УДК 004

І.Воропай, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВИЯВЛЕННЯ УРАЗЛИВИХ ДОДАТКІВ У МЕРЕЖЕВИХ CLOUD-СЕРВІСАХ

У статті розроблено програмне забезпечення, яке призначено для системи виявлення уразливих додатків у мережевих Cloud-сервісах. Метою розробки є дослідження та принципи побудови системи виявлення уразливих додатків у мережевих Cloud-сервісах. Об'єктом дослідження є процес виявлення уразливих додатків у мережевих Cloud-сервісах. Предметом дослідження є методи виявлення уразливих додатків у мережевих Cloud-сервісах. Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи виявлення уразливих додатків у мережевих Cloud-сервісах. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

уразливі додатки, Cloud-сервіси

Постановка проблеми. При розміщенні клієнтських додатків у хмарі необхідно передбачити міри захисту на випадок наявності в них уразливостей і інших недекларованих можливостей. Забезпечення безпеки хмарного сервісу – досить складне завдання. Зобов'язання щодо доступності сервісу й захищеності даних у ньому – невід'ємна частина пропозиції й важливий пункт SLA. Провайдери хмарних сервісів не скупляться на реалізацію засобів і мер інформаційної безпеки, оскільки захищеність забезпечує ним вагому конкурентну перевагу. Для цього використовуються антивірусні засоби, міжмережні екрани різних рівнів, системи протидії DDoS і запобігання вторгнень, різноманітні «пісочниці», SOC/SIEM і т.п. У гарному хмарному центрі є цілодобова служба моніторингу й відбиття атак, що складає із кваліфікованих фахівців. Однак забезпечення захисту стає куди більше складним завданням, коли хмарний провайдер надає своїм користувачам можливість розміщати їхні власні сервіси по моделі IaaS і PaaS. Тоді в системі, яка захищається, виникає шар клієнтських додатків, контролювати якість яких провайдер не в змозі. Уразливий додаток може стати проблемою не тільки для тих, хто його написав, але й для інших клієнтів хмарного провайдеру. Неодноразово вже виникали ситуації, коли атаці піддавався додаток, розміщений в центрі обробки даних, але під її впливом виявлялися недоступні всі додатки. Крім того, зламавши один додаток, наприклад одержавши до нього привілейований доступ, зловмисник здатний заразити й скомпрометувати інші в цій же хмарі. Як би не були ізольовані ресурси, керування ними (або їхньою частиною) нерідко здійснюється з одного центра.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи виявлення уразливих додатків у мережевих Cloud-сервісах.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи виявлення уразливих додатків у мережевих Cloud-сервісах.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем виявлення уразливих додатків у мережевих Cloud-сервісах.
- Дослідження системи виявлення уразливих додатків у мережевих Cloud-сервісах.

– Програмна реалізація системи виявлення уразливих додатків у мережевих Cloud-сервісах.

Об'єктом дослідження є процес виявлення уразливих додатків у мережевих Cloud-сервісах.

Предметом дослідження є методи виявлення уразливих додатків у мережевих Cloud-сервісах.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Загальнодоступні й приватні хмари піддаються як атакам зловмисників, так і збоям інфраструктури, наприклад, відключенням живлення. Такі події можуть вплинути на роботу серверів доменних імен, зробити хмара недоступним або прямо порушити функціонування хмари.

Наприклад, атака на Akamai Technologies, проведена 15 червня 2004 р., викликала проблеми з дозволом доменних імен і великий збій, що торкнувся Google Inc., Yahoo! Inc. і багато інших сайтів. У травні 2009 р. Google виявився метою серйозної DoS-атаки (denial-of-service), що вивела з ладу на кілька днів такі сервіси як Google News і Gmail.

Блискавка викликала тривалий простий Amazon.com Inc. 29 і 30 червня 2012. Хмара Amazon Web Services (AWS) у східному регіоні Сполучених Штатів, що складає з десяти центрів даних у чотирьох зонах доступності, спочатку випробовувала проблеми через коливання електроживлення, імовірно, викликаних грозою. 29 червня 2012 гроза на східному узбережжі США вивела з ладу деяку апаратуру Amazon, розташовану у Віргінії, що порушило роботу компаній, що використовувала системи тільки із цього регіону. Як повідомляють, однієї з жертв цього простою виявився сервіс обміну фотографіями Instagram.

