УДК 004

ОГЛЯД ТА СТАТИСТИКА ТЕХНОЛОГІЙ ВИЯВЛЕННЯ ВІРТУАЛІЗАЦІЇ ШКІДЛИВИМ ПЗ

О. О. Григор'єва[1], І. В. Стьопочкіна[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут*

Анотація

У роботі розглянуто варіанти таксономії технік ухилення від віртуалізації та запропоновано їх узагальнення. Надано опис кожної з груп технік та приклади реальних варіантів їх використання. Проведено статистичний аналіз технік на базі ATT&CK від MITRE, виділено найбільші та найперспективніші групи з них, запропоновано напрямки подальших досліджень.

Ключові слова: anti-virtualization, evasive malware, context-aware malware

Вступ

Автори шкідливого програмного забезпечення (ШПЗ) знаходяться у постійному протиборстві з фахівцями з безпеки. Доки перші створюють зловмисний код та вигадують способи його розповсюдження, другі вимушені винаходити його слабкості та досліджувати механізми поведінки. Для зручного та бкзепечного аналізу вже багато років використовуються віртуальні машини (ВМ), які дають можливість при делікатних налаштуваннях виконати будь-який зловмисний функціонал. Проте, з часом виявилося, що перейматися при виборі конфірацій треба не лише про безпеку хостової машини, а про маскування дослідного середовища, адже ШПЗ навчились розріняти у якій системі відбувся їх запуск та при випадках зараження віртуальних самознищуватися чи просто не проводити шкідливі дії. Така поведінка легко пояснюється тим, що якщо ШПЗ потрапляє під докладний аналіз фіхівців, їм набагато простіше розробити захист від нього, ніж коли воно приховує себе.

Актуальність роботи та досліджень у цій галузі завжди висока, бо протистояння між зловмисниками та захисниками вічне: коли з'являється техніка ухилення, дослідники одразу починають її знешкоджувати та шукати подальшу протидію. Попит теж лишається значним попри факт, що зараз все більше компаній запроваджують у своб структуру віртуальні робочі станції, бо за статистикою все рівно «понад 98 відсотків шкідливих програм ... використовують принаймні одну тактику ухилення, і 32 відсотки зразків ШПЗ ... містять шість або більше методів ухилення від виявлення»[1].

Отже, враховуючи таку популярність технік ухилення, необхідно розуміти які з них найпоширеніші та від яких доцільно захищатись.

1. Постановка задачі

Основною метою роботи є дослідження різноманітних технік ухилення, їх поширеності, варіативності та розуміння у якому напрямку потрібно проводити посилення захисту віртуальних машин, що використовуються для аналізу підозрілих зразків. Для цього потрібно вирішити питання:

1) Вирішити на які групи доцільно поділяти техніки ухилення;
2) Надати опис кожної з них;
3) Обрати джерело статистичних даних;
4) Проаналізвувати отримані дані;
5) Зробити висновки.

2. Класифікація технік ухилення

2.1. Існуюча класифікація

Техніки ухилення, що їх використовують ШПЗ для того, аби зробити висновок про те, чи запущені вони у реальному чи у віртуальному середовищі, хоча й відрізняються різноманітністю та можуть бути поділені на скільки завгодно різних груп, мають дещо спільне: всі вони тим чи інакшим чином експлуатують той факт, що будь-яке віртуальне середовище досі не може зімітувати раельну машину у повному обсязі. Завжди лишаються якісь параметри, які чи складно виконати ресурсами віртуального процесора, чи неможливо приховати, адже вони потрібні для коректної роботи ВМ, або які потребують присутності живого, а не програмного користувача (інтерактивні вікна, перевірки на кшталт `CAPTCHA`). Дій ШПЗ при виявлення факторів, що викривають віртуалізацію, можуть бути такими ж різним, як спектр технік, що воно реалізує: від миттєвого видалення себе з системи до демонстрування лише легітимних дій. Можна виділити чотири основні типи технік ухилення, засновані на: «

