of cyber protection of information and telecommunications systems (critical information infrastructure facilities) of critical infrastructure facilities of the state.
Key words: *objects of critical infrastructure of the state, set of criteria of criticality, critical information infrastructure.*

Дрейс Юрій Олександрович, кандидат технічних наук, доцент, старший науковий співробітник Національної академії СБ України.
Дрейс Юрий Александрович, кандидат технических наук, доцент, старший научный сотрудник Национальной академии СБ Украины.
Yurii Dreis, PhD in Eng. (Information security), Associate Professor, Senior Research Fellow of the National Academy of Security Service of Ukraine (Kyiv, Ukraine).

Деркач Леонід Васильович, старший науковий співробітник Національної академії СБ України.
Деркач Леонид Васильевич, старший научный сотрудник Национальной академии СБ Украины.
Leonid Derkach, General of the Army of Ukraine, Senior Research Fellow of the National Academy of Security Service of Ukraine (Kyiv, Ukraine).

Отримано *15 березня 2021 року*, затверджено редколегією *19 квітня 2021 року*

ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ / PRIVACY&PROTECTION FROM IDENTITY THEFT

DOI: 10.18372/2225-5036.26.15574

РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ЗА ДОПОМОГОЮ ПРИМАНОК У ХМАРНОМУ СЕРЕДОВИЩІ

Опірський Іван, Сусукайло Віталій, Василишин Святослав

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: професор кафедри захисту інформації з 2019 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com.
Orcid ID:0000-0002-8461-8996.

ВАСИЛИШИН Святослав Ігорович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 1995 рік, м. Львів, Львівська область, Україна.
Наукові інтереси: засоби захисту інформації в гібридних та кібер війнах, білий хакінг
E-mail: swat2244@gmail.com.
Orcid ID:0000-0003-1944-2979.

СУСУКАЙЛО Віталій Андрійович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 1995 рік, м. Львів, Львівська область, Україна.
Наукові інтереси: системи менеджменту інформаційної безпеки, системи дослідження кіберзлочинів.
E-mail: vitalii.susukailo@gmail.com.
Orcid ID:0000-0003-4431-9964.

Анотація. *Хмарні технології дедалі частіше використовуються. Хоча хмарне середовище може дати організаціям свободу експериментувати та масштабувати ресурси, воно також збільшує поверхню атаки. Ця стаття досліджує можливості приманок в хмарних середовищах. Аналізує проблему розслідування кіберзлочинів у хмарах. Визначає та вивчає відповідні технології, що використовуються фахівцями з кібербезпеки під час розслідування кіберзлочинів. Визначає переваги використання приманок у хмарній інфраструктурі. Для хмарних середовищ загрозою номер один є порушення даних. Порушення можуть завдати великої репутаційної та фінансової шкоди. Вони можуть потенційно призвести до втрати інтелектуальної власності та значних юридичних зобов'язань. Неадекватне управління доступом, у хмарному середовищі, загроза, що може призвести до компрометації хмарної системи. Щоб уникнути цієї загрози, клієнти хмари повинні захищати облікові дані, забезпечувати автоматичне обертання криптографічних ключів, паролів та сертифікатів, забезпечувати масштабованість, вимагати від адміністраторів хмарних служб використання багатофакторної автентифікації, визначати політику паролів для площини управління та кожної служби, розгорнутої в хмарі. Визначено, що рекомендується використовувати мережу "приманок" у хмарній службі як послугу (HaaS). Це дозволяє зменшити початкові та експлуатаційні витрати на підтримку Інфраструктури, підвищити ефективність розгортання системи та забезпечити можливість віддаленого управління.*

Ключові слова: *приманка, хмарне середовище, хмарна інфраструктура, кіберзлочинність, веб-служби Amazon, хмарна платформа Azure, IaaS, PaaS, SaaS.*

Вступ

Хмарні технології дедалі частіше використовуються. Хоча хмарне середовище може дати організаціям свободу експериментувати та масштабувати ресурси, воно також збільшує поверхню атаки.

Хмарна безпека є спільною відповідальністю хмарного провайдера та хмарного замовника. Залежно від моделі хмарного сервісу, обов'язки щодо захисту інформації повинні бути адекватно визначені та задокументовані.

