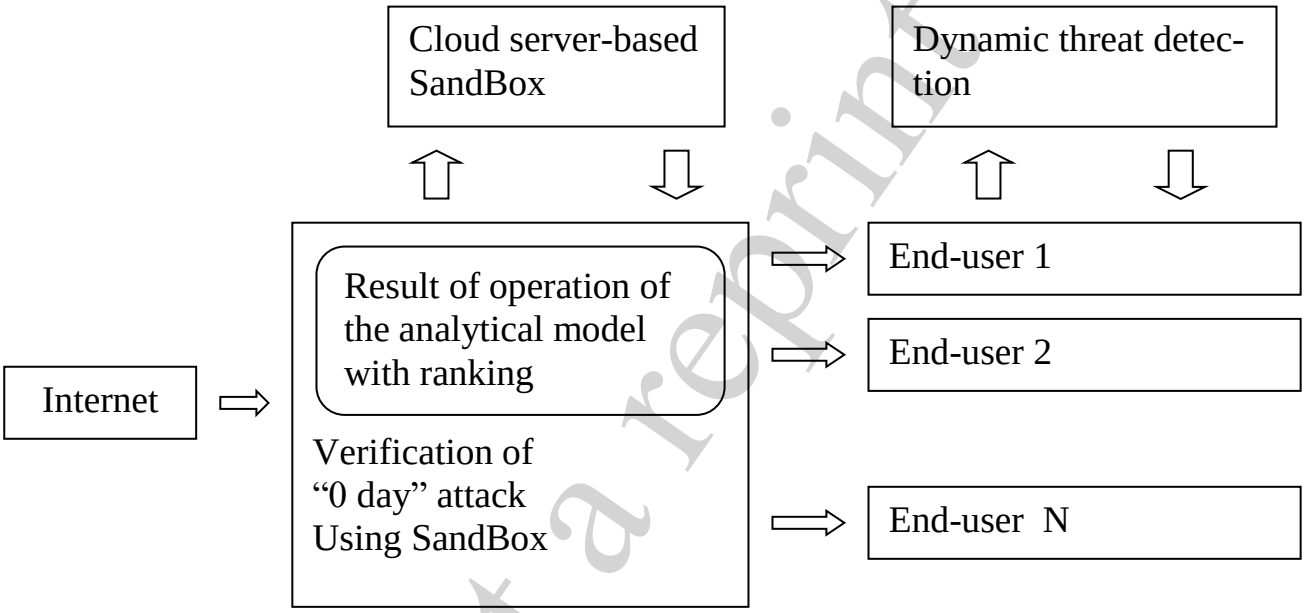

Рис. 1. Реалізація методу захисту від атак нульового дня за допомогою технологій мережевих та антивірусних пісочниць у корпоративних мережах

Мережева пісочниця приймає файли невеликого розміру для аналізу. Файли, які матимуть розмір більше 50 мегабайтів ігноруватимуться для емуляції у антивірусній пісочниці. Дане рішення зменшить навантаження і прискорить час емуляції.

Антивірусне програмне забезпечення виконуватиме аналіз підозрілих файлів, отриманих з переносних носіїв та хмарних додатків, які не розшифровуються. Такий підхід забезпечує найвищий захист від потрапляння шкідливого програмного забезпечення (ПЗ) у мережу та на кінцеві точки [26, 27].

Таким чином, загалом схему реалізації можна формально описати наступним чином (рис. 1):

1. Файл надходить із зовнішнього джерела до системи, де розшифровується та потрапляє до зовнішнього шлюзу, представленого мережевою пісочни-

цею. Файли більше 50 мегабайтів ігноруватимуться не будуть емульовані у антивірусній пісочниці

2. Проводиться аналіз файлів з використанням аналітичної моделі з ранжуванням. В разі виявлення підозрілого файлу, він відправляється для подальшого аналізу у хмару. Користувачу відправляється файл, конвертований в формат PDF.

3. Перевірені файли направляються до кінцевих користувачів.

4. Файли розміром більші за 50мб, та отримані з зовнішніх джерел, як наприклад зовнішніх дисків та мереж, перевіряються на комп'ютерах кінцевих користувачів. Для цього використовується алгоритм динамічного виявлення загроз.

