УДК [342.9:343.98] (477)
DOI https://doi.org/10.32782/forensic.science.2025.1.13

Олександр Закс
головний судовий експерт,
Науково-дослідний центр незалежних судових експертиз
Міністерства юстиції України
https://orcid.org/0009-0005-3820-1435

CAPE SANDBOX – ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ З ВІДКРИТИМ ВИХІДНИМ КОДОМ ДЛЯ АВТОМАТИЗОВАНОГО АНАЛІЗУ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПІД ОПЕРАЦІЙНИМИ СИСТЕМИ НА БАЗІ ЯДРА LINUX

У статті стисло викладено огляд функціоналу програмного забезпечення Cape Sandbox, яке дозволяє досліджувати в автоматизованому режимі поведінку шкідливого програмного забезпечення у ізольованому середовищі під операційними системами Microsoft Windows XP/7/10/11 та Ubuntu 32/64-bit з використанням як хоста операційної систем на базі ядра Linux.

***Ключові слова**: аналіз шкідливого програмного забезпечення з використанням відкритого програмного забезпечення, інструмент для аналізу шкідливого програмного забезпечення на Linux, пісочниця Cape Sandbox, аналог Cuckoo для дослідження шкідливого програмного забезпечення.*

Дослідження шкідливого програмного забезпечення у сучасних реаліях є критично важливим під час проведення комп'ютерно-технічних експертиз і потребує спеціалізованого комерційного програмного забезпечення. Однак таке програмне забезпечення має значну вартість і не завжди доступне для використання в певних країнах і в такому разі в пригоді стає програмне забезпечення з відкритим вихідним кодом, яке за своїм функціоналом не поступається комерційному.

Аналіз шкідливого програмного забезпечення за допомогою програмного забезпечення з відкритим вихідним кодом на операційних системах на базі ядра Linux забезпечує економічно ефективний і потужний підхід до розуміння функціонування шкідливого програмного забезпечення та, як наслідок, його повного та всебічного дослідження.

Основна мета цієї роботи – продемонструвати функціонал програмного забезпеченням з відкритим вихідним кодом Cape Sandbox, яке дозволяє здійснювати комплексний автоматизований аналіз шкідливого програмного забезпечення під операційними системами на базі ядра Linux.

Cape Sandbox – програмне забезпечення з відкритим вихідним кодом для автоматизованого аналізу шкідливого програмного забезпечення на гостьових системах з операційними системами Windows XP/7/10/11 [2] та Ubuntu 32/64.

На сьогодні програмне забезпечення CAPE може аналізувати такі види об'єктів: виконуючі файли Windows, DLL файли, PDF документи, документи Microsoft Office; URL адреси та HTML файли; PACP дампи, PHP скрипти, CPL файли, Visual Basic скрипти, ZIP архіви, JAR файли, Python скрипти тощо.

Cape Sandbox складається з центрального програмного забезпечення, з якого можна здійснювати керування та аналіз, його ще називають хостом «Рисунок 1». Відправка об'єкта на аналіз здійснюється з використанням командного рядка або через веб-інтерфейс. Після імпорту відбувається запуск ізольованої віртуальної машини, в якій інстальований агент, який здійснює завантаження,

запуск та збір інформації про активність шкідливого програмного забезпечення.

Варто зазначити, що для кожного нового аналізу використовується нова ізольована віртуальна машина, це досягається завдяки використанню засобів віртуалізації з використанням снапшотів. Cape підтримує роботу з гіпервізорами та сервісами KVM, VirtualBox, VMWare, XenServer та Azure [3].