Відновлення після цих подій зажадало багато часу й було пов'язане з рядом проблем. Наприклад, один з десяти центрів не зміг перемкнутися на запасні генератори до того, як сіли джерела безперебійного живлення (UPS). AWS застосувало «площини керування» (control planes), щоб дозволити користувачам перемкнутися на ресурси в інших регіонах, але цей програмний компонент також відмовив.

Процес початкового завантаження виявився недосконалим і збільшив час, необхідне для перезапуску сервісів Elastic Compute Cloud (EC2) і Elastic Block Store (EBS). Ще однією критичною проблемою став «баг» в Elastic Load Balancing (ELB), що служив для маршрутизації трафіку на сервери з доступними ресурсами. Аналогічний «баг» порушив процес відновлення Relational Database Service (RDS). Ця подія виявила «сховані» проблеми, які можуть відбутися тільки при особливих обставинах.

Частини хмари

Провайдер хмарних додатків, провайдер хмарного сховища й провайдер мережі можуть реалізовувати різні політики. Непередбачена взаємодія між балансувальником навантаження й інших реактивних механізмів може привести до втрати динамічної стійкості. Непередбачене сполучення незалежних компонентів, керуючих навантаженням, споживанням енергії й елементами інфраструктури може привести до виникнення небажаного зворотного зв'язка й нестабільності, аналогічно тому, як це може відбутися при маршрутизації, заснованої на політиках, при використанні Internet Border Gateway Protocol (BGP).

Наприклад, балансувальник навантаження провайдеру додатків може взаємодіяти з оптимізатором споживання енергії провайдеру інфраструктури. Деякі з таких сполучень можуть виникати тільки в надзвичайних ситуаціях, і їх буває дуже складно виявити при роботі в нормальних умовах. Це може привести до катастрофічних наслідків, коли система буде намагатися відновитися після серйозного збою, як це й відбулося в 2012 р. з AWS.

Кластеризація ресурсів у центрах даних, розташованих у різних географічних областях, – один із засобів, застосовуваних для зниження ймовірності катастрофічних збоїв. Такий географічний розподіл ресурсів може мати додатковий позитивний побічний ефект. Воно дозволяє скоротити трафік обміну інформацією й витрати на електрику, переводячи

обчислення в ті місця, де електроенергія дешевше. Також це може підвищити продуктивність за рахунок застосування інтелектуальної й ефективної стратегії балансування навантаження.

При організації хмарної інфраструктури ви повинні ретельно збалансувати мети системи, такі як максимальна пропускна здатність, використання ресурсів і фінансові переваги з потребами користувачів, такими як низькі витрати, низький час відгуку й максимальна доступність. За будь-яку оптимізацію системи доводиться платити ростом її складності. Наприклад, затримка при обміні інформацією через глобальну мережу (WAN) істотно більше, ніж у локальній мережі, і вимагає розробки нових алгоритмів глобального прийняття рішень.

Проблеми, що виникають при наданні хмарних послуг

Хмарні обчислення успадковують деякі із проблем від паралельних і розподілених обчислень. Але їм властиві й деякі власні проблеми. Конкретні проблеми відрізняються для трьох моделей надання хмарних послуг, але у всіх випадках вони обумовлені самою природою надання обчислювальних ресурсів як комунальних послуг, заснованого на спільному використанні й віртуалізації ресурсів, і потребуючу модель довіри, відмінну від повсюдно прийнятої моделі, орієнтованої на користувача, що довгий час була стандартом.

Сама значна проблема – безпека. Для майбутнього хмарної послуги надто важливо завоювати довіру великої кількості користувачів. Не можна розраховувати, що загальнодоступна хмара буде прийнятним середовищем для всіх додатків. Додатка підвищеної відповідальності, що управляють критично важливими інфраструктурами, додатка для охорони здоров'я й інші, швидше за все, будуть виконуватися в закритих хмарах.