7. Тестування запропонованої схеми реалізації моделі з використанням пісочниць

Запропоновані метод та модель був протестований на базі комерційного підприємства з 500-ми кінцевими пристроями. На периметрі було встановлено два шлюзи антивірусного програмного забезпечення, зібрані у кластер для забезпечення відмовостійкості. На кожний сервер та кінцевий пристрій встановлено класичну антивірусну програму. Тестування побудованої системи захисту інформації на основі запропонованого методу здійснювалось за допомогою синтетичного тесту та тесту на реальному трафіку.

Цілями даного тестування було: оцінка ефективності та доцільності застосування «пісочниць» в складі комплексної системи інформаційної безпеки; оцінка ефективності побудованої моделі захисту від атак нульового дня.

Тестування «пісочниць» проводилося в два етапи: тестування з використанням синтетичних зразків шкідливого коду; тестування на реальному інтернет-трафіку користувачів [28].

Синтетичні тести проводилися з використанням тимчасових віртуальних машин. При доставці вірусів в тестову зону застосовувалися методи, що ускладнюють виявлення традиційними сигнатурними засобами захисту:

– архівація файлу з використанням форматів RAR, ZIP, 7-ZIP;

– поштові повідомлення з веб-посиланнями на шкідливий файл, в тому числі с використанням «коротких» URL (URL shortening);

– шифрування шкідливого коду (payload) макросу в документах Microsoft Word через макроси.

Необхідно відзначити, що всі рішення тестувалися в реальній мережі (в ізольованому мережевому середовищі). Тому перш ніж потрапити на аналіз в пісочницю, файли з шкідливим кодом проходили аналіз і блокувалися наявними засобами захисту, з використанням сигнатурних і репутаційних механізмів. Даний алгоритм тестування виконувався в тому числі для оцінки ефективності існуючих засобів захисту.

В рамках тестів аналізувалися основні канали отримання шкідливого програмного забезпечення: файли, завантажуванні з веб-ресурсів; вкладені файли в електронній пошті; файли на зовнішніх носіях інформації.

В рамках тестування на реальному інтернет-трафіку мережева пісочниця встановлювалася в режимі TAP і отримувала для аналізу копію мережевого інтернет трафіка. Збір мережевого трафіку тривав 1 місяць.

Контролювалися основні канали отримання вірусів із зовнішніх мереж: електронна пошта; взаємодія з веб-сервісами в інтернеті; взаємодія з хмарними додатками; взаємодія з зовнішніми носіями інформації. Для синтетичного тестування побудованої системи було відібрано 55 зразків шкідливого програмного забезпечення, які потрапили до бази даних сигнатур за 2018 рік. На мережевій та антивірусній пісочниці був відключений метод сигнатурного аналізу. Таким чином, побудована система отримувала шкідливе програмне забезпечення без можливості перевірки у базі даних [29].

З 55 екземплярів, які використовуються при тестуванні аналізу веб-трафіку, на аналіз в пісочниці потрапило 32 файлу з шкідливим кодом, не виявлених існуючими засобами антивірусного захисту. При тестуванні на поштовому трафіку традиційні засоби захисту виявили тільки 1 з 15 шкідливих програм – на аналіз в пісочниці надійшло 14 з 15 файлів. У синтетичному тесті для веб-трафіку використовувалося 55 різних шкідливих файлів. Існуючими засобами захисту (захищений шлюз доступу в інтернет) було заблоковано 23 з 55 екземплярів. На тестування в пісочницю надійшло 32 з 55 шкідливих файлів.

Результати синтетичного тесту «мережевих пісочниць» для веб-трафіку, синтетичного тесту для поштового трафіку та виявлені за допомогою пісочниць шкідливі програми представлені в табл. 1–3.

Сумарно за один місяць система захисту від цільових атак зафіксувала 72 загрози, які не заблоковані і не зафіксовані існуючими сигнатурними засобами захисту.

Кількість виявлених загроз побудованою системи захисту інформації у порівнянні з існуючою на підприємстві за 1 місяць спостерігання також представлена на рис.2.

Разом з класичною антивірусною системою та використання запропонованого методу, також було протестовано ще два підходи, а саме сенсорних пасток (Sensory Traps) [12] та використання медових горщиків (Honey Pots) [13].