1) Взаємодії з людиною – натискання миші та діалогові вікна;
2) Специфічній конфігурації – відкладене виконання, тригери на виконання у певний час, приховування процесів, шкідливі завантажувачі, відмова запуску у разі спроби перейменування, зчитування інформації про унікальний номер розділу жорсткого диску, виконання після перезавантаження системи;
3) Специфічному середовищу – перевірка версії ОС або програм, приховування шкідливого коду у не виконуваних файлах (`jpg`, `gif`), у динамічних бібліотеках (`DLL`);
4) Специфічній ВМ — списки системних служб, унікальні файли та порти, які використовуються для комунікації з хостом (`vMX-port`).

[2]

2.2. Пропонована класифікація

Враховуючи велику кількість варіантів технік ухилень та варіативність їх експлуатації, наведений вище розподіл видається занадто загальним, тому пропонується дещо звузити категорії, на які можна поділяти техніки:

1) Перевірка ключів реєстру;
2) Перевірка фізичних характеристик;
3) Перевірка артефактів;
4) Час виконання операцій;
5) Спрацювання тригеру-умови;
6) Перевірка на активність користувача;
7) Анти-аналіз (але не анти-дебаг).

Таким чином, аби розуміти про які саме дії йдеться у кожній з категорій, необхідно розглянути їх всі. Для початку, перша з них, а саме «Перевірка ключів реєстру» включає в себе як зрозуміло з назви будь-які запити до реєстру, з метою зчитування значень певних ключів та за допомогою цього викрити віртуальність цільового середовища, адже робота будь-якого ПЗ, у тому числі такого, що використовується для віртуалізації, не може обійтись без створення та дій над ключами реєстру. Для реалізації цього типу технік можливі звернення до реєстру з пошуком рядків, які вказують на назву певної ВМ, наприклад «`Vmware`» чи «`VirtualBox`». Можлива перевірка на присутність деяких значень за замовчуванням, наприклад `MAC` адрес чи інших полів, специфічних длч конкретного середовища.

Дві наступні категорії стосуються перевірок специфікацій апаратного та відповідно програмного забезпечення: окрім записів у реєстрі, дана інформація може міститися у структурах даних або може бути отримана шляхом виклику певних утиліт. При налаштування дослідного середовища фахівці з безпеки неодмінно будуть встановлювати таку операційну систему (ОС) і програми, які актуальні на даний момент, адже інакше оцінити захищенність сучасних ситем від ШПЗ буде майже неможливо. Проте, коли діло доходить до виділення апаратних ресурсів, їх переважно економлять, звідси і з'являються системи з малою кількістю оперативної або внутрішньої пам'яті, з процесором, що має одне ядро, та без звукових карт, проте з оновленою ОС. Все це для ШПЗ свідчить на користь віртуальності системи. Що ж до поняття «артефактів», то ними виступають окрім програм та відповідно процесів, файли, каталоги, динамічні бібліотеки, інші об'єкти системи, що можуть містити у собі назву ВМ.

Четверта категорія – «Час виконання операцій» належить до перевірок на рівні інструкцій операційної системи та базується на факті, що деякі з них не можуть бути виконані на віртуальному процесорі, а отже передаються процесору хостової машини, звісно така передача викликає затримки у часі виконання операції. Якщо у результаті цей переіод виявляється підозріло довгим, для ШПЗ це може стати фактором зупинки зловмисної діяльності.

