Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ
ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: АКТУАЛЬНІ ПИТАННЯ ТА ІННОВАЦІЇ

Матеріали Міжнародної науково-практичної конференції

(м. Дніпро, 4 листопада 2021 р.)

Дніпро
2021

УДК 33+004+4+35
Е40

Схвалено науково-методичною радою
Дніпропетровського державного університету
внутрішніх справ протокол № 3 від 18.11 2021)

Е 40 **Економічна та інформаційна безпека: актуальні питання та інновації** : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 4 листоп. 2021 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 399 с.

ISBN 978-617-8032-40-1

Збірник містить матеріали однойменної міжнародної науково-практичної конференції. У заході взяли участь науковці, викладачі та здобувачі вищих навчальних закладів та наукових установ України і зарубіжжя, а також фахівці-практики правоохоронних органів. Тематика публікацій охоплює актуальні питання економічної та інформаційної безпеки.

Матеріали конференції можуть бути використані в науково-дослідній роботі та навчальному процесі спеціалізованих ВНЗ, а також у законотворчості та правоохоронній діяльності.

ISBN 978-617-8032-40-1

Вітальне слово
ректора Дніпропетровського державного університету внутрішніх справ
ФОМЕНКА АНДРІЯ ЄВГЕНОВИЧА,
доктора юридичних наук, доцента,
заслуженого юриста України,
полковник поліції

Шановні учасники конференції! Радий Вас вітати від імені науково-педагогічного колективу Дніпропетровського державного університету внутрішніх справ та від себе особисто на Міжнародній науково-практичній конференції «Економічна та інформаційна безпека: актуальні питання та інновації». Статус заходу є міжнародним і це підтверджує актуальність питань, що нами розглядаються.

Сучасний вік – вік інформації не тільки відкриває можливості, а й ставить нові завдання, та потребує вирішення нових проблем. Тому необхідно адекватно реагувати на подібні виклики. Можна сміливо стверджувати, що економічна та інформаційна небезпеки становлять один з найбільш небезпечних видів загроз, і свідченням цього є постійне обговорення проблем економічної та інформаційної безпеки як науковою спільнотою, практиками, так і на офіційних зустрічах на найвищому політичному рівні.

Наш університет має певні досягнення в цьому напрямі. Останнім часом створено відповідну кафедру та факультет підготовки курсантів для підрозділів стратегічних розслідувань Національної поліції за спеціалізацією «фінансово-економічна безпека». Споруджено спеціалізований полігон для відпрацювання фабул з документування та розкриття злочинів в економічній сфері. Відкриті нові спеціальності для підготовки студентів у сфері менеджменту за спеціалізацією «економіко-фінансова безпека» й економіки за спеціалізацією «захист економіки».

Зважаючи на сучасні реалії, тема нашого обговорення є надзвичайно актуальною, глибокою і водночас складною.

Складність і глобальний характер завдань вимагають розробки ґрунтовного наукового супроводження і консолідації зусиль представників наукової спільноти.

Тож з огляду на зазначене мета сьогоднішнього наукового заходу – обговорити такі питання:

- використання інформаційних технологій в діяльності поліції;
- безпека в інформаційній та економічній сфері;

– сучасний стан, проблеми та перспективи розвитку фінансової та економічної безпеки підприємств, регіонів, суспільства.

Саме для отримання відповідей на ці проблемні питання та удосконалення практичних і теоретичних навичок проводиться цей захід.

Завдяки присутності на заході фахівців різних сфер науки і практики, а саме: економіки, менеджменту, інформаційних технологій, економічної та інформаційної безпеки, юриспруденції, бізнесу та правоохоронних органів ми маємо виняткову змогу перейняти позитивний досвід у зазначеній сфері, а також поділитися власним досвідом.

Переконаний, що наукова дискусія під час обговорення визначених питань матиме глибокий та плідний характер і сприятиме розвитку вітчизняної науки, подальшому підвищенню рівня протидії злочинності в економічній та інформаційній сферах.

Від імені оргкомітету конференції щиро дякую вам за те, що знайшли час взяти участь у конференції з цієї, безперечно актуальної на сьогодні, проблематики.

Вітальне слово
т.в.о. начальника Департаменту
інформаційно-аналітичної підтримки
Національної поліції України,
кандидата юридичних наук
ТИМЧЕНКА ЛЕОНІДА ЛЕОНІДОВИЧА

Дозвольте мені від імені колективу Департаменту інформаційно-аналітичної підтримки поліції України привітати вас з проведенням Міжнародної науково-практичної конференції «Економічна та інформаційна безпека: питання та інновації».

Варто зауважити, що розвиток публічних послуг дозволяє провідним країнам світу в цій сфері не лише підвищувати швидкість та якість обслуговування, але й суттєво економити бюджетні кошти та час держави на обслуговування громадян.