Таблиця 1

Результати синтетичного тесту «мережевих пісочниць» для веб-трафіку

	Кращий результат побудованої системи захисту інформації	Існуючі системи захисту інформації (WatchGuard)
Виявлені шкідливі програми	29/32	0/32

Таблиця 2

Результати синтетичного тесту для поштового трафіку

	Кращий результат побудованої системи захисту інформації	Існуючі системи захисту інформації (WatchGuard)
Виявлені шкідливі програми	9/14	0/14

Таблиця 3

Виявлені за допомогою пісочниць шкідливі програми

Тип шкідливого програмного забезпечення	Виявлено [кількість]
Trojan	34
Worm	2
Backdoor	5
Trojan.Downloader	18
Ransomware	2
Spyware	2
Riskware/Adware	7
Використання уразливості в веб-браузереWeb.Exploit	1
Використання уразливості в веб-браузереMal/FakeAV-SE	1
Спроб комунікацій із зовнішнім сервером управління ботнет-мережами (callbacks)	25
Разом (без урахування callbacks)	72

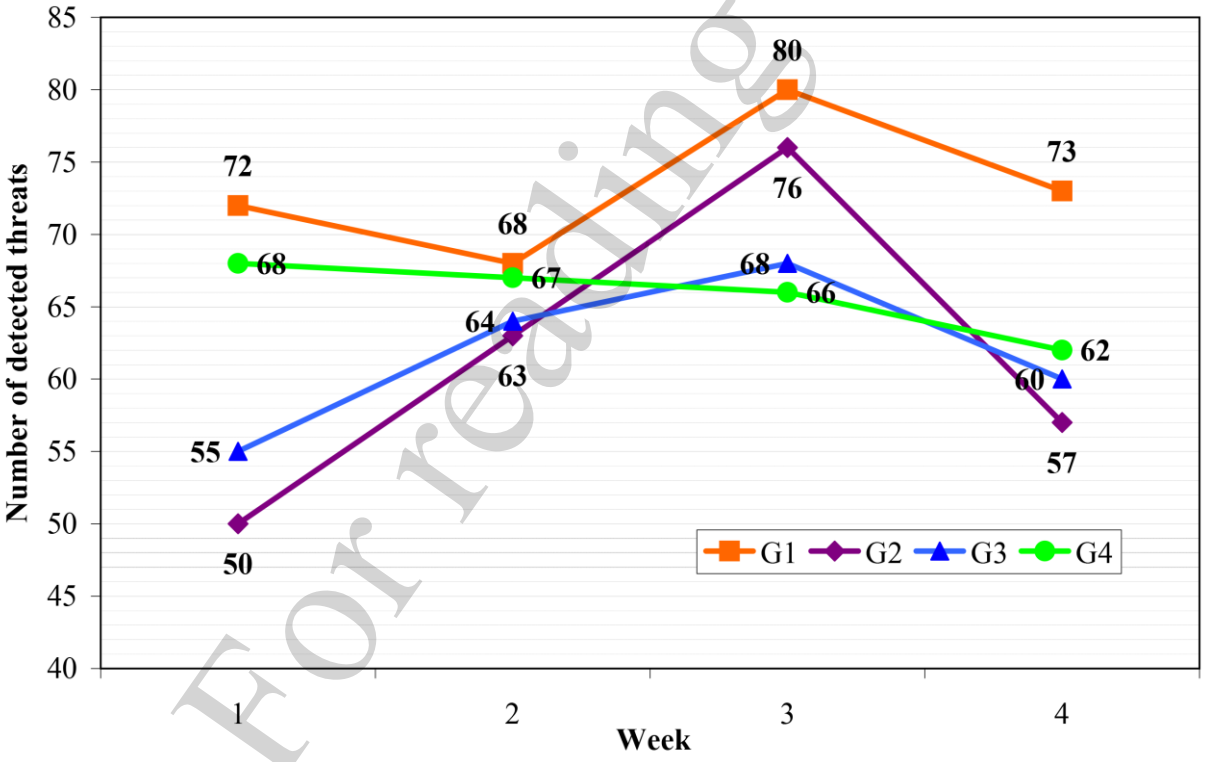

Рис. 2. Кількість виявлених загроз побудованою системи захисту інформації у порівнянні з існуючою на підприємстві за 1 місяць спостерігання. Графіки: G1 – розроблена модель захисту; G2 – класична антивірусна система; G3 – сенсорні пастки [12]; G4 – медові горщики [13].

