– використовувати багатофакторну аутентифікацію співробітників, електронний підпис для захисту повідомлень електронної пошти;

– відслідковувати факти наявності програм для створення діпфейків на комп'ютерах користувачів і спроби пошуку таких додатків в мережі «Інтернет», звертати особливу увагу на подібних працівників і проводити в їх відношенні внутрішні перевірки;

– забезпечити узгоджене поширення інформації;

– обмежити фото- і відео контент за участю керівних осіб підприємства;

– розробити план реагування на дезінформацію (по аналогії з інцидентами безпеки);

– мінімізувати число каналів комунікацій компанії;

– всередині компанії і для зв'язку з контрагентами застосовувати практику введення усних паролів, кодових слів або контрольних питань, відповідь на які відомий лише двом сторонам;

– стежити за новими способами виявлення діпфейків і методами боротьби з ними.

В даний час ринок ІБ не пропонує спеціалізованих рішень для захисту від діпфейків. Розвиток інструментів, здатних розпізнати підроблений контент, поки знаходиться в зародковому стані. Єдине рішення, яке існує в даний час, полягає в тому, щоб інформувати користувачів про нові типи атак і бути насторожі щодо будь-якої поведінки, яка здається незвичайною.

Список використаних джерел

1. In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://arxiv.org/pdf/1806.02877.pdf.

2. New Deepfake Spotting Tool Proves 94% Effective – Here's the Secret of Its Success [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://scitechdaily.com/new-deepfake-spotting-tool-proves-94-effective-heres-the-secret-of-its-success/.

3. Creating a dataset and a challenge for deepfakes [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://ai.facebook.com/blog/deepfake-detection-challenge.

4. Deepfake [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Deepfake.

5. DeepFaceLab [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/iperov/DeepFaceLab.

6. Unsupervised image-to-image translation [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/mingyuliutw/unit.

УДК 004.318

МЕТОД ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ

Шамара Н. В., здобувач вищої освіти гр.КБ-191
Науковий керівник: **Петренко Т. А** , викладач
Національний університет «Чернігівська політехніка»

Комп'ютер давно вже став частиною життя майже всіх людей. Він використовується для роботи, навчання, розваг, спілкування, в тому числі і кіберзахисту Для багатьох комп'ютер або ноутбук є єдиним джерелом доходу. Тож його продуктивність є однією з найголовніших складових вдалої роботи. Це сприяє швидкості та якості виконання технічних задач в сфері КіберБезпеки.

Не дивно, що на сьогодні все більше зростає потреба у наявності продуктивного комп'ютера. На жаль, люди зіштовхуються з проблемою невідповідності ціни та характеристик товару. Опис може відрізнятися від реальності, або взагалі вводити в оману

некомпетентних користувачів. Як результат, більшість покупців отримують комп'ютер, складові та функціональність якого не відповідають ціні.

Актуальністю збільшення продуктивності процесора є можливість покращити роботу комп'ютера з найменшими витратами. Споживачі матимуть можливість власноруч підвищити продуктивність процесора, зекономити кошти та стати більш обізнаними в структурі та функціональності свого робочого пристрою.

На прикладі процесорів сімейства Haswell [1], а саме – Xeon, ми пропонуємо метод збільшення продуктивності обчислювальної системи. Xeon особливий завдяки можливості розблокування тактової частоти, а саме – максимального навантаження на всі ядра процесора.

Блокування дозволяє зафіксувати максимальну частоту турбо-буста, але не на 1-2 ядра, як це було задумано Intel, а на всі ядра. Залежно від моделі процесора, приріст може бути цілком значним.

Весь процес модифікації полягає у видаленні з біоса мікрокодів для процесорів Haswell, а саме 306F2. Приступаючи до анлоку також слід мати на увазі, що температура процесора може підскочити на 5-10 градусів.

На практиці є два способи анлока в залежності від типу використовуваного драйвера EFI [2] - зчитується з диска при старті системи і FFS, який вшивається в BIOS. Перевага FFS драйвера, що анлок не злітає при скиданні налаштувань біоса, переустановлення системи і т.п. і працює не залежно від структури розділів завантажувального диска, а при використанні FFS (PEI) анлок не злітає після сну. При використанні EFI драйвера анлок може злетіти, з різних причин, що б не вдаючись в подробиці - причини зльоту ті ж по яким може порушиться завантаження системи (наприклад помилки файлової системи), а так само він вимагає структуру розділів завантажувального диска GPT. За твердженням експертів EFI драйвер , показує кращі результати по продуктивності, ніж FFS драйвер з аналогічними параметрами. Перевага EFI драйвера можливість швидкої його заміни без перепрошивки біоса. Саме цей метод анлока найбільш зручний.. Для цього ми будемо використовувати заздалегідь підготовлену утиліту MMtool [3]

Її алгоритм налагодження :

1. Запускаємо програму.
2. Натискаємо «Load Image» і відкриваємо дамп.
3. Переходимо на вкладку «Cpu Patch» щоб отримати список мікрокодів
4. Переходимо на стовпець «Cpu ID», нам потрібен 06F, виділяємо його.
5. Ставимо галочку навпроти «Delete a patch data», потім тиснемо "Apply» і підтверджуємо видалення.
6. Зберігаємо біос кнопкою «Save imege as ...».