Багато додатків, що працюють у реальному часі, також, швидше за все, помістять у закриті хмари. Деяким додаткам найкраще підійде гібридне хмарне середовище. Такі додатки можуть зберігати коштовні дані в закритій хмарі й використовувати загальнодоступну хмару для певних видів обробки.

У моделі Software as a Service (SaaS) виникають ті ж проблеми, що й в інших онлайнових послугах, що вимагає захисти особистої інформації, таких як фінансові або медичні послуги. У цьому випадку користувач взаємодіє із хмарними сервісами через чітко певний інтерфейс. Тому, у принципі, у провайдеру сервісів виникає менше складностей з перекриттям деяких каналів атаки (attack channels).

Проте, такі сервіси уразливі для DoS-атак і зловмисних внутрішніх користувачів. Найбільш уразливі для атак дані в сховище, тому приділите особливу увагу захисту серверів зберігання. Реплікація даних, необхідна, щоб забезпечити безперервність обслуговування при відмові систем зберігання, збільшує уразливість. Шифрування даних може захистити дані при зберіганні, але, в остаточному підсумку, дані прийде розшифрувати для обробки. І тоді вони будуть уразливі для атаки.

Модель Infrastructure as a Service (IaaS), безсумнівно, сама складна з погляду захисту від атак. Справді, користувач IaaS має набагато більше волі, чим у двох інших моделях надання хмарних послуг. Додаткове джерело проблем – те, що чимала кількість хмарних ресурсів можна задіяти для атаки на мережу й інфраструктуру обчислень.

Украй важливою архітектурною особливістю цієї моделі є віртуалізація, але вона робить системи підданими новим видам атак. Довірена обчислювальна база (trusted computing base, TCB) віртуального середовища містить не тільки встаткування й гіпервізор, але й керуючу ОС. Можна зберегти стан всієї віртуальної машини (VM) у файл, щоб її було можна переносити й відновлювати – підтримка цих двох операцій дуже бажана.

Проте, ця можливість ускладнює стратегії по змісту серверів, що належать організації, у необхідному стабільному стані. Справді, заражена VM може бути неактивної під час перевірки систем. Потім вона почне працювати й заразить інші системи. Це – ще один приклад того, як у базових технологіях хмарних обчислень сполучаються корисні й шкідливі ефекти.

Наступна істотна проблема пов'язана з керуванням ресурсами хмари. Кожне стратегія систематичного керування ресурсами (на відміну від керування по ситуації) вимагає

існування керуючих компонентів, призначених для реалізації декількох класів політик: керування доступом, виділення ресурсів, балансування навантаження, оптимізації енергоспоживання й – останнє один по одному, але не по важливості – надання гарантій якості обслуговування (quality of service, QoS).

Щоб реалізувати ці політики, що управляють компоненти повинні мати точну інформацію про глобальний стан системи. Визначення стану складної системи з 106 або більше серверами, розподіленими по великій території, – нездійсненне завдання. Справді, зовнішнє навантаження, а також стан окремих ресурсів, дуже швидко міняються. У результаті керуючі компоненти повинні функціонувати в умовах неповного або приблизного знання про стан системи.

Здається розумним очікувати, що така складна система може функціонувати тільки на основі принципів самоврядування. Але самоврядування й самоорганізація підвищують вимоги до реалізації процедур ведення журналів і аудита, критично важливих для забезпечення безпеки й довіри до провайдеру хмарних обчислень.

При самоврядуванні стає майже неможливим ідентифікувати, з яких причин почате та або інша дія, через якого виник пролом у захисті.

Остання велика проблема, що я торкнуся, пов'язана із сумісністю й стандартизацією. Залежність від постачальника – той факт, що користувач «прив'язаний» до певного постачальника хмарних послуг – серйозна проблема для хмарних користувачів. Стандартизація забезпечує сумісність і, отже, у якімсь ступені, рятує від побоювань, що сервіс, критично важливий для великої організації, буде недоступним протягом тривалого часу.