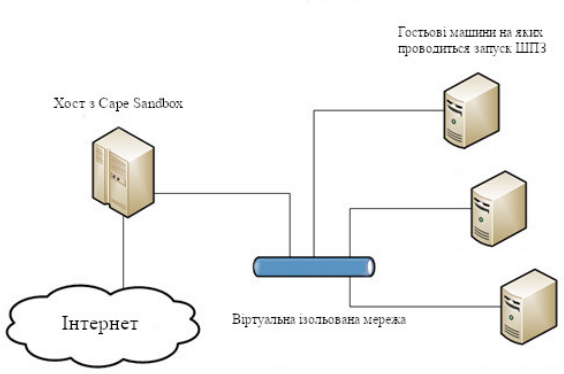

Рис. 1. Архітектура програмного забезпечення Cape

Cape було створено на базі Cuckoo v1 і тому він перейняв певну частину функціональних можливостей, таких як: поведінковий інструментарій на базі перехоплення API; захоплення файлів – створених, змінених та видалених під час виконання аналізу; захоплення мережевого трафіку у форматі PCAP; класифікація шкідливого програмного забезпечення на основі поведінки і мережевих сигнатур; скріншоти робочого столу, які створюються під час виконання шкідливого програмного забезпечення на гостьовій системі, тобто в ізольованому середовищі та повні дампи пам'яті гостьової системи.

Програмне забезпечення Cape розширює функціонал програмного продукту Cuckoo наявністю автоматизованого динамічного розпакування шкідливого програмного забезпечення «Рисунок 2».

Під час аналізу Cape використовує низку технік, які можна охарактеризувати як «шкідливі». Такими техніками є ін'єкції шелл-коду, DLL ін'єкції, ін'єкції пустого процесу, процесу «DopopelGanging» та вилучення із виконуючого модуля чи шелл-коду в пам'яті.

Вказані техніки спрямовані на збільшення успішних перехоплень незапакованого корисного навантаження та подальшого його дослідження.

Крім того, Cape в процесі своєї роботи автоматично створює дампи процесу для кожного процесу або образу бібліотеки DLL у разі необхідності. Такий спосіб дозволяє отримати розпаковану інформацію з дампу образу модуля, однак цей спосіб спрацьовує лише для простих пакувальників.

За замовчуванням механізм «активного» розпакування вимкнений і для його активації необхідно у веб-інтерфейсі встановити відповідний чек-бокс або передати відповідний параметр. З режимом «активного» розпакування слід бути досить обережним, позаяк можуть виникнути хибні спрацювання.

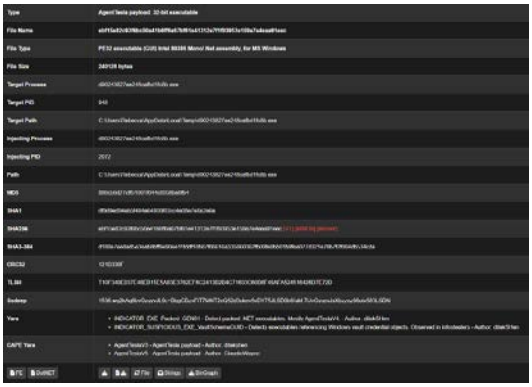

Рис. 2. Результат роботи розпакування шкідливого програмного забезпечення

У програмне забезпечення Cape інтегровано механізми, які дозволяють проводити класифікацію шкідливого програмного забезпечення з використанням сигнатур YARA, скануванням мережевого трафіку на наявність ознак шкідливого трафіку та поведінкові сигнатури вихідних даних «Рисунок 3».

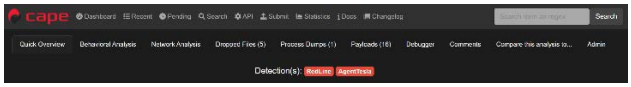

Рис. 3. Результат класифікації шкідливого програмного забезпечення

У програмному забезпеченні Cape наявний функціонал для статичного та динамічного вилучення конфігурацій зі шкідливого програмного забезпечення з використанням вбудованого фреймворку Cape «Рисунок 4» або з використанням сторонніх фреймворків, таких як: RATDecoders, DC3-MWCP, MalDuck або MaCo. Ця особливість робить Cape досить гнучким і дозволяє краще адаптуватися під нові види та техніки шкідливого програмного забезпечення.