У 2020 році, порівняно з попереднім роком, міжнародна пропускна здатність Інтернету зросла на 35 %, приблизно з 450 до 600 Тбіт/с. З 2014 року зростання відбувалося майже тричі.

Кількість користувачів Інтернету у світі досягла майже 5 млрд осіб, що становить приблизно 63 % від загальної кількості світового населення. За 2020 рік в Україні кількість користувачів зросла з 19 до 26 млн, або з 45 % до 58 % населення. До 2023 року в уряд України має намір приєднати 95 % соціальної інфраструктури до Інтернету.

Говорячи про зростання даних, можна відмітити, що тільки ютуб

завантажується до 300 годин відео. Однак оцінки дозволяють припустити, що тільки 0,5 % усіх даних коли-небудь аналізуються та використовуються.

Стрімке поширення цифрових технологій робить «цифрові» навички людей одними з основних. Цифровізація та робота з даними зараз головні тренди на загальному ринку праці. Тобто вміння працювати з цифровими технологіями поступово стає необхідним для більшості спеціальностей. Для всебічної цифровізації ДІАП розбудовує середовище інформаційних технологій для користувачів баз даних, цифрових сервісів, телекомунікаційних послуг та радіозв'язку.

Сподіваюсь, що під час обговорень та наукових дискусій учасниками конференції буде розроблено нові методи та підходи створення якісного цифрового сервісу. Розроблені рекомендації сприятимуть розробленню законодавства та практики його застосування.

Вітальне слово т.в.о. начальника
Департаменту кримінального аналізу
Національної поліції України
ХУДЕНКА ДМИТРА МИКОЛАЙОВИЧА

Шановний голово організаційного комітету! Шановні члени організаційного комітету та учасники Міжнародної науково-практичної конференції! Щиро вітаємо всіх від імені колективу Департаменту кримінального аналізу Національної поліції України з нагоди відкриття цього заходу! Проведення конференції на міжнародному рівні та заявлені учасниками теми наукових розвідок наголошують на особливій актуальності досліджень питань економічної та інформаційної безпеки.

Вкрай важливою передумовою інновацій у згаданих сферах безпеки залишається наука. Не менш важливою для науки є практика. Ці два феномени взаємозалежні у своєму розвитку і потребують обміну думок між українськими науковими школами, фахівцями й представниками міжнародних організацій та наукових еліт іноземних країн.

Програма нашої конференції містить різноаспектний масив питань, зокрема пов'язаних із кримінальними аналізом. Для Департаменту кримінального аналізу, який також розробляє, впроваджує та застосовує нові методи та напрями здійснення кримінального аналізу, спрямовані на підвищення ефективності протидії злочинності, цей формат конференції є надзвичайно цікавим.

У сучасних умовах світового розвитку, коли, наприклад, економіка зазнала впливу пандемії, назріває чергова науково-технічна революція, обсяг

інформації зростає шаленими темпами, а фізичний світ шукає альтернатив у віртуальному, представники злочинного світу користуються не лише класичними способами вчинення злочинів у зазначених сферах, але й вдаються до нових або досі не бачених способів їх підготовки та вчинення. Саме тому ми змушені постійно підвищувати протидію злочинності.

55 років досягнень Дніпропетровського державного університету внутрішніх справ та якісний склад учасників Міжнародної науково-практичної конференції дають нам міцний фундамент для полеміки та успішного розвитку системного наукового та міждисциплінарного підходу до вивчення проблем економічної та інформаційної безпеки.

Ми сподіваємось, що знання, досвід та пропозиції учасників Міжнародної науково-практичної конференції стануть в нагоді на шляху забезпечення економічної та інформаційної безпеки суспільства.

Бажаємо всім плідної співпраці, вагомих результатів на практиці, творчих успіхів та наукових відкриттів!

Приветственное слово ректора Бухарестского университета «ARTIFEX», профессора, доктора философии АЛЕКСАНДРУ-ЛУЧИАН МАНОЛЕ

Уважаемые коллеги! Для меня большая честь участвовать в качестве представителя Бухарестского университета «ARTIFEX» в престижной конференции по экономической и информационной безопасности, организованной уважаемым Днепропетровским государственным университетом внутренних дел. Тема конференции чрезвычайно важна и актуальна, когда экономическая информация является одним из ключей к управлению политическими отношениями. Развитие (и преимущества) компьютерной обработки информации вместе с расширением сетей сопряжено с некоторыми издержками, одна из которых связана с безопасностью информации, которую необходимо защищать любой ценой. Мы можем согласиться с тем, что после компрометации конфиденциальность информации не может быть восстановлена.