Уводити стандарти в період, коли технологія ще розвивається, складно, і може виявитися контрпродуктивним, оскільки, можливо, це буде перешкоджати нововведенням. Важливо усвідомлювати складність проблем хмарних обчислень і розбиратися в цілому ряді технічних і соціальних проблем, що виникають при хмарних обчисленнях. Зусилля по переносу IT-операцій у загальнодоступні й закриті хмари, виправдаються в довгостроковій перспективі.

АНБ могло використовувати Logjam для атаки на VPN сервери

Безліч хмарних сервісів піддаються недавно знайденої в TLS-протоколі уразливості за назвою Logjam (CVE-2015-4000), повідомляє компанія по інформаційній хмарній безпеці Skyhigh.

Logjam дуже нагадує уразливість FREAK, однак відрізняється тим, що замість ініціювання зміни шифрів RSA на RSA_EXPORT в Logjam виробляється відкат протоколу Діффі-Хеллмана, використовуваного для одержання ключа для подальшого шифрування, до слабозахищеного рівня DHE_EXPORT. Уразливість може бути проексплуатована для здійснення атаки «людина по-середині», що дозволить одержати доступ до даних, що проходять через TLS-З'єднання.

Logjam вражає всі сервери, які підтримують 512-бітне експортне шифрування, а також всі сучасні браузери. Відповідно до експертів, більше 8% з Топ-мільйона web-сайтів, що використовують HTTPS, і більше 3% ресурсів, відображуваних у браузері як заслуговують довіри, піддані даної уразливості.

У ході атаки з експлуатацією Logjam зловмисники можуть знизити стійкість шифрування в мільйонів HTTPS, SSH і VPN серверів, які підтримують DHE_EXPORT і використовують для генерації ключа прості 512-розрядні групи початкових чисел Діффі-Хеллмана.

На думку фахівців Skyhigh, команда вчених може зламати 768-бітне просте число, а група хакерів, фінансована державою, може замахнутися на 1024-бітне. Злом єдиного, найпоширенішого 1024-бітного простого числа, використовуваного web-серверами, дозволить прослуховувати підключення до 18% з мільйона найбільш популярних HTTPS-сайтів. Експерти вважають, що АНБ могло використовувати Logjam для атаки на VPN сервери.

Злом хмарних сервісів: Соціальний інжиніринг у дії

Захисне програмне забезпечення сучасних комп'ютерів – антивіруси, файрволи, антишпигуни, антиспамові рішення, системи виявлення вторгнень і т.д. – виконує завдання будь-якої навіть найвищої складності, але всіма цими високотехнологічними рішеннями управляти набагато легше, ніж людьми. Як би складним не було програмне забезпечення, будь-який фахівець із області інформаційної безпеки з легкістю підтвердить, що сама слабка ланка в будь-якій захисній системі – це людський фактор.

В останні роки в багатьох країнах одержав поширення соціальний інжиніринг, тобто метод керування діями людини без використання технічних засобів, заснована на використанні людських слабостей. Пояснення сутності соціального інжинірингу й, зокрема, таких його різновидів, як гіпноз і нейролінгвістичне програмування (НЛП), гідно окремої статті, саме головне, що ключем до розуміння уразливості людського фактора, є взаємодія між свідомістю й підсвідомістю. Люди вірять у те, що приймають рішення усвідомлено, але НЛП і гіпноз уже давно продемонстрували силу підсвідомості, а дослідження останнього років підтвердили, що підсвідоме прийняття рішень випереджає свідоме часом на 10 секунд.

На цьому засновані технології, що дозволяють маніпулювати людьми, щоб змусити їх виконати певні дії й тим самим розкрити конфіденційну інформацію. Розглянемо, як такі методи можуть бути використані для злому хмарних систем.