Частина виявлених в рамках тестування шкідливих програм не виявляється деякими сигнатурними антивірусами навіть через кілька місяців після закінчення тестування.

8. Обговорення результатів тестування розробленого методу захисту та відповідної моделі

Запропонований метод виявлення загроз з використанням «мережевих пісочниць» та створеної математичної моделі дозволяє не лише виявляти загрозу після її активності, а опереджати проникнення. Ефективність методу доведено при тестуванні, результати показано в табл. 1–3. Пояснити таку значну ефективність можна апріорним використанням математичної моделі, що відслідковує зміни в стані системи, а не лише збирає статистику пост-фактум, як більшість антивірусних систем.

Систему адаптивного аналізу станів можна порівняти з алгоритмами штучного інтелекту, наприклад нейронними мережами [9, 31]. Проте, нейронні мережі потребують довготривалого процесу навчання на достовірних прикладах, що унеможливлює виявлення нових типів загроз. Класичні ж методи виявлення не здатні відстежити атаку на перших етапах, та виявляють загрозу лише після масового зараження системи.

Порівнюючи запропонований метод з методами сенсорних пасток та медових горщиків можна зробити наступні висновки: обидва вищезгадані методи з часом втрачають свою актуальність, оскільки забезпечують захист від наперед відомих атак. Тому такі підходи є актуальними якщо заздалегідь відомо про потенційно слабкі місця в системі чи дані, які найбільш цікаві для зловмисника.

Крім того, запропонований метод є досить гнучким завдяки простоті математичної моделі, що дозволяє адаптувати його до кожної конкретної задачі та системи. Це є одночасно перевагою та недоліком, оскільки потребує уваги досвідченого спеціаліста, який зможе правильно налаштувати коефіцієнти системи. Але така гнучкість дозволить виявляти події, що мають різне тлумачення з точки зору небезпеки для різних систем.

Як один з недоліків слід зазначити ймовірність помилкового спрацьовування системи, тобто виявлення та розпізнавання безпечних повідомлень як атаки. Подібний випадок можливий, наприклад, при постійній масовій розсилці файлів по всіх комп'ютерах мережі.

Незважаючи на значну перевагу методу, що показано в табл. 1–3, на даний момент він знаходиться на початкових етапах розробки. Аналітична модель потребує вдосконалення, наприклад з використанням вагових коефіцієнтів та можливістю зміни параметрів безпосередньо під час роботи алгоритму. Також слід дослідити можливість імплементації існуючих алгоритмів кіберзахисту.

9. Висновки

1. Створення аналітичної моделі станів інформаційної системи дозволяє в реальному часі оцінити вплив різних чинників та відслідкувати можливі деструктивні дії, не піддаючи загрозі саму систему. Завдяки цьому запропонована модель є універсальною, але в той же час дозволяє проводити досить глибокий аналіз та відслідкувати деструктивні зовнішні впливи. Впровадження ймовірнісного бінарного ранжування переходів між станами системи дає змогу в автоматичному режимі відслідкувати потенційно небезпечні зміни в системі. Це є неможливим в ручному режимі через велику кількість запитів, що надходять в кожен момент часу. Для виявлення та оцінки потенційної загрози в тому чи іншому стані

використано вагові коефіцієнти, які характеризуються не інтенсивністю виникнення випадкових подій в системі, а інтенсивною переходів між станами. Також використано аналітичний ряд з врахуванням динамічної послідовності випадкових станів для забезпечення коректності аналітичного представлення.

Така система дозволяє виявити небезпечну активність ще до нанесення шкоди системі, що відрізняється від більшості класичних методик захисту, які діють вже постфактум, тобто після здійснення атаки. Впровадження вагових коефіцієнтів дає змогу індивідуально налаштувати параметри виявлення загрози, оцінюючи ймовірності переходів системи в небезпечні стани. Тобто, експерт має змогу вказати, яка сама інтенсивність запитів повинна вважатися небезпечною.

