відбувається при виході об'єкта із зони спостереження ближньої IP-камери.

Система індивідуальної зйомки передбачає доповнення створюваного фільму-звіту фрагментами індивідуальної IP-камери. Для цього особа яка веде спостереження повинна мати IP-камеру якщо існує покриття Wi-Fi, або камеру, сполучену з мобільним телефоном по якому передавати відео потік. При цьому фрагменти індивідуальної IP-камери через засоби мобільного оператора або через Wi-Fi канали зв`язку будуть автоматично вмонтовані у фільм-звіт.

Розглядаються напрямки використання видеофіксації переміщень об`єкта.

Перше це спостереження за об`єктом. Другий напрям це збір доказової бази присутності об`єкта в даному місті в даний час. Яка може бути використана як для звинувачення підозрюваного, так і для його захисту. Третій напрям це пошук свідків подій. Які мають мобільні телефони і знаходились в полі зору веб-камери.

Висновок. Удосконалення системи відеоспостереження дозволяє більш ефективно реалізовувати роботу правоохоронних органів. Система дозволить підвищити ефективність діяльності поліції в протидії торгівлі людьми. Система запатентована авторами [1].

Список бібліографічних посилань

1. Мордвинцев М. В., Машкаров Ю. Г. Спосіб відео документування переміщень об`єкта за допомогою системи відеофіксації. Патент на корисну модель № 73635, 2012. 4 с.

2. Мордвинцев М. В. Удосконалення систем видеоспостереженя при реалізації завдань правоохоронних органів. *Международный научный журнал.* 2016. № 5. С. 59-61. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/mnj_2016_5(1)__17.pdf (дата звернення: 29.10.2018).

Одержано 29.10.2018

УДК 004.056.5

Ярослав Віталійович ОСІПОВ,
курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ;
Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук,
доцент кафедри кібербезпеки факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ
ORCID: https://orcid.org/0000-0003-3381-3350

АТАКА НУЛЬОВОГО ДНЯ (N-DAY ATTACK). ЩО ЦЕ І ЯК З ЦИМ БОРОТИСЯ?

Вступ і постановка проблеми. Даний термін застосовують щоб визначити не усунутий уразливості, що не знайдені розробниками

«дірки» в програмному коді на стадії тестування. А також шкідливі програми, віруси, мережеві черв'яки, боти і трояни проти яких ще не розроблена хоч якогось захисту. Із самої назви зрозуміло, що у розробників не було ні дня, тобто, не було ніякої можливості виправити помилки і прорахунки в коді, вони про них просто не знали. Про уразливості стає відомо до того моменту, коли виробник програмного забезпечення випустить оновлення з виправленням, або нову версію програми. Тобто до цього моменту, всі комп'ютери, що працюють з цим.

Атака з нульовим днем – це небезпека від якої неможливо захиститися, тому що неможливо захиститися від того, що не знаєш.

Нульовий день – недолік програмного забезпечення, апаратного або програмного забезпечення, який невідомий стороні чи сторонам, відповідальним за виправлення чи інше виявлення недоліків. Термін «нульовий день» може відноситись до той самої вразливості або атаки, яка має нульові дні від часу виявлення вразливості та першої атаки. Після того, як вразливість на нульовий день була оприлюднена, вона відома як n-day або одноденна вразливість.

Зазвичай, коли хтось виявляє, що програма містить потенційну проблему безпеки, ця особа або компанія сповістять компанію про програмне забезпечення (а іноді і в цілому світі), щоб зробити це. Потенційні атакуючі чують про вразливість, можливо, знадобиться деякий час для його використання. Однак іноді хакер може бути першим, хто виявить вразливість. Оскільки вразливість невідомо заздалегідь, не існує способу захищатись від експлуатації, перш ніж це станеться. Компанії, що піддаються подібної експлуатації можуть, проте, запровадити процедури для раннього виявлення. Співробітники служби безпеки співпрацюють з постачальниками і зазвичай погоджуються утримувати всі деталі вразливостей до нульового часу протягом розумного періоду перед публікацією цих даних. Наприклад, *Google Project Zero* дотримується рекомендацій галузі, які надають постачальникам до 90 днів для виправлення вразливості перед тим, як шукач цієї уразливості публічно розкриває недолік.

Підвищення нульового дня, як правило, дуже важко виявити. Програмне забезпечення *Antimalware* та деякі системи виявлення вторгнень (*IDS*) та системи захисту від вторгнень (*IPSes*) часто неефективні, оскільки жодна атака не існує. Ось чому найкращим способом виявлення атаки з нульовим днем є аналіз поведінки користувачів. Більшість організацій, уповноважених отримувати доступ до мереж, демонструють певні моделі використання та поведінки, які вважаються нормальними. Діяльність, що виходить за рамки звичайного обсягу операцій, може бути показником атаки з нульовим днем. Деякі атаки з нульовим днем були пов'язані з акторами з найсучаснішою постійною загрозою (APT), групами зловмисників або кіберзлочинність, пов'язаними з частиною національних урядів. Зловмисники, особливо APTs або організовані групи з використанням

кіберзлочинності, як вважають, резервувати свої нульовий день подвиги для цінних цілей. Уразливості N-day продовжують жити і піддаються експлуатації довго після того, як вразливості були виправлені чи іншим чином встановлені постачальниками.