От имени академического сообщества Бухарестского университета «ARTIFEX» выражаю самые искренние пожелания, поздравления и уважение организаторам и участникам конференции. Мы считаем, что усилия исследователей должны быть капитализированы в ценной и полезной базе знаний и собрании передового опыта, что будет способствовать усилению безопасности физических и электронных систем обработки информации.

З М І С Т

ТЕЗИ ВИСТУПІВ

КУРСАНТИ ТА СТУДЕНТИ

Недєлков К. Ю., здобувач 2-го курсу магістратури Одеського державного університету внутрішніх справ, співробітник відділу research and forensic ТОВ «Група інформаційної безпеки «ФС ГРУП», м. Одеса
Науковий керівник – Ісмайлов К. Ю., старший науковий співробітник НДЛ з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ, начальник 5-го відділу 3-го управління ДКП НПУ, кандидат юридичних наук, доцент, підполковник поліції

АВТОМАТИЗОВАНИЙ АНАЛІЗ ОБРАЗІВ ФАЙЛОВОЇ СИСТЕМИ ТА ЗБІР ЦИФРОВИХ ДОКАЗІВ КРИМІНАЛЬНОГО ХАРАКТЕРУ ЯК СПОСІБ ЗАПОБІГАННЯ КІБЕРАТАК

Витонченість хакерських інструментів зростає мало не щодня. Якщо кілька років тому шкідливе програмне забезпечення (ПЗ) найчастіше купувалося у самого розробника, який міг зникнути відразу після продажу, не гарантуючи працездатності продукту, то сьогодні практично будь-яка людина з мінімальними теоретичними і практичними навичками в комп'ютерній вірусології та кібербезпеці може придбати malware-as-a-service [1] з повною технічною підтримкою, включно з розробкою ботнету під ключ, купівлею доменного імені, орендою сервера, розгортанням контрольної панелі на сервері (далі C&C-сервер) [2], послугою шифрування шкідливого ПЗ або обфускації коду, тестуванням на детектування великою кількістю антивірусних рішень тощо.

За даними міжнародної некомерційної організації «The Spamhaus Project», яка, у тому числі, досліджує активність ботнетів [3] та географічне розташування їхніх C&C серверів, у своєму звіті [4] за 2-й квартал 2021-го року помістило Україну на 8-ме місце у світі за кількістю розміщених C&C серверів зловмисників (рис. 1).

Порівняно з першим кварталом цього ж року – у другому кварталі кількість зафіксованих серверів зловмисників збільшилась вдвічі. Крім того, один з українських хостинг-провайдерів посів п'яту сходинку (рис. 2) у рейтингу найпопулярніших у зловмисників «майданчиків» для розміщення контрольних панелей ботнетів.

Rank	Country	Q1 2021	Q2 2021	% Change Q on Q
#1	United States	338	281	-17%
#2	Russia	195	233	19%
#3	Netherlands	207	168	-19%
#4	Germany	99	117	18%
#5	France	71	92	30%
#6	Latvia	31	84	171%
#7	United Kingdom	49	57	16%
#8	Ukraine	22	44	100%
#9	Switzerland	59	41	-31%
#10	Seychelles	29	38	31%

Rank	Country	Q1 2021	Q2 2021	% Change Q on Q
#11	Czech Republic	-	31	New entry
#12	Moldova	29	29	0%
#13	Panama	-	16	New entry
#13	Canada	26	16	-38%
#15	Malaysia	-	15	New entry
#15	Poland	-	15	New entry
#17	Finland	-	14	New entry
#18	Vietnam	-	13	New entry
#18	Turkey	25	13	-48%
#20	Brazil	20	12	-40%

Рис. 1. Рейтинг країн, в яких були розміщені C&C сервери
у 2-му кварталі 2021-го року

Через що ще більше актуалізується питання потенційної загрози та превентивних методів виявлення контрольних серверів зловмисників.

Рис.2. Рейтинг хостинг-провайдерів, на яких зафіксовано розміщення C&C серверів у 2-му кварталі 2021-го року

Метою дослідження є розробка алгоритму виявлення та дослідження контрольних серверів ботнетів завдяки автоматизованому аналізу файлової системи цих та збір криміналістичних цифрових доказів.