Рис. 4. Результат вилучення конфігурації шкідливого програмного забезпечення

Автоматизований налагоджувач Cape підтримує сигнатури YARA та дозволяє створювати користувацькі розпакування/конфігурації екстракторів та динамічні засоби для контрзаходів проти пісочниці та трасування інструкцій. Захоплення за замовчуванням виконується після того, коли неупаковані корисні дані почали виконуватися і це своєю чергою дозволяє визначити пакувальника за допомогою користувацької сигнатури YARA «Рисунок 5». Після чого здійснюється встановлення точки зупинки (брекпоінт) на останній інструкції пакувальника, що дає змогу захопити корисні дані у їх вихідній точці входу (OEP) до їх виконання [1].

```
rule UPX
{
    meta:
        author = "kevoreilly"
        description = "UPX dump on OEP (original entry point)"
        cape_options = "bp0=$upx32+9,bp0=$upx64+11,action0=step2oep"
    strings:
        $upx32 = {6A 00 39 C4 75 FA 83 EC ?? E9}
        $upx64 = {6A 00 48 39 C4 75 F9 48 83 EC ?? E9}
    condition:
        uint16(0) == 0x5A4D and any of them
}
```

Рис. 5. Зразок правила YARA

Cape має потужний налагоджувач, який має функціонал для динамічного обходу запобігань від ухилення. Досить часто шкідливе програмне забезпечення намагається уникнути аналізу різноманітними методами, наприклад, використовуючи інформацію про обладнання комп'ютерної техніки, наявність інформації від датчиків температури, крім того, більшість шкідливого програмного забезпечення використовує техніки для визначення віртуалізації або виявлення перехоплень API, програмне забезпечення Cape дозволяє розробляти динамічні контрзаходи, поєднуючи дії налагоджувача сигнатур YARA для виявлення шкідливого програмного забезпечення «Рисунок 6», яке намагається ухилитися під час аналізу та виконує маніпуляції з потоком керування, щоб змусити шкідливе програмне забезпечення відпрацювати повністю.

Рис. 6. Зразок правила YARA

У своїй роботі Cape використовує користувацькі компоненти, які стежать за поведінкою шкідливих процесів під час роботи в ізольованому середовищі, одночасно контролюючи їх динамічну поведінку та забираючи криміналістичні артефакти.

Потужна інтеграція з VirusTotal, MWDB, MalwareBazaar, Mitre att&ck та можливість використання різноманітних утиліт для розширення функціоналу з наявністю кастомізації збільшують можливості аналізу та його ефективності.

У світі, який швидко оцифровується, сувора реальність кіберзагроз продовжує кидати тінь на нові технологічні досягнення. Потреба в надійних, універсальних і комплексних інструментах аналізу шкідливого програмного забезпечення ще ніколи не була такою важливою. Програмне забезпечення Cape Sandbox з відкритим вихідним кодом дає потужні можливості для ідентифікації, класифікації та розуміння роботи шкідливого програмного забезпечення.

Вказане в цій статті програмне забезпечення для аналізу має унікальні переваги та можливості від ізольованого програмного середовища до утиліт зіставлення шаблонів, зворотного проєктування, аналізу мережевого трафіку тощо та, крім того, не поступається комерційним аналогам та є економічно виправданим.

Список використаної літератури:

1. Cape Sandbox Book Copyright 2010–2015, Cuckoo Foundation, 2016–2024, kevoreilly. Revision 4c1af810. URL: https://capev2.readthedocs.io/en/latest (дата звернення: 13.12.2022).
2. Rebaker501, Instruction for getting CAPEv2 Malware Sandbox up and running URL: https://github.com/rebaker501/capev2install (дата звернення: 12.12.2022).
3. Yan Sandman, Deploying CAPEv2 on AWS – A Comprehensive Guide URL: https://y4nush.com/posts/installation-of-capev2-sandbox-on-aws/ (дата звернення: 12.12.2022).

Oleksandr Zaks. Cape Sandbox open-source software for automated malware analysis on Linux-based operating systems

The article briefly presents an overview of the functionality of the Cape Sandbox software, which allows you to study the behavior of malicious software in an isolated environment under Microsoft Windows XP/7/10/11 and Ubuntu 32/64-bit operating systems using a Linux kernel-based operating system as a host in an automated mode.

Keywords: *malware analysis using open source software, malware analysis tool for Linux, Cape Sandbox, Cuckoo counterpart for malware research.*