2. Було запропоновано та протестовано схему реалізації розробленої моделі за допомогою мережевих "пісочниць" та інтеграції з наявними методами та програмами антивірусного захисту, що дозволяє використовувати сильні сторони різних підходів. Як приклад, було використано антивірусну систему, що дало значні позитивні результати. Використання методів багаторівневої мережевої пісочниці дозволяє більш об'єктивно оцінити ситуацію в інформаційній системі та виявити приховану активність. Крім того, використання зовнішньої антивірусної системи дозволяє також перевіряти великі файли, отримані з зовнішніх носіїв, та зменшити навантаження на мережеву пісочницю.

3. За результатами тестів, запропоноване поєднання методу мережевої пісочниці на базі розробленої моделі та антивірусних систем показує свою ефективність в порівнянні з класичними методами. Деякі атаки не були діагностовано класичними системами протягом кількох місяців. В той же час, важливо пам'ятати про можливість помилкового виявлення, що потребує подальшої роботи над алгоритмом. Розроблений метод захисту від атак нульового дня за допомогою технології «пісочниць», використано у поєднанні з методами багаторівневої мережевої пісочниці та антивірусної пісочниці на основі повної віртуалізації. Багаторівнева мережева пісочниця базується на аналітичній моделі системи з врахуванням ранжування станів. Зазначений підхід дозволив покращити захист корпоративної мережі від невизначених типів атак у порівнянні з класичними методами захисту на 15 %.

Література

1. Moussouris, K., Siegel, M. (2015). The Wolves of Vuln Street: The 1st System Dynamics Model of the 0day Market. RSA Conference 2015. San Francisco. URL: https://ic3-2017.mit.edu/sites/default/files/documents/MichaelSiegelKatieMoussouris_VulnMarketsRSAC2015Speaker.pdf

2. Schwartz, A., Knake, R. (2016). Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process. Discussion Paper 2016-04. Harvard Kennedy School. URL: https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Disclosure%20Web-Final4.pdf

3. Yudin, O., Ziubina, R., Buchyk, S., Bohuslavska, O., Teliushchenko, V. (2019). Speaker's Voice Recognition Methods in High-Level Interference Conditions. 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON). doi: https://doi.org/10.1109/ukrcon.2019.8879937

4. Gurzhiy, P., Gorodetsky, B., Yudin, O., Ryabukha, Y. (2019). The Method of Adaptive Counteraction to Viral Attacks, Taking Into Account Their Masking in Infocommunication Systems. 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT). doi: https://doi.org/10.1109/aiact.2019.8847893

5. Edwards, J. (2001). Next-generation viruses present new challenges. Computer, 34 (5), 16–18. doi: https://doi.org/10.1109/2.920606

6. Hedberg, S. (1996). Combating computer viruses: IBM's new computer immune system. IEEE Parallel & Distributed Technology: Systems & Applications, 4 (2), 9–11. doi: https://doi.org/10.1109/88.494599

7. Zhao, F., Li, Q., Jin, L. (2006). An Intrusion-Tolerant Intrusion Detection Method Based on Real-Time Sequence Analysis. 2006 International Conference on Machine Learning and Cybernetics. doi: https://doi.org/10.1109/icmlc.2006.258927

8. Jensen, M. (2013). Challenges of Privacy Protection in Big Data Analytics. 2013 IEEE International Congress on Big Data. doi: https://doi.org/10.1109/bigdata.congress.2013.39

9. Tesauro, G. J., Kephart, J. O., Sorkin, G. B. (1996). Neural networks for computer virus recognition. IEEE Expert, 11 (4), 5–6. doi: https://doi.org/10.1109/64.511768

10. Bonneau, J., Anderson, J., Danezis, G. (2009). Prying Data out of a Social Network. 2009 International Conference on Advances in Social Network Analysis and Mining. doi: https://doi.org/10.1109/asonam.2009.45

11. Azzedin, F., Suwad, H., Alyafeai, Z. (2017). Countermeasureing Zero Day Attacks: Asset-Based Approach. 2017 International Conference on High Performance Computing & Simulation (HPCS). doi: https://doi.org/10.1109/hpcs.2017.129