Приклади несанкціонованого доступу до даних

Дослідницькою групою були внесені зміни в роботу сайту – про це знало керівництво компанії, який належав сайт, але IT-фахівці не були попереджені. Для того щоб користувач міг працювати з електронною поштою, на додаток до звичайної вимоги відповістити на секретне запитання система попросила ввести ім'я користувача й пароль. Як результат, протягом години було уведено 25% логінів/паролів. Крім того, пройшло 2 години, перш ніж IT-команда зміркувала, що відбувається, і ще 2 години, перш ніж фахівці компанії змогли опублікувати попередження для користувачів. Незважаючи на вжиті заходи, облікових даних користувачів надходили ще кілька годин після того, як було розіслане попередження.

В іншому випадку дослідницька група зареєструвала домен, дуже схожий на домен цільової компанії. Потім всім співробітникам компанії був розісланий лист, що описує нову процедуру уведення пароля, у результаті чого співробітники попадали на фальшивий сайт компанії. Адреса підробленого сайту, що містить схожий з реальним домен, відкрито розміщався в листі; дослідники не робили спроб замаскувати URL. Як і передбачалося, більшість співробітників, що одержали лист, слухняно виконали зазначені дії.

Ще одне дослідження показало, що наявність строгих процедур у процесі внесення змін в адміністративний інтерфейс також є уразливим місцем системи безпеки через відсутність гнучкості. Тобто, якщо хакеру вдається реалізувати позаштатну ситуацію, користувач, швидше за все, буде шукати шляхи до її виправлення, і зловмисникові залишиться тільки «підказати» йому відповідь. Таким чином, часто строгі алгоритми роботи системи відкривають особам, які у достатній мері володіють методами соціального інжинірингу, доступ до конфіденційної інформації компанії.

У цілому експерименти показали, що користувачі не просто не бачать різниці між офіційним і підробленим доменом, проблема набагато глибше. Незважаючи на регулярно проведені в компаніях тренінги й впроваджувані навчальні програми, більшість співробітників воліє знайомитися не з усіма методами виявлення й протидії вторгненням, а лише з тими, які для них важливі, приміром, особливо популярні можливості безпечного онлайн-банкинга й роботи з відомими онлайн-аукціонами. Таким чином, співробітники компаній своїми діями підтвердили, що не очікують фішинг-атак, спрямованих на їхні робітники дані, хоча й знають, що така атака можлива.

Лов на живця

Зрозуміло, розроблювачі програмного забезпечення не можуть повною мірою враховувати людський фактор, але для того, щоб визначити найбільш уразливі місця в системі безпеки окремо взятої компанії, як ні парадоксально, не обійтися знову ж без

допомоги користувачів. Мова йде про імітацію хакерських атак на систему замовника, результати яких дадуть клієнтові механізм для виміру ефективності поточного захисту системи від соціального інжинірингу. Під атакою, таким чином, розуміються різні тестові сценарії, які призначені для оцінки успішності/неуспішності системи.

Певні труднощі представляє розробка подібних атак, оскільки, по-перше, атакувати потрібно не якого-небудь із користувачів, а безпосередньо службу підтримки, змушуючи її надати хакеру права адміністратора, а по-друге, потрібно досить точно й швидко визначити сектор системи для перевірки, щоб не затягувати процес і швидше ліквідувати уразливість.

Злом хмарного сервісу

Здійснювану в дослідницьких цілях атаку можна розділити на кілька фаз. Протягом першої – відбувається збір початкових даних про систему, приміром, про розташовані в інших країнах підрозділах, про територіальне покриття службою підтримки, інформації про клієнтів, а також збір відомостей про топ-менеджерів і директорів компанії.

Друга фаза містить у собі доступ до мереж компанії в нічний час доби, для того щоб оцінити, що відбувається із системою безпеки у відсутності адміністраторів, а також для того, щоб при необхідності змінити IP-адреса. Також у другій фазі відбувається збір даних про недавно зроблені звільнення й скорочення співробітників, а заодно перевіряється, чи внесли адміністратори відповідні зміни в систему. На третьому етапі дослідниками беруться під контроль облікові записи керуючих і технічного директорів цільової компанії. На четвертому здійснюється контакт зі співробітниками, щоб домогтися їхнього особистого розташування.