«Спрацювання тригеру-умови» приховує у собі дві групи технік ухилення: засновані на очікуванні часу чи дії як умови для початку зловмисної активності. Перші переходять у сплячий режим на визначений проміжок часу або використовують менш помітний спосіб затримати час початку виконання шкідливого коду, який заключається у розміщенні перед ним так званого `stalling code` – він може зовсім не мати сенсу і більше ніде не використовуватися далі, бути ресурсновибагливим чи повторювати одні й ті самі дії безліч разів. Це потрібно аби перевищити той ліміт часу, який мусять визначати дослідники для кожного зразку. Іноді автори зловмисних програм пишуть їх таким чином, аби результати ресурсновибагливих операцій «використовувати на наступних частинах виконання (наприклад, отримання криптографічного ключа в результаті багатьох трудомістких операцій), щоб змусити системи аналізу дійсно виконувати гальмуючий код» [3]. Друга ж група технік направлена на очікування спрацювання дії-тригеру: відкриття чи іншої дії над документом, внесення змін до реєстру, проведення пошукового запиту чи перезавантаження мережного адаптера.

Найрізноманітнішою та такою, що їй часто приділяють недостатньо уваги, є категорія «Перевірка на активність користувача». Вона включає в себе аналіз цільової системи на наповненість, тому перевіряються нещодавно створені файли, наявність активних процесів, пошукових запитів, встановлених офісних програм (без яких важко уявити хоч який реальний комп'ютер), активність миші та клавіатури, типовість екранного розширення тощо.

Потрібно зазначити, що така подія як натиснення клавіші чи кнопки миші також можна розцінювати як виконання тригер-умови, тому треба зрозуміти, що існують ситуації, в яких різниця між техніками «Перевірка на активність користувача» та «Спрацювання тригеру-умови» досить умовна та носить чисто формальний характер. Наприклад, якщо існує зразок ПЗ, яке потрапляє у систему у вигляді офісного документу та доки не проведено подвійного натиска лівої кнопки миші у будь-якому місці файлу, не виявляє зловмисних дій, то як розцінювати таку техніку? Натиск кнопки миші може відноситись до будь-якої з двох згаданих категорій. Необхідно

домовитись, що під «Перевіркою на активність користувача» розуміють перевірку, яка спрямована на активність загалом, просто на підтвердження, що користувач присутній у системі, а категорія «Спрацювання тригеру-умови» потребує чітко визначеної події – якою у тому числі може виступати натиск мишею двічі, але у певному визначеному місці як картинка чи вікно з вибором опцій.

Остання категорія носить назву «Анти-аналіз (але не анти-дебаг)», до неї потрапляють техніки, які не виходить віднести до будь-якої з перших шести категорій, причому під поняттям аналізу маються на увазі інакші від налагоджування способи, такі як аналіз мережевого трафіку, заплутування логіки виконання зловмисного коду, використання файлових розширень, не типових для ВМ, перевірка на моніторинг викликів системних функцій.

3. Збір даних для статистики

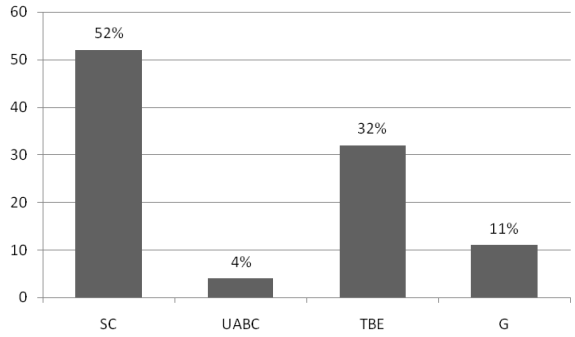
На жаль не існує відкритих та безкоштовних баз ШПЗ з інформацією про техніки ухилення, окрім бази проекту `ATT&CK` від `MITRE`. Цей проект займається вивченням цілей ШПЗ – тактик, та способів їх досягнення – технік. Одним із способів реалізації цілі `Defense Evasion` являються ті самі техніки ухилення, яким присвячена дана робота. Вони у даному проекті зібрані під назвою `Virtualization/Sandbox Evasion` (`T1497`)[4] і саме зразки з цієї техніки та її підвидів буде використано далі для того, аби проаналізувати відсотковий розподіл між раніше виділеними сімома категоріями технік ухилення. Мітре, на противагу, використовує дещо вужчу категорізацію, виділяючи такі підтехніки: Системні Перевірки (`System Checks` – `SC`), Перевірки, засновані на активності Користувача (`User Activity Based Checks` – `UABC`), Перевірки, засновані на Часі (`Time Based Evasion` – `TBE`). Кожна підтехніка має свій перелік ШПЗ, які її реалізують тим чи іншим способом. Всього було проаналізовано 99 зразків ШПЗ та виділено дані про те, яку саме техніку ухилення воно використовує. Статистика використання різних технік ухилення розглядається у наступному розділі.