Отримано готовий файл для прошивки біоса, переходимо до наступного пункту.

Всього існує чотири способи перепрошивки Bios :

1. За допомогою програми AfuWin
2. За допомогою програми Intel Flash Programming Tool (FPT)
3. За допомогою флешки-завантажувача
4. Програматором для материнських плат.

Розглянемо прошивку за допомогою програми AfuWin [4]. Основна перевага цього методу - швидкість, та легкий інтерфейс.

1. Відкриваємо AfuWin
2. Натискаємо «Save» і зберігаємо файл. Тим самим зробимо дамп нашого біоса.
3. Якщо програма не сумісна з чипсетом системної плати з'являється повідомлення з помилкою. Таким чином перед прошивкою біоса є можливість перевірити сумісність програми з чіпом біоса, якщо процес бекапа пройшов вдало, значить чіп системної плати сумісний з програмою.
4. Натискаємо кнопку «Open», вибираємо файл біоса для прошивки, та прошиваємо його.

Для перевірки можна використовувати програму HwInfo, яка показує частоти для кожного ядра. Паралельно можна запустити будь-якої бенчмарк або стрес-тест (наприклад cpu-z), щоб навантажити процесор. Якщо все пройшло вдало - частота кожного ядра буде дорівнює максимальному значенню турбо-буста процесора.

Порівнюємо анлок турбо-буста та стокового біоса, за допомогою програми Corona BenchMark бачимо що в рендері процесор з модифікованим біосом показує себе набагато краще , тим самим випереджаючи на 40 секунд стоковий біос.

В деяких іграх описаний метод показує високий приріст продуктивності , а в деяких ні. Це обумовлено оптимізацію ігор під наш процесор, а саме тактовою частотою процесора, деякі оптимізовані під високу частоту процесора , а інші такої оптимізації не мають, але все таки процесор з розблокованим TurboBoost, показує кращий результат.

Розглянутий метод дозволяє підвищити продуктивність обчислювальної системи на 20-50%,за допомогою видалення мікрокоду , що в свою чергу дозволить підвищує ефективність використання зазначених систем для вирішення задач кіберзахисту.

Список використаних джерел

1. https://uk.wikipedia.org/wiki/Haswell
2. https://ru.wikipedia.org/wiki/Extensible_Firmware_Interface
3. https://forums.overclockers.ru/viewtopic.php?f=1&t=479847&start=7560
4. http://xeonlive.ru/instruktsii/afuwin-proshivka-bios-iz-pod-windows

---

УДК 004.056.55

KUBERNETES - ОРКЕСТРАЦІЇ КОНТЕЙНЕРІВ, ЩО ЗАБЕЗПЕЧУЄ ВІДМОВОСТІЙКІСТЬ ТА ДОСТУПНІСТЬ ДОДАТКУ

Ткач Ю. М., д.п.н., проф.,
завідувач кафедри кібербезпеки та математичного моделювання,
Клименок В. О., здобувач вищої освіти гр. МКБп-201
Національний університет "Чернігівська політехніка"

Kubernetes - це потужна система з відкритим кодом, спочатку розроблена Google, для управління контейнерними програмами в кластерному середовищі. Вона спрямована на забезпечення кращих способів управління пов'язаними, розподіленими компонентами та послугами у різноманітній інфраструктурі.

Kubernetes, на своєму базовому рівні, є системою для запуску та координації контейнерних програм через кластер машин. Це платформа, призначена для повного управління життєвим циклом контейнерних програм та служб, використовуючи методи, що забезпечують передбачуваність, масштабованість та високу доступність.

Користувач Kubernetes може визначити, як повинні працювати програми та способи їх взаємодії з іншими програмами чи зовнішнім світом. Є можливість масштабувати сервіси вгору або вниз, виконувати оновлення, а також переключати трафік між різними версіями програм, щоб перевірити функції або відмовити розгортання. Kubernetes надає інтерфейси та складні примітивні елементи платформи, які дозволяють визначати та керувати своїми програмами з високим ступенем гнучкості, потужності та надійності.

Контейнери - це хороший спосіб об'єднати та запустити ваші програми. У production середовищі потрібно керувати контейнерами, в яких запущені програми, і переконатися, що немає простоїв. Наприклад, якщо контейнер виключається, потрібно запускати інший контейнер.