Результат експериментальної атаки перевершив всі очікування дослідників: вони домоглися бажаного всього за три цілеспрямованих телефонних дзвінка з використанням психологічних методів соціального інжинірингу в підрозділи компанії – у Великобританії, США й у Китаї. Спочатку керуючий директор подзвонив у британський офіс компанії незадовго до закінчення робочого дня, попередив про можливі проблеми й запросив інформацію про доступ до підтримки, але, відпрацьовуючи сценарій зловмисника, не просив відкрити йому доступ у систему. Другий дзвінок надійшов в офіс у США від клієнта керуючого директора, що просив внести зміни в логін і пароль, пояснюючи це тим, що в нього виникли труднощі з доступом у систему. Третій дзвінок надійшов у китайський офіс компанії від технічного директора компанії, що перебуває в надзвичайних обставинах.

Внаслідок атаки дослідникам удалося обійти строгі процедури забезпечення безпеки; співробітники компанії представили дослідникам подробиці облікових записів; трафік удалося перенаправляти на нову адресу, і в цьому був задіяний співробітник компанії; по телефоні був продиктований новий пароль адміністратора. Надзвичайно важливо, що ніхто зі співробітників не спробував установити особистість що дзвонила.

Учасники експерименту, з огляду на характер атаки, відсутність аудита й повідомлень про зміни в системі, прийшли до виводу, що в результаті вторгнення реальних хакерів несанкціонований доступ міг залишатися непоміченим протягом тривалого часу. Таким чином, незважаючи на те, що хмарна система є технічним рішенням, подібні сервіси залежать від людського фактора так само, як більшість систем інформаційної безпеки. Як підтвердив експеримент, соціальний інжиніринг виявився найшвидшим і легенею шляхом до порушення інформаційної безпеки й самим трудновизначаємим. Методи соціально інжинірингу, на відміну від електронного злому сайтів, майже неможливо каталогізувати, а вплив доводиться оцінювати, покладаючись на показання свідків співробітників, що стали жертвами, причому треба враховувати, що вони можуть псувати реальність, бажаючи врятувати свою репутацію.

У список найпоширеніших застосувань хмарних сервісів входять: зберігання сканів паспорта й інших особистих документів; синхронізація бази паролів, контактів, листів; створення сайтів; зберігання версій вихідних кодів і т.д. Коли хмарний сервіс зберігання даних Dropbox повідомив про закриття уразливості в генераторі посилань, в інтернеті знову заговорили про те, як важливо шифрувати конфіденційні дані, перш ніж викладати їх на

який-небудь ресурс, навіть якщо він приватний. Шифрування файлів (FLE) дійсно дозволить забезпечити захист конфіденційної інформації в хмарі, навіть у випадку виявлення уразливостей контролю доступу до документів користувачів у тім або іншому хмарному сервісі.

Може зложитися враження, що якщо не викладати в хмари секретні дані, або їх шифрувати, то й ризиків ніяких не буде. Чи не так це? Як виявилося, не зовсім.

В інтернеті часто зустрічаються рекомендацій з «ефективного використання хмарних файлових сервісів», наприклад – інструкції з вилученого керування комп'ютером, стеженню за комп'ютером під час своєї відсутності, керування torrent-завантаженнями й багато інше. Інакше кажучи, користувачі самі створюють усілякі діри, якими з легкістю скористається й троянець, і хробак, і тим більше хакер, особливо якщо мова йде про цільові атаки.

Ми задалися питанням – наскільки великий ризик зараження корпоративної мережі через хмарний сервіс?

Спочатку, використовуючи фішинг, розроблювач заразив ноутбук співробітника, далі – впровадив шкідливі скрипти в документи, що зберігаються в «хмарній» папці ноутбука. Dropbox автоматично обновив (синхронізував) заражені документи на всіх пристроях, пов'язаних з аккаунтом користувача. Щодо цього Dropbox не унікальний – функція автоматичної синхронізації є у всіх популярних додатках для доступу до хмарних файлових сервісів, у тому числі Onedrive (він же Skydrive), Google Disk, Yandex Disk і т.д.

