УДК 303.7
Сущевських О. В.[1], Зайко Т. А.[2]
[1]студ. гр. КНТ-117 НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька Політехніка»

СУЧАСНІ ТЕХНОЛОГІЇ ДАМПІНГА І ЗАХИСТУ ВІД НЬОГО

Як відомо, одним із найпоширеніших механізмів захисту ПЗ є використання навісного захисту. Основна ідея такого захисту – ускладнити аналіз роботи програми за допомогою шифрування коду програми і розшифровування його безпосередньо перед виконанням. Такий захист забезпечує відносно стійкий та дешевий захист. При його використанні оригінальний код програми шифрується, модифікується PE-заголовок, до програми додається розшифровувач. Перед виконанням програма розшифровується, частково відновлюється оригінальний PE-заголовок, і керування передається програмі. Але такий захист, як і будь-який інший, не є гарантією того, що програма буде повністю і назавжди захищеною. І одним з

методів зняття захистів такого виду є використання дамперів, тобто програм, які можуть зберегти дамп пам’яті під час роботи програми в момент закінчення спрацьовування захисту.

Зняття такого захисту проходить в три етапи:

– знаходження моменту передачі керування оригінальній програмі;

– знімання дампу пам’яті програми;

– відновлення PE-заголовку.

З цього можна зробити такий висновок: посилити захист можна, максимально ускладнивши для хакера виконання цих операцій. Оскільки предметом даного розділу є дослідження можливості зняття образу програми з пам’яті.

Дамп пам'яті – це копія вмісту оперативної пам'яті, що знаходиться на жорсткому диску або іншому енергонезалежному пристрої пам'яті [1].

Всі дампери процесів побудовані на функціях OpenProcess / ReadProcessMemory / VirtualQueryEx e.t.c. Для отримання списку модулів завантажених в процес зазвичай використовуються функції ToolHelp API, які в свою чергу читають пам'ять процесу через ReadProcessMemory. На рівні NativeAPI при цьому відбувається виклик функцій ZwOpenProcess і ZwReadVirtualMemory. Очевидний спосіб протидії дампу - це встановити драйвер, який перехопить в ядрі ці функції і заборонить доступ до захищаємого процесу.

Все добре в теорії, але при практичній реалізації цього методу зустрічаються підводні камені. Наприклад, в Windows XP існує служба стилів. Для правильної її роботи потрібно дозволяти доступ процесу сервера підсистеми (csrss.exe) до пам'яті захищаємого процесу.

Захист в нульовому кільці відкриває дійсно багаті можливості (обмежені тільки уявою). Наприклад вельми непоганий спосіб антидампа - руйнування таблиці сторінок захищаємого процесу. Для цього треба втрутитися в роботу планувальника і перехопити функцію яку не можна експортувати(SwapContext), яка викликається при зміні робочого потоку, в обробнику перехоплення, при перемиканні на захищаємий процес потрібно відновлювати таблицю сторінок, а при відключенні від нього - руйнувати. Це найпростіше, що можна протиставити драйверному дампу.[2]

Інший розповсюджений метод захисту від зняття дампу – динамічне розпаковування. Суть його в тому, що протектор розпаковує захищувану програму не повністю, а частинами. Спочатку розпаковується перша сторінка, а коли відбувається звернення за її межі, протектор перехоплює виключення і розпаковує запитану сторінку, при цьому він може прибрати з пам'яті попередню сторінку. Таким чином, образ захищеного процесу в пам'яті ніколи не існує повністю, отже звичайним дампером його не зняти не можна. Для зняття цього захисту більшість хакерів обирають не зовсім

оптимальний шлях – реверсинг і зміну коду протектора з метою змусити його розшифрувати код повністю. Це дуже трудомістка операція, тим більш, що в кожній новій версії автори міняють реалізацію цього захисного механізму, і тоді старі програми для зламу стають неактуальними.

Підводячи підсумок, можна сказати, що метод динамічного розпаковування, є кращим захистом з перерахованих методів та активно запровадженим рішенням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1 Каплун, В. А. Захист програмного забезпечення. Частина 2 : навчальний посібник / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев. – Вінниця : ВНТУ, 2014. – 105 с.

2. Современные технологии дампинга и защиты от него. https://wasm.in/blogs/sovremennye-texnologii-dampinga-i-zaschity-ot-nego.396/(Електронний ресурс)