Для моделей SaaS та PaaS постачальник відповідає за засоби контролю рівня інфраструктури, такі як виправлення послуг та операційної системи, управління уразливістю, зміцнення гіпервізора, фізичну безпеку центру обробки даних тощо.

Але в той же час це не означає, що клієнт не несе відповідальності за засоби захисту інформації. Клієнти хмарних служб, які використовують сервіси SaaS та PaaS, повинні дотримуватися рекомендацій щодо посилення постачальників та найкращих практик безпеки для програм чи служб, якими вони користуються.

Також необхідно регулярно проводити оцінку безпеки постачальника для оцінки засобів контролю, що надаються SaaS або постачальником послуг PaaS, щоб переконатися, що програма забезпечує відповідний контроль безпеки та відповідає вимогам міжнародних законів та норм.

Для Інфраструктури як моделі послуги, клієнт хмари відповідає за конфігурацію операційної системи, масштабування ресурсів, програмне управління мережами та підтримку рівня інфраструктури, крім фізичної безпеки, гіпервізорів, управління мережею та віртуальними машинами.

Це означає, що існує більше засобів контролю, які слід визначити для IaaS, таких як моніторинг безпеки, управління вразливістю, управління інцидентами, зміцнення операційної системи тощо. Це також відповідальність клієнта хмари за виявлення та відповідь на загрози хмарної безпеки та забезпечення належного захисту від кіберзлочинів. Існує безліч інструментів та технологій кібербезпеки, що надаються постачальниками хмарних послуг, які можуть виявити та запобігти кіберзлочинам. Тим не менш, у цій статті основна увага буде приділена надійним та зрозумілим рішенням для розслідування інцидентів у IaaS.

Загрози кібербезпеки для хмарних середовищ. Для хмарних середовищ загрозою номер один є порушення даних. Порушення можуть завдати великої репутаційної та фінансової шкоди. Вони можуть потенційно призвести до втрати інтелектуальної власності (ІВ) та значних юридичних зобов'язань. Неадекватне управління доступом, у хмарному середовищі, загроза, що може призвести до компрометації хмарної системи.

Щоб уникнути цієї загрози, клієнти хмари повинні захищати облікові дані, забезпечувати автоматичне обертання криптографічних ключів, паролів та сертифікатів, забезпечувати масштабованість, вимагати від адміністраторів хмарних служб використання багатофакторної автентифікації, визначати політику паролів для площини управління та кожної служби, розгорнутої в хмарі.

Ще однією поширеною загрозою хмарної безпеки є незахищені інтерфейси та API. API та користувальницькі інтерфейси часто є найбільш відкритими частинами системи, і це заохочує безпеку шляхом дизайнерського підходу до їх побудови.

Для забезпечення захисту від цих загроз компанія Cloud Security Alliance запропонувала такі засоби контролю:

– Повинні бути встановлені найкращі практики безпеки API, такі як нагляд за такими предметами, як інвентаризація, тестування, аудит та захист від ненормальної діяльності.

– Ключі API слід захищати, а також уникати повторного використання будь-якого ключа.

– Рекомендується використовувати відкриту структуру API, таку як Open Cloud Computing Interface (OCCI) або Cloud Infrastructure Management Interface (CIMI).

Відсутність архітектури та стратегії хмарної безпеки - ще одна критична загроза, яку слід враховувати при оцінці ризиків хмарних служб.

Архітектура безпеки повинна узгоджуватися з бізнес-цілями та завданнями, моделювання загроз слід проводити регулярно, а також слід забезпечувати постійний моніторинг для кожного типу моделі хмарних служб.

Ці засоби управління можуть допомогти організаціям забезпечити безпечну архітектуру для хмарної інфраструктури.

Зловмисники використовують законні хмарні сервіси для підтримки своєї діяльності. Хакери можуть використовувати популярний сервіс для зберігання зловмисного програмного забезпечення на таких веб-сайтах, як GitHub, тому для хмарних клієнтів дуже важливо контролювати вміст, що використовується їхнім хмарним рішенням.