12. Popereshnyak, S., Suprun, O., Suprun, O., Wieckowski, T. (2018). Intrusion detection method based on the sensory traps system. 2018 XIV-Th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH). doi: https://doi.org/10.1109/memstech.2018.8365716

13. Tian, Z.-H., Fang, B.-X., Yun, X.-C. (2003). An architecture for intrusion detection using honey pot. Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.03EX693). doi: https://doi.org/10.1109/icmlc.2003.1259851

14. Yudin, O., Boiko, Y., Ziubina, R., Buchyk, S., Tverdokhleb, V., Beresina, S. (2019). Data Compression Based on Coding Methods With a Controlled Level of Quality Loss. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/atit49449.2019.9030431

15. How to Choose your Next Sandboxing Solution. Featuring insight from gartner's market guide for network Sandboxing (2016). Check Point Software Technologies Ltd. URL: https://www.checkpoint.com/downloads/products/check-point-gartner-how-to-choose-sandboxing-solution-whitepaper.pdf

16. Burnap, P., French, R., Turner, F., Jones, K. (2018). Malware classification using self organising feature maps and machine activity data. Computers & Security, 73, 399–410. doi: https://doi.org/10.1016/j.cose.2017.11.016

17. ESET Dynamic Threat Defense. URL: https://www.eset.com/int/business/dynamic-threat-defense/

18. Lakhno, V., Kasatkin, D., Kozlovskyi, V., Petrovska, S., Boiko, Y., Kravchuk, P., Lishchynovska, N. (2019). A model and algorithm for detecting spyware in medical information systems. International Journal of Mechanical Engineering and Technology, 10 (1), 287–295.

19. The Problem with Traditional Sandboxing. URL: https://blog.checkpoint.com/2015/09/14/the-problem-with-traditional-sandboxing/

20. Villalba, L. J. G., Orozco, A. L. S., Vidal, J. M. (2015). Malware Detection System by Payload Analysis of Network Traffic. IEEE Latin America Transactions, 13 (3), 850–855. doi: https://doi.org/10.1109/tla.2015.7069114

21. Yudin, O., Ziubina, R., Buchyk, S., Matviichuk-Yudina, O., Suprun, O., Ivannikova, V. (2020). Development of methods for identification of information-controlling signals of unmanned aircraft complex operator. Eastern-European Journal of Enterprise Technologies, 2 (9 (104)), 56–64. doi: https://doi.org/10.15587/1729-4061.2020.195510

22. Yudin, O., Symonychenko, Y., Symonychenko, A. (2019). The Method of Detection of Hidden Information in a Digital Image Using Steganographic Methods of Analysis. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). doi: https://doi.org/10.1109/atit49449.2019.9030479

23. D'Hoinne, J., Orans, L. (2015). Market Guide for Network Sandboxing. Gartner. URL: https://www.gartner.com/en/documents/2995621

24. Cooke, E., Jahanian, F., McPherson, D. (2005). The zombie roundup: Understanding, detecting, and disrupting botnets. SRUTI '05: Steps to Reducing Unwanted Traffic on the Internet Workshop, 39–44.

25. Koller, D., Friedman, N. (2009). Probabilistic Graphical Models. Principles and Techniques. MIT Press.

26. National Vulnerability Database. Statistics. NIST. URL: https://nvd.nist.gov/vuln/search?adv_search=true&cves=on&pub_date_start_month=0&pub_date_start_year=2010&pub_date_end_month=9&pub_date_end_year=2016&cvss_version=3

27. CVSS Severity Distribution Over Time. NIST. URL: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

28. Ablon, L., Libicki, M. C., Abler, A. M. (2017). Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. RAND Corporation. URL: https://www.rand.org/pubs/research_reports/RR610.html

29. Allodi, L., Massacci, F. (2014). Comparing Vulnerability Severity and Exploits Using Case-Control Studies. ACM Transactions on Information and System Security, 17 (1), 1–20. doi: https://doi.org/10.1145/2630069

30. Chandrasekaran, M., Baig, M., Upadhyaya, S. (2006). AVARE: Aggregated Vulnerability Assessment and Response against Zero-day Exploits. 2006 IEEE International Performance Computing and Communications Conference. doi: https://doi.org/10.1109/.2006.1629458