Коли користувач відкрив заражений документ на робочому комп'ютері, що перебуває в корпоративній мережі, впроваджені в документ скрипти встановили в систему бекдор DropSmack, створений розроблювачем спеціально для цього пен-тесту. Як можна догадатися за назвою, ключова особливість DropSmack – використання хмарного файлового сховища Dropbox як канал для керування бекдором і передачі корпоративних документів назовні крізь корпоративний файервол.

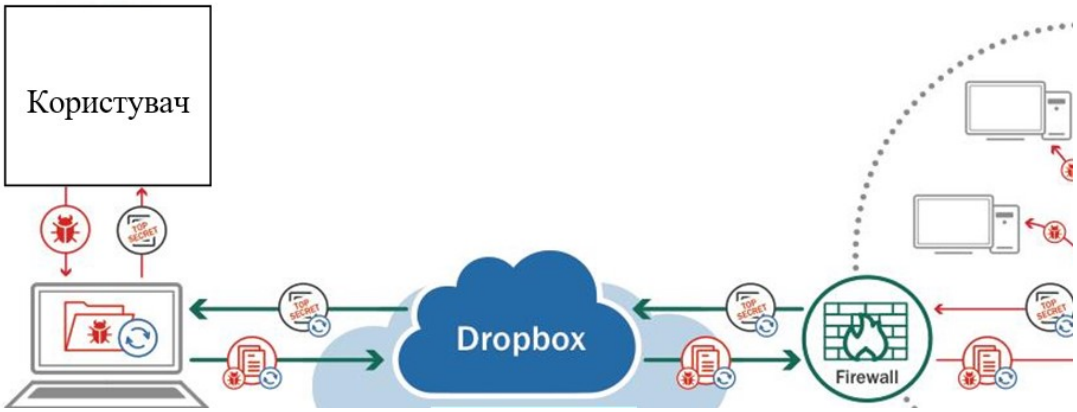

Рисунок 1 – Структурна схема системи

Метод проникнення в корпоративну мережу, використаний розроблювачем у ході пен-тесту, дивує своєю простотою – так, це очевидна діра!

Ми вирішили перевірити, чи використовують справжні зловмисники Dropbox, OneDrive, Yandex Disk і Google Disk для поширення шкідливого ПЗ. Зібравши інформацію з KSN про детектах вірусів, виявлених в «хмарних» папках на комп'ютерах користувачів, ми з'ясували, що такі зараження зафіксовані в дуже невеликого числа користувачів: у травні цього року тільки 8,7 тис. чоловік зштовхнулися із зараженням «хмарної» папки. У користувачів домашніх продуктів ПК на такі шкідливі програми доводиться 0,42% всіх детектів, у користувачів корпоративних продуктів – 0,24%.

Слід зазначити одну немаловажну деталь – якщо вірус потрапив у хмару з одного пристрою, всі підключені до зараженого аккаунту клієнти самі завантажать його на свої пристрої, так ще й по протоколі HTTPS. Навіть якщо на одному із пристроїв антивірус

помітить і видалить заразу прямо в папці синхронізації, хмарний клієнт буде, з обов'язку служби, боротися зі сформованої рассинхронізацією, без кінця завантажуючи вірус із хмари.

За нашим даними, близько 30% шкідливого ПЗ, виявленого в «хмарних» папках на домашніх комп'ютерах, попадає на комп'ютери через механізми синхронізації! У корпоративних користувачів цей показник досягає 50%. Таким чином, механізм, що використовувався демонстраційним вірусом розроблювача, приводить до заражень у реальному житті. На щастя, ми поки не виявили цільових атак з використанням хмарних сервісів зберігання даних.

Серед шкідливого ПЗ, виявленого нами в «хмарних» папках на комп'ютерах користувачів, переважають файли форматів Win32, MSIL, VBS, PHP, JS, Excel, Word, Java. Варто відзначити, що між корпоративним і домашнім користувачами є невелика різниця – у перших частіше зустрічаються заражені файли MS Office, у других у списку є унікальні звірі – шкідливі Android-додатка.