Поширені локальні загрози застосовні до хмарних середовищ, такі як DDoS-атаки, видобуток цифрових валют, грубі атаки для викрадення облікових даних, використання вразливостей застарілого програмного забезпечення тощо.

Ці загрози повинні оцінюватися та пом'якшуватися клієнтами хмарних служб, щоб уникнути потенційної злочинності в хмарі, що спричинить підприємницьку шкоду.

Розслідування злочинів у хмарній безпеці за допомогою хмарного рішення безпеки. Розслідування злочинів у хмарній безпеці може здійснюватися за допомогою інструментів, наданих постачальником хмарних послуг.

Існує безліч технологій моніторингу, виявлення та реагування на безпеку, які можна використовувати для аналізу злочинів у хмарній безпеці та їх запобігання, а також сторонніх технологій, які можна використовувати в хмарному середовищі, таких як Splunk, стек ELK, LogRhythm тощо.

Але найпопулярніші постачальники хмарних послуг, такі як Amazon Web Services та Azure, мають вбудовані рішення для кібербезпеки.

Одним із рішень, яке можна використовувати для розслідування злочинів у хмарній безпеці, є Azure Log Analytics, технологія управління хмарними подіями Azure і частина Центру безпеки Azure.

Log Analytics є частиною загального рішення моніторингу Microsoft Azure. Log Analytics відстежує хмарне та локальне середовища для підтримки як кінцевих точок, так і доступності та продуктивності корпоративних служб. Azure Log Analytics як інструмент для дослідження подій у хмарному середовищі Azure може виконувати такі функції:

– Збір інформації - детальних поточних показників та журналів - із ресурсів Azure та місцевої інфраструктури.

– Візуалізація - вбудовані інформаційні панелі для візуалізації, які допоможуть швидко зрозуміти, що сталося.

– Аналіз - аналіз програм та інфраструктури.

– Відповідь - автоматична реакція на випадки.

– Інтеграція - використання 20+ партнерських інтеграцій та відкритої структури з API та SDK.

Azure Log Analytics може аналізувати будь-які завантажені в неї дані. Ця функціональність забезпечує аналіз системних та службових подій без обмежень, що дуже важливо для аналізу даних з кількох джерел під час розслідування інцидентів у хмарній безпеці. Також можна створити власні пошуки та правила оповіщення для автоматизації пошуку погроз та процесів розслідування інцидентів. Також усі журнали, що зберігаються на платформі Azure Log Analytics, можуть використовуватися для подальшої криміналістики.

Amazon Web Services мають власні засоби контролю безпеки, такі як Amazon Guard Duty та AWS Cloud Trail. Amazon представляє AWS CloudTrail як технологію, яка забезпечує історію подій активності облікового запису, включаючи дії, вжиті через площину управління, SDK AWS, інструменти CLI та інші служби Amazon. Історія викликів API спрощує аналіз безпеки, відстеження змін та усунення несправностей. Крім того, CloudTrail можна використовувати для виявлення незвичної активності в облікових записах Amazon. Amazon GuardDuty - це служба виявлення загроз, яка контролює зловмисні дії та несанкціоновану поведінку для захисту хмарних облікових записів, робочих навантажень та даних, що зберігаються в Amazon S3.

Служба використовує машинне навчання, виявлення аномалій та інтегровану інформацію про загрози для виявлення та визначення пріоритетів потенційних загроз. GuardDuty може аналізувати кілька подій у кількох джерелах даних AWS, таких як журнали подій AWS CloudTrail, журнали потоків Amazon VPC та журнали DNS. Обидва ці сервіси Amazon GuardDuty та Cloud Trail повинні ефективно розслідувати злочини хмарної безпеки в Amazon Web Services.Вбудовані технології моніторингу хмарної безпеки можна ефективно використовувати з іншими рішеннями безпеки для запобігання та виявлення кіберзлочинів хмарної безпеки.

Типи пасток, поведінка та ефективність у хмарному середовищі. Пастка принципово відрізняється від усіх подій у галузі безпеки. Як правило, усі продукти на цьому ринку розроблені для вирішення суворо визначеної функції (неважливо, чи йдеться про апаратне чи програмне забезпечення): брандмауер вирішує завдання обмеження доступу з однієї мережі в іншу на різних рівнях, SSH Послуга призначена для зашифрованого доступу до ресурсів операційної системи тощо.