4. Результат та аналітика

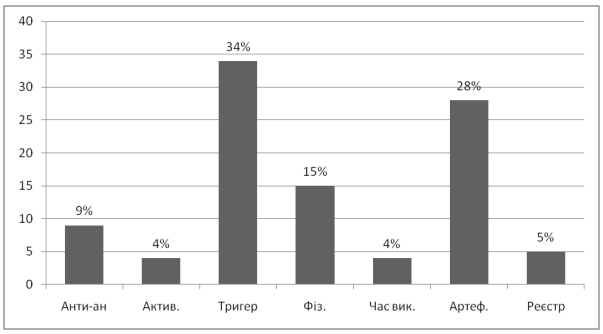
За результатами зібраних даних найбільшою кількістю технік представлена підтехніка Системних Перевірок – її доля склала більше половини, а саме 53% від загальної. На другому місці – Перевірки, які базуються на часі, а найменшою виявилась, як би це було дивно, група Перевірок, заснованих на активності користувача. Такий розподіл може пояснюватись обмеженістю публічно доступних даних або специфічністю таких перевірок. Також присутня четверта група – Загальні техніки ухилення (`G` – `General`), до яких `MITRE` заносить дані про такі зразки, які неможливо чітко віднести до окремої групи. Усі результати можна побачити на Рис. 1а. Що ж до статистики серед 7 виділених у цій праці категорій, то переважну долю від усіх інших перевірок, а саме сумарні 78%, склали Перевірки артефактів, Перевірки фізичних характеристик та Спрацювання тригеру-умови. Розподіл між цими та іншими категоріями наведений на Рис. 1б.

Домінування трьох найбільших категорій з Рис. 1б прямо випливає з Рис. 1а, адже дві з них являються за своєю суттю перевірками системних артефактів, програмних чи апаратних, а доля категорії «Спрацювання тригеру-умови» повністю включається у `TBE`-перевірки. Інші ж напрямки у сумі представляють 22%, що залишились після іменування трьох призерів, і незважаючи на те, що загалом цей відсоток є значним, за свєю природою вони настільки різні, що фахівці, плануючи та виділяючи ресурси на захист дослідних середовищ повинні зважати чи доцільно витрачати такі об'єми людських та технічних зусиль на групи, які займають лише одну п'яту частину у масі інших технік ухилення.