Найчастіше вирусописувачі використовують хмарні сховища не як платформу для поширення, а в якості хостингу для шкідливих програм – у ході дослідження ми не зустріли жодного хробака або бекдора (не вважаючи DropSmack), спеціально націленого на хмарні файлові сховища. Звичайно, самі сервіси намагаються активно боротися зі шкідливими програмами, які займають вільне місце в хмарі. Крім того, хостинг шкідливих програм негативно впливає на репутацію сервісу, хоча формально хмарні сервіси й не несуть відповідальності за те, які файли завантажуються клієнтами в сховище. Очевидно, що регулярне сканування всіх файлів, що втримуються в хмарі, зажадає занадто багато ресурсів, які сервісам вигідніше використовувати для зберігання даних.

Підсумком проведеного дослідження стало розуміння, що ризик зараження корпоративної мережі через хмарне сховище порівняно невеликий – протягом року заразитися ризикує 1 з 1000 корпоративних користувачів, що використовують хмарні сервіси. Однак треба враховувати, що в деяких випадках навіть одиничне зараження комп'ютера в корпоративній мережі може привести до значного збитку.

Можливі міри захисту корпоративної мережі:

– Підсилити захист в Firewall/IDS, заблокувати доступ до серверів відомих сервісів. Більшим мінусом такого підходячи є більша ресурсоємність – необхідно уважно стежити, чи не з'явилися нові кандидати в «чорний список».

– Установити багатофункціональний Security Suite, що включає в себе евристичний і поведінковий антивірус, функції обмеження доступу (HIPS), контроль за роботою операційної системи (System Watcher або Hypervisor), захист від експлуатації уразливостей і т.д. При цьому необхідно ретельно все настроїти.

– Тому що навіть самий навернений Security Suite може пропустити APT, варто звернути увагу на технологію Контроль додатків (у режимі «Заборонено за замовчуванням»). Це, мабуть, один із самих надійних засобів, що дозволяє заблокувати будь-яке невідоме ПЗ (у тому числі розповсюджуване в ході цільової атаки). Саме складне завдання, що виникає під час впровадження Контролю додатків, – настроїти відповідні правила, щоб всі дозволені додатки запускалися й обновлялися без проблем. Для цього виробниками продуктів з функцією Контролю додатків були розроблені спеціальні інструменти – функція відновлення ПЗ через довірені програми відновлення, передвстановлені списки білого ПЗ, що включають всі можливі системні й користувальницькі файли, доступ до величезних хмарних сервісів і баз інформації про все різноманіття білого ПЗ.

– В особливих випадках, варто використовувати «Контроль додатків», щоб обмежити використання хмарних клієнтів у корпоративній мережі, тобто дозволити запуск додатків синхронізації «хмарної» папки тільки довіреним співробітникам.

Ну, а для самих-самих закритих систем, таких, які управляють роботою електростанцій, систем водопостачання, зберігають держтайну або дозволяють запускати міжконтинентальні ракети – настійно рекомендуємо повністю відмовити від використання хмарних файлових сховищ.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів виявлення уразливих додатків у мережевих Cloud-сервісах. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем виявлення уразливих додатків у мережевих Cloud-сервісах.

– Досліджена система виявлення уразливих додатків у мережевих Cloud-сервісах.

– На основі отриманих результатів досліджень створена програмна реалізація системи виявлення уразливих додатків у мережевих Cloud-сервісах. Розроблені алгоритми дозволяють успішно вирішувати завдання виявлення уразливих додатків у мережевих Cloud-сервісах. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». Cybersecurity Defensive Walls in Edge Computing, 2025. pp. 21-61.
2. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». Ceur Workshop Proceedings, 2025, 4024, pp. 530–542.
3. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.
4. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025
5. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
6. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
7. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
8. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
9. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
10. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
11. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
12. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
13. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
14. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
15. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.

16. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
17. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
18. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56
19. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
20. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
21. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
22. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
23. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
24. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
25. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
26. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
27. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
28. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
29. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
30. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
31. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
32. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.