Технологія приманки не призначена для вирішення конкретної проблеми, а представляє цілу філософію - гнучка, настроювана відповідно до мети. Як можна здогадатися, це не формалізований продукт чи технологія, а такий собі інструмент, щось на зразок мікроскопа в руках біолога.

Пастка надає фахівцям із безпеки значні переваги. Перш за все, це збір необхідної інформації, часто містить цінну інформацію. Розгортання та експлуатація приманок не представляє особливих труднощів, а інструменти пастки, як правило, не вимагають системних ресурсів.

Особливу увагу слід приділити встановленню та експлуатації пасток. Як правило, весь спектр заходів зводиться до "встановлення та очікування". Найпоширеніший випадок - із виділеним сервером під контролем фахівців.

Сьогодні існує багато фальшивих програм, які створюють враження справжніх, але не так, їх головне завдання - записати весь обмін. Перевага пастки полягає в тому, що копію програмного забезпечення можна зробити на морально застарілому сервері, який не може впоратися з типовими обчислювальними завданнями електронного бізнесу.

Залежно від рівня складності та його можливостей їх можна класифікувати на три групи: слабкі, середні та сильні рівні взаємодії:

1. Низький рівень: простий у використанні та дуже надійний. Вони імітують лише частину служб, і зловмисник буде обмежений у взаємодії з ними. Наприклад, вони можуть імітувати систему UNIX, на якій запущено telnet. Такі системи призначені для самих початківців зломщиків. Ризик використання пасток низького рівня мінімальний, але він є. Це пов'язано з тим, що саме програмне забезпечення теж є програмою; отже, воно може бути вразливим. Якщо його можна обійти, зловмисник отримає доступ до решти вузлів мережі. Сильною стороною цих найпростіших пасток у тому, що вони прості самі по собі. Відомо, що чим простіші, тим надійніші, тому ці програми мінімізують ризик, пов'язаний з можливою поломкою самої приманки і наступною поломкою системи.

2. Приманки середнього рівня надають більше можливостей для реконструкції зломщика, більш складного і, отже, більш вразливого. Наприклад, така система може моделювати більш складні веб-сервери, які можуть реагувати на нестандартні команди та мати більш досконалу систему логування. В UNIX ви можете використовувати можливості команд chroot, а в Windows - віртуальні машини VMWare. Таким чином, розширюється середовище зловмисника (тобто він зможе взаємодіяти не тільки з «підробленими» службами, але і з «підробленою» ОС), і це дасть більше можливостей для логування. Але такий підхід також створить більше проблем.

3. Високий рівень: надає максимум інформації про нападника і є максимально складними та небезпечними. Вони дають зловмиснику доступ до реальної системи, яка нічого не робить і не підключена до інших систем. Структура такої приманки найчастіше така: вузол приманки, мережевий датчик та сховище інформації. Такий вузол може бути розташований у мережі за брандмауером, і тоді фактичний контроль лежить на брандмауері. Якщо вузол приманки неправильно налаштований або трапляються якісь інші непередбачені ситуації, зловмисник зможе отримати доступ до мережі.

Одним з недоліків такого рішення може бути складність його реалізації та відносна вартість підтримки. Згідно з останніми дослідженнями загалом системи приманки мають високу оцінку та широко використовуються в різних організаціях.

Ідея пастки представлена в більш широкому розумінні - на рівні всієї мережі. Це певний вид приманки; однак така система складається не з одного комп'ютера або активного мережевого пристрою, а з цілої мережі.

Пастка - інструмент розслідування. Найцінніша причина розслідування кіберзлочинів через пастки у мережі - це інформація, яку вона надає; те, чого не може забезпечити жодна система виявлення та запобігання вторгнень.

Озброївшись інформацією та попередженнями, які вони реєструють, адміністратори мережі дізнаються про типи атак, на які вони націлені, та мають попередні знання, щоб зрозуміти, що їм потрібно зробити для посилення захисту.

Таблиця порівняння пасток показує відмінності між постачальниками в таблиці 1.