Rank	Q1 2021	Q2 2021	% Change	Network	Country
#1	35	82	134%	pq.hosting	Russia
#2	53	74	40%	google.com	United States
#3	21	68	224%	serverion.com	Netherlands
#4	51	56	10%	ovh.com	France
#5	23	53	130%	itldc.com	Ukraine
#6	-	49	New Entry	nano.lv	Latvia
#7	131	48	-63%	privacyfirst.sh	Germany
#8	-	47	New Entry	mgnhost.ru	Russia
#9	19	46	142%	hetzner.de	Germany
#10	-	40	New Entry	baxet.ru	Russia
#11	-	35	New Entry	ipjetable.net	France
#12	45	29	-36%	cloudflare.com	United States
#12	-	29	New Entry	digitalocean.com	United States
#14	-	28	New Entry	Internet.it	Russia
#15	26	26	0%	alibaba-inc.com	China
#16	-	25	New Entry	hostsailor.com	U. Arab Emirates
#17	-	22	New Entry	microsoft.com	United States
#18	-	21	New Entry	m247.ro	Romania
#19	-	16	New Entry	offshoreracks.com	Panama
#19	-	16	New Entry	mivocloud.com	Moldova

Зловмисники нерідко вдаються до розгортання своїх послуг і сервісів на «білих» чи «сірих» хостингах, що спричиняє фінансові та репутаційні втрати як жертвам шкідливих кампаній, так і самим хостинг-провайдерам.

Найчастіше для розгортання C&C-панелей використовується VPS (Virtual Private Server) або VDS (Virtual Dedicated Server) з т. з. LAMP

конфігурацією (Linux (ОС), Apache (WEB-сервер), MySQL (СУБД – система управління базами даних), phpMyAdmin (вебінтерфейс для адміністрування СУБД)). Ця конфігурація цілком схильна до автоматизації отримання необхідної інформації для проведення аналізу і збору криміналістичних доказів.

Більш детально зупинимось на розробленій нами концепції автоматизованого рішення для аналізу файлових систем підозрілих орендарів VPS/VDS з отриманням цифрових доказів зловмисників, що дозволить як припинити підготовку шкідливої кампанії, так і потенційно встановити наміри і самого зловмисника. Алгоритм ПЗ, який дозволить отримати з C&C-сервера зловмисника таку інформацію (у разі вилучення дампа ОС у хостинг-провайдера з боку правоохоронних органів у межах кримінального провадження або розслідування):

- SQL дамп бази даних та їх структуру;
- лог-файли підключень SSH/RDP протоколів;
- отримання даних про жертви вірусних кампаній;
- отримання даних про зловмисників.

Щодо одержуваної структури бази даних, то за інформацією з відкритих джерел (наприклад, збірника вихідних кодів C&C-панелей деяких троянів-стілерів внаслідок витоку інформації або припинення розробки і підтримки шкідливого програмного забезпечення (далі ШПЗ) хакером (надається для дослідницьких цілей – https://github.com/threatland/TL-TROJAN)), зустрічаються порожні «шаблони» баз даних того чи іншого ШПЗ, в якому присутня структура та назва таблиць бази даних. За цими даними можна визначити унікальні особливості і з високою точністю визначати приналежність бази даних до того чи іншого виду ШПЗ безпосередньо за структурою бази даних, тобто створення певних сигнатур.

Отже, проаналізувавши усю згадану вище інформацію, робимо висновок, що для розробки алгоритму виявлення, дослідження C&C серверів та збору цифрових доказів необхідно:

- мінімізація часу обробки дампу до ~10 хвилин (залежності від кількості та обсягу інформації, що знаходиться в дампі ФС та потужності дослідного ПК);
- уніфікування процесу обробки дампів файлових систем (далі ФС) з різними версіями і родинами ОС (Ubuntu, Debian, Centos, Windows та інші);
- підвищення відмовостійкості для того, щоб на процес і подальшу обробку дампів не впливали вихід з ладу локального серверу бази даних MySQL завдяки інтеграції можливості діагностики та відновлення БД в разі виникнення помилок;
- створення сигнатур баз даних найчастіших шкідників, які дозволяють категоризувати бази даних і відразу ж виокремлювати потрібну інформацію з потрібних таблиць БД;
- ведення статистики отриманої інформації з кожного дампа і

сумарну кількість отриманої інформації після всього циклу обробки дампів ОС;

- автоматизація роботи за планувальником завдань без участі «ззовні»;
- додавання повного журналювання процесу роботи скрипта і збирати налагоджувальну інформацію в разі якихось несправностей для максимально оперативного вжиття заходів і локалізації проблеми.

Цей проєкт призначений для спрощення і прискорення процедур ідентифікації призначення деяких серверів, на які можуть надходити скарги, а також ті сервери, які можуть використовуватися у вірусних кампаніях зловмисниками.

Бібліографічні посилання

1. Malware-as-a-Service: Who Can Put an End to It? URL: https://clario.co/blog/malware-as-a-service.
2. Command and Control [C&C] Server. URL : https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server.
3. Ботнет. URL : https://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82.
4. Spamhaus Botnet Threat Update: Q2-2021. URL : https://www.spamhaus.org/news/article/813/spamhaus-botnet-threat-update-q2-2021