Захист проти атак нульового дня. Нульові дні подвиги важко захистити, тому що їх важко виявити. Програмне забезпечення для сканування уразливості спирається на перевірки підписів на шкідливі програми для порівняння підозрілого коду з підписами відомих шкідливих програм; коли шкідлива програма використовує експлуатацію з нульовим днем, яка раніше не зустрічалася, такі сканери уразливості не зможуть блокувати шкідливе програмне забезпечення. Оскільки нульове значення вразливості не може бути відомо заздалегідь, неможливо захиститись від конкретної експлуатації, перш ніж це станеться.

Однак існують деякі речі, які компанії та прості люди можуть зробити, щоб зменшити рівень ризику:

– використовуйте віртуальні локальні мережі, щоб відокремити деякі області мережі або використовувати спеціальні сегменти для фізичної або віртуальної мережі для ізоляції;

– впровадити IPsec, IP-протокол безпеки, щоб застосувати шифрування та автоідентіфікацію до мережевого трафіку;

– розгортання IDS або IPS. Незважаючи на те, що підписані продукти безпеки IDS та IPS, можливо, не зможуть ідентифікувати атаку, вони можуть повідомити захисників про підозрілу активність, яка виникає як побічний ефект від нападу;

– використовуйте контроль доступу до мережі, щоб запобігти викраденням машин із важливих частин середовища підприємства;

– блокування вниз точок бездротового доступу та використання схеми захисту, наприклад Wi-Fi Protected Access 2, для максимального захисту від атак на базі бездротових мереж;

– зберігайте всі системи та оновлюйте їх. Хоча патчі не припиняють атаки з нульовим днем, зберігаючи ресурси мережі повністю, це може ускладнити напад. Коли патч нульового дня стає доступним, застосуйте його якомога швидше;

– виконуйте регулярну сканування вразливостей проти корпоративних мереж і закрийте будь-які виявлені уразливості.

Підтримуючи високі стандарти безпеки інформації, це не може запобігти експлуатацію з нульовим днем, це може допомогти поразки атак, які використовують експерименти з нульовим днем після виправлення вразливостей.

Приклади атак нульового дня:

1) кілька атак на нульовий день зазвичай трапляються щороку. У 2016 році, наприклад, з'явився атака з нульовим днем (CVE-2016-4117), яка експлуатувала раніше нерозкритий вади Adobe Flash Player. Також в 2016 році більш ніж 100 організацій піддалися нульовій помилці дня (CVE-2016-0167), яка експлуатувалася для підвищення нападу привілеїв, націлених на Microsoft Windows;

2) у 2017 році була виявлена вразливість нульової доби (CVE-2017-0199), в якій було показано, що документ Microsoft Office у формі багатофункціонального тексту може викликати виконання відкритого базового сценарію, що містить команди PowerShell. Ще одна експлуатація 2017 (CVE-2017-0261) використовувала вбудований PostScript як платформу для ініціації інфікування.

Висновок. У зв'язку із застосуванням спеціальних технологій, 0day-загрози не можуть бути визначені класичними антивірусними технологіями. Саме з цієї причини продукти, в яких зроблена ставка на класичні антивірусні технології, показують досить посередній результат в динамічних антивірусних тестуваннях. На думку антивірусних компаній, для забезпечення ефективного захисту проти 0day шкідливих програм і вразливостей потрібно використовувати активні технології антивірусного захисту. Завдяки специфіці активних технологій захисту вони здатні однаково ефективно забезпечувати захист як від відомих загроз, так і від 0day-загроз. Хоча варто відзначити, що ефективність проактивного захисту не є абсолютною, і вагома частка 0day-загроз здатна завдати шкоди жертвам зловмисників. Незалежних підтверджень цим твердженням на даний момент немає.

Список бібліографічних посилань

1. Уязвимость нулевого дня // Вікіпедія: вільна енциклопедія. URL: https://ru.wikipedia.org/wiki/Уязвимость_нулевого_дня (дата звернення: 28.10.2018).

2. Vulnerability // Techtarget. Whatis.Com. September 2014. URL: https://whatis.techtarget.com/definition/vulnerability (дата звернення: 28.10.2018).

3. Zero-day (computer) // Techtarget. SearchSecurity. November 2017. URL: https://searchsecurity.techtarget.com/definition/zero-day-vulnerability (дата звернення: 28.10.2018).

4. What is a Zero-Day Exploit? // FireEye. URL: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html (дата звернення: 28.10.2018).

Одержано 30.10.2018