Існує два типи приманок:

1. Підприємницька «пастка» - це «пастка», яка розміщена у виробничому середовищі та служить інструментом для розслідування атак з метою використання знань для подальшого посилення безпеки мережі.

2. Дослідницька пастка - це «пастка», яка використовується дослідниками з надією вивчити методології нападу та інші характеристики, такі як мотиви нападу. Потім, наприклад, використовуючи знання для створення захисних рішень (антивірусів, антивірусів тощо), які можуть запобігти подібним атакам у майбутньому. Типи даних, які збирають (або подібне) зловмисники "пасток", можуть включати, але не обмежуючись ними:

1. Імена користувачів, ролі та привілеї, якими користуються зловмисники;

2. IP-адреси мережі або хоста, що використовуються для атаки;

3. Які дані досягнуті, модифіковані чи виключені;

4. Фактичні натискання клавіш набирання тексту, дозволяючи адміністраторам точно бачити, що вони роблять.

Пастки також допомагають утримувати увагу хакерів відверненою від головної мережі, запобігаючи повному обсягу атак, поки адміністратори не будуть готові вжити належних контрзаходів. Нарешті, ми повинні згадати плюси та мінуси використання пасток у вашій мережі.

Плюс: це недорогий захід безпеки, який може надати цінну інформацію про ваших зловмисників.

Мінус: не легко встановити та налаштувати, і божевільно пробувати це, не маючи під рукою експерта; це може дати негативні наслідки та піддати мережу найгіршим атакам.

Однак само собою зрозуміло, що приманки - це, мабуть, найкращий спосіб зловити хакера або атакувати, як це трапляється.

Це дозволяє адміністраторам пройти весь процес крок за кроком, стежачи за всім у реальному часі з кожним попередженням.

Таблиця 1

Порівняння пасток

Постачальник /	**Платформа**	**TrapX DeceptionGrid**	**Платформа**
Фейкові платформи ОС		Windows, Linux	Windows,Linux
Поетапне виявлення атаки	Активний інте-	Активний інтелект	Активний інтелект
Виявлення C&C	–	+	–
Виявлення MITM	–	+	–
Емульовані пастки	+	+	+
Промислові приманки	+	+	–
Інтеграція NAC	+	+	–
Повні пастки ОС	+	+	+
Інтеграція SIEM	+	+	+
Інтеграція кінцевої точки	+	+	+
EDR	+	+	+
Активна Директорія	+	+	+
Вбудована кореляція	+	+	+
Інтеграція пісочниці	–	+	–
База даних	–	+	+
POS	–	+	–
ATM	–	+	–
SCADA	+	+	+
IoT	+	+	+
Хмари	невідомо	AWS/Azure/OpenStack	–
Використання клієнтських зображень	+	+	+
Відкритий API для інтеграції	+	+	+
Виявлення ботнетів	–	+	Дорожня карта
Автоматичний аналіз коду	–	+	–
Конструктор пастки	–	+	+
Передача стану API	–	+	+
Колекція криміналістики	+	–	+
Роздача приманок справжнім господарям	+	–	+
Механізм створення приманки при AD	–	–	+
Інтеграція з системами оркестрації контейнерів	–	невідомо	+

Не потрібно глибокого втручання в мережеву інфра-	+	–	+
Можливість повного адміністративного доступу в ОС	+	–	+

Висновок

Основним завданням, яке вирішують фахівці з інформаційної безпеки на об'єктах інформаційно-телекомунікаційної інфраструктури, є збір інформації для запобігання атакам на об'єкти інформації, що захищаються. Раніше збір інформації проводився після виникнення інциденту з інформаційною безпекою, потім на основі отриманих даних були випущені "латки" та "латання дірок" в системі безпеки.

Єдиною інформацією, якою мали у своєму розпорядженні спеціалісти з інформаційної безпеки, була інформація, залишена в скомпрометованій системі. Як правило, цієї інформації дуже мало, і її не вистачає для запобігання подальшій загрозі безпеці захищених інформаційних ресурсів. Використання мережевих точок доступу для виявлення атак на захищені інформаційні ресурси дозволить зібрати якомога більше інформації про саму атаку та про цілі зловмисників, а також запобігти несанкціонованому доступу до захищених інформаційних ресурсів. Мережева пастка повинна працювати в стелс-режимі, щоб зловмисник не знав про її присутність.