Деякі з категорій представлені різними та цікавими техніками, деякі, як наприклад «Перевірки, засновані на Часі», у більшості випадків (у 23 з 32) реалізують лише одну, а саме затримку початку часу виконання, різниться тільки часовий інтервал, причому він може складати як декілька хвилин, так і діб. Лише у 4 зразках ШПЗ, які потрапили до згаданої категорії, наявна більш делікатна операція з часом – перевірка системного часу на прискорення, що часто свідчить про спробу ВМ завадити зразкам піти у «сплячку». Найобширніша підтехніка від `MITRE` – «Системні Перевірки» – переважно представлені різними варіаціями пошуку небажаних рядків (значень за замовчуванням чи назв платформ віртуалізації) у частинах ВМ. Від того, де такий рядок шукається, залежить по суті категорія, до якої відноситься техніка ухилення. Так, усі пошуки у реєстрі загалом є Перевірками ключів реєстру; пошук назв виробників та номерів апаратного обладнання (процесора, дисків, драйверів) – Перевірка фізичних характеристик; пошук у назвах об'єктів фалової системи або у списку процесів чи доменів – Перевірка артефактів. Остання категорія взагалі дуже обширна, бо у системі будь-що може вистувати артефактом для аналізу, у тому числі версія чи назва ОС, магічне значення `VMXh` та налаштування мережі. Щодо більш специфічних та рідких перевірок, то такі були направлені на зчитування температури термальних зон процесора та на моніторинг використання технологій перехоплень системних викликів, для реалізації останньої техніки, яка до речі належить до Анти-аналізу, ШПЗ може виконувати ті самі дії, що приховуються за зручним системних викликом, аби уникнути перехвату, або ж навпаки, викликати такі функції, але з помилковими параметрами, що теж зашкоджує коректному аналізу. Ще однією специфічною технікою є перевірка назви файлу, у який було збережено шкідливий код, адже часто платформи віртуалізації іменують зразки їх хешем. Зрозумілим є використання перевірок на активність миші (положення курсору, кількість натисків) чи клавіатури для категорії «Перевіркок, заснованих на активності Користувача».



(а) Статистика за підтехніками



(б) Статистика за категоріями

Рис. 1. Статистика технік ухилення

База даних ATT&CK від MITRE щодо технік ухилення хоча й містить доволі обмежену кількість зразків ШПЗ, що їх використовують, проте усі вони були розглянуті та категорізовані у рамках даної роботи, що свідчить на користь повноти проведеного огляду.

Висновки

У роботі було наведено класифікацію технік ухилення, які ШПЗ може використати, аби уникнути запуску у віртуальному середовищі. Як було продемонстровано, у цільовій системі немає сутності, яка б не могла стати об'єктом для аналізу зловмисного коду. Наявність реального користувача теж являється важливим вектором перевірок, тому зважаючи на неможливість повного захисту цільової системи через надзвичайні витрати у ресурсах, матеріальних чи програмних та навантаження на фахівців з безпеки, потрібно приймати рішення щодо пріотеризації зусиль на окремих напрямках. За результатами статистичного аналізу такими напрямками можуть бути: перевірки артефактів, апаратних та програмних, а також перевірки, засновані на спрацюванні часового тригеру.

Отже, враховуючи аналіз статистичних даних, доцільним є подальше поглиблене вивчення технік, які належать до вище згаданих категорій та розробка технічних засобів їх моніторингу чи приховування об'єктів їх перевірок. Важливим є також розширення бази даних технік ухилення проекту ATT&CK від MITRE, адже публічність таких даних допомагає усім фахівцям розуміти тренди та

Перелік використаних джерел

1. Stefnisson Siggi. Evasive Malware Now a Commodity [Electronic resource]. — Security Week. — 2018. — Access mode: https://www.securityweek.com/evasive-malware-now-commodity (online; accessed: 2022-05-30).
2. Singh Abhishek, Bu Zheng. Hot Knives Through Butter: Evading File-based Sandboxes [Electronic resource] // Mandiant. — 2013. — Access mode: https://www.mandiant.com/resources/hot-knives-through-butter-evading-file-based-sandboxes.
3. Bulazel Alexei, Yener Bülent. A Survey On Automated Dynamic Malware Analysis Evasion and Counter-Evasion: PC, Mobile, and Web [Electronic resource] // ResearchGate. — 2017. — Access mode: https://www.researchgate.net/publication/322588326_A_Survey_On_Automated_Dynamic_Malware_Analysis_Evasion_and_Counter-Evasion_PC_Mobile_and_Web.
4. ATT&CK MITRE. Virtualization/Sandbox Evasion [Electronic resource]. — 2021. — Access mode: https://attack.mitre.org/techniques/T1497/ (online; accessed: 2022-05-30).