В даний час існує стійка тенденція передачі обчислювальних потужностей хмарній інфраструктурі. Технологія хмарних обчислень - це технологія та бізнес наступного покоління.

Постачальники хмарних послуг повинні забезпечувати безпеку послуг, які вони надають. Підприємства прагнуть перенести свою інформаційну інфраструктуру на хмарні сервіси, але більшість з них не можуть дозволити собі загрози інформаційної безпеки.

Здебільшого існуючі хмарні служби пропонують стандартний набір засобів захисту інформації, таких як різні брандмауери, використання різних методів автентифікації, системи виявлення атак на основі аналізу підписів тощо.

Хмарні служби, в порівнянні з класичними інформаційними системами, є більш вразливими з точки зору шкоди.

У хмарному середовищі всі інформаційні ресурси взаємопов'язані та контролюються централізованими контролерами.

Якщо ви отримаєте доступ до одного інформаційного ресурсу в хмарі, всі інші знаходяться під загрозою. Замість того, щоб накопичувати різні системи безпеки у хмарній службі, ефективніше впроваджувати підроблені інформаційні ресурси.

Вирішити цю проблему пропонується за допомогою технології мережевої "приманки". Бажано використовувати мережу "приманок" у хмарній службі як послугу (HaaS). Це дозволяє зменшити початкові та експлуатаційні витрати на підтримку Інфраструктури, підвищити ефективність розгортання системи та забезпечити можливість віддаленого управління.

Список літератури

[1]. Vitalii Susukailo, Ivan Opirskyy, Sviatoslav Vasylyshyn, Analysis of the use of software baits as a means of ensuring information security, *2020 IEEE 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)*. – p. 242-245.

[2]. John Wiley. Carbon Black Special Edition, Inc. 111 River St. Hoboken, NJ 070305774. "*Threat Hunting For Dummies*®", 2017. – 53 p.

[3]. Huijun Wu, Dijiang Huang. *Mobile Cloud Computing: Foundations and Service Models (1st. ed.)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2017. – 336 p.

[4]. Jeff Petters. *Varonis. Endpoint Detection and Response (EDR): Everything You Need to Know*, 2017 [Електронний ресурс] – [Режим доступу] https:// www. varonis.com/blog/endpoint-security/.

[5]. Oleksandr Milov, Alexander Voitko, Iryna Husarova, Oleg Domaskin, Yevheniia Ivanchenko, Ihor Ivanchenko, Olha Korol, Hryhorii Kots, Ivan Opirskyy, Oleksii Fraze-Frazenko. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems, *Eastern-european journal of enterprise technologies. Information and controlling system*. – Vol 2, No 9(98), 2019. – pp. 56-66.

[6]. Khan, Z.A.; Abbasi, U. "*Reputation Management Using Honeypots for Intrusion Detection in the Internet of Things*". Electronics 2020, 9, 415. – 30 p.

[7]. Akiyama M., Yagi T., Hariu T., *Honey Circulator: distributing credential honeytoken for introspection of web-based attack cycle*. Int. J. Inf. Secur. 17, 2018. – pp. 135–151.

[8]. Rich Mogull, James Arlen, Francoise Gilbert, Adrian Lane, David Mortman, Gunnar Peterson, Mike Rothman *The Security Guidance for Critical Areas of Focus in Cloud Computing* v4.0, 2017 Cloud Security Alliance. – 152 p.

УДК 654.071

Opirskyy I.R., Vasylyshyn S.I., Susukailo V.A.. Investigating cybercrime with honeypots in the cloud

Abstract. *Cloud technologies are increasingly used. While a cloud environment can give organizations the freedom to experiment and scale resources, it also increases the surface area of attack. This article explores the possibilities of baits in cloudy environments. Analyzes the problem of investigating cybercrimes in the clouds. Identifies and studies relevant technologies used by cybersecurity professionals in the investigation of cybercrime. Determines the benefits of using baits in cloud infrastructure. For cloud environments, the number one threat is data breaches. Violations can cause great reputational and financial damage. They can potentially lead to the loss of intellectual property and significant legal obligations. Inadequate access control, in a cloud environment, is a threat that can compromise the cloud system. To avoid this threat, cloud clients must protect credentials, provide automatic rotation of cryptographic keys, passwords, and certificates, ensure scalability, require cloud service administrators to use multi-factor authentication, and define password policies for the management plane and each service deployed in the cloud. The trap provides significant benefits to security*

professionals. First of all, it is a collection of necessary information, often containing valuable information. Deployment and operation of baits is not particularly difficult, and trap tools usually do not require system resources. Particular attention should be paid to the insttion and operation of traps. As a rule, the whole range of measures is reduced to "establishment and expectation". The most common case is with a dedicated server under the supervision of specialists. Today, there are many fake programs that give the impression of real, but not true, their main task - to record the entire exchange. The advantage of the trap is that a copy of the software can be made on an obsolete server that cannot cope with the typical computational tasks of e-business. It is determined that it is recommended to use the network of "baits" in the cloud service as a service (HaaS). This reduces the initial and operating costs of maintaining the Infrastructure, increases the efficiency of system deployment and provides remote management.
Key words: *honeypot, cloud environment, cloud infrastructure, cybercrime, Amazon web services, cloud platform Azure, IaaS, PaaS, SaaS.*

Опирский И.Р., Василишин С.І., Сусукайло В.А. Расследование киберпреступлений с помощью приманок в облачной среде

Аннотация. *Облачные технологии все чаще используются. Хотя облачную среду может дать организациям свободу экспериментировать и масштабировать ресурсы, оно также увеличивает поверхность атаки. Эта статья исследует возможности приманок в облачных средах. Анализирует проблему расследования киберпреступлений в облаках. Определяет и изучает соответствующие технологии, используемые специалистами по кибербезопасности при расследовании киберпреступлений. Определяет преимущества использования приманок в облачной инфраструктуре. Для облачных сред угрозой номер один является нарушение данных. Нарушения могут нанести большой репутационный и финансовый ущерб. Они могут потенциально привести к потере интеллектуальной собственности и значительных юридических обязательств. Неадекватное управление доступом, в облачной среде, угроза, что может привести к компрометации облачной системы. Чтобы избежать этой угрозы, клиенты облака должны защищать учетные данные, обеспечивать автоматическое вращение криптографических ключей, паролей и сертификатов, обеспечивать масштабируемость, требовать от администраторов облачных служб использование многофакторной аутентификации, определять политику паролей для плоскости управления и каждой службы, развернутой в облаке. Определено, что рекомендуется использовать сеть "приманок" в облачной службе как услугу (HaaS). Это позволяет уменьшить начальные и эксплуатационные затраты на поддержание инфраструктуры, повысить эффективность развертывания системы и обеспечить возможность удаленного управления.*
Ключевые слова: *приманка, облачную среду, облачная инфраструктура, киберпреступность, веб-службы Amazon, облачная платформа Azure, IaaS, PaaS, SaaS.*

Опірський Іван Романович, доктор технічних наук, професор, професор кафедри захисту інформації Національного університету "Львівська політехніка".
Опирский Иван Романович, доктор технических наук, профессор, профессор кафедры защиты информации Национального университета "Львовская политехника".
Opirskyy Ivan Romanovych, Doctor of Technical Sciences, Professor, Professor of the Department of Information Security of the National University "Lviv Polytechnic".

Василишин Святослав Ігорович, аспірант, асистент кафедри Захисту інформації в національному університеті "Львівська політехніка".
Василишин Святослав Игоревич, аспирант, ассистент кафедры Защиты Информации в национальном университете "Львовская политехника".
Sviatoslav Vasylyshyn, postgraduate student, Assistant at the Lviv Polytechnic National University (Information security).
Сусукайло Віталій Андрійович, аспірант кафедри Захисту інформації в національному університеті "Львівська політехніка".
Сусукайло Виталий Андреевич, аспирант кафедры Защиты Информации в национальном университете "Львовская политехника".
Vitalii Susukailo, postgraduate student at the Lviv Polytechnic National University (Information security).

Отримано *15 березня 2021 року*, затверджено редколегією *19 квітня 2021 року*