УДК 004.5

ЦИФРОВІ ЗАЛИШКИ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ

Роман Стецик, Віталій Носов

DIGITAL LOSS OF CLOUD SERVICES USAGE

Roman Stetsyk, Vitalii Nosov

Харківський національний університет внутрішніх справ, вул. Лесі Українки 30, м. Кам'янець-Подільський, Хмельницька обл., 32301, Україна

***Abstract**. Digital traces of cloud services usage on Windows 10 were investigated for digital forensics purposes.*

Під час розслідувань злочинів проти національної безпеки України цифрові докази часто зберігаються на комп'ютерах, а використання хмарних технологій ускладнює їх виявлення, що зумовлює потребу фіксації факту їх використання під час огляду.

Під хмарними технологіями (coud computing) розуміється надання за запитом мережевого доступу до спільно використовуваних, налаштовуваних обчислювальних ресурсів [1]. Наразі лідерами надання послуг хмарних технологій є Amazon Web Services (AWS), Microsoft Azure і Google Cloud Platform (GCP) [2]. Ці провайдери пропонують безліч послуг, які діляться на категорії, основні з яких є: обчислення (compute), зберігання (ctorage), бази даних (databases), мережі (networking), аналіз даних (data analytics), штучний інтелект/машинне навчання (AI/ML), безпека (security), моніторинг та управління (monitoring&management). Керування послугами може здійснюватись через вебінтерфейс (браузер) або/та інтерфейс командного рядка (Command-Line Interface, CLI).

Для ОС Windows 10, яка поки що залишається найбільш масовою серед сімейства Windows [3], було проведено експериментальне дослідження із встановлення слідів, які утворюються в ОС при використанні хмарних технологій AWS, Microsoft Azure, GCP. У дослідженні використовувалась програма моніторингу Process Monitor [4], найбільш популярні браузери [5]: Google Chrome, Microsoft Edge, Mozilla Firefox (табл. 1), та інтерпретатор команд cmd.exe (табл. 2).

Таблиця 1 – Сліди використанні хмарних сервісів через вебінтерфейс

Браузер	**Файли/каталоги, що утворюються при використанні хмарних сервісів через вебінтерфейс**
Mozilla Firefox	C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\k8jbfeys.default-release\cache2\entries
	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\goocle cloud web (2).lnk
	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms\goocle cloud web.lnk
	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\Event viewer.lnk
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\places.sqlite-shm
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\SiteSecurityServiceState.bin

Браузер	Файли/каталоги, що утворюються при використанні хмарних сервісів через вебінтерфейс
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\favicons.sqlite
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\permissions.sqlite
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\storage/default
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\content-prefs.sqlite
	C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\k8jbfeys.default-release\thumbnail
	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\sessionstore-backups\recovery.baklz4
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\sessionstore-backups\upgrade.jsonlz4-20241021175835
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\sessionstore-backups\recovery.jsonlz4
	C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\k8jbfeys.default-release\settings\main\ms-language-packs\browser\newtab\asrouter.ftl
	C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms
	C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\k8jbfeys.default-release\cookies.sqlite
Google Chrome	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Preferences
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\History
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Sessions
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Affiliation Database
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Login Data
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb

Браузер	Файли/каталоги, що утворюються при використанні хмарних сервісів через вебінтерфейс
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Session Storage
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\
	C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\JumpListIconsRecentClosed
	C:\Users\User\AppData\Local\Google\Chrome\User Data\segmentation_platform\ukm_db
Microsoft Edge	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\load_statistics.db
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Historyl
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Favicons
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13376094555857426 (Tabs_13376094556813223)
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Web Data
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\WebAssistDatabase
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\WebStorage\QuotaManager
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\Login Data
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\WebStorage\QuotaManager
	C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_us-east-2.console.aws.amazon.com_0.indexeddb.leveldb

Таблиця 2 – Сліди використання хмарних сервісів через CLI

Тип слідів	Хмарний провайдер		
	Google Cloud CLI	AWS CLI	Azure CLI
Каталоги /файли	C:\Users\User\AppData\Roaming\gcloud	C:\Program Files\Amazon\AWSCLIV2	C:\Program Files\Microsoft SDKs\Azure\CLI2
	C:\Users\User\AppData\Local\Google\Cloud SDK	C:\Users\User\.aws	C:\Users\User\.azure
Запис у реєстрі	HKEY_CURRENT_USER\Environment	HKEY_CLASSES_ROOT\Installer	HKEY_CLASSES_ROOT\Installer\Products

Тип слідів	Хмарний провайдер		
	Google Cloud CLI	**AWS CLI**	**Azure CLI**
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\UFH	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products\E4D23E32DF18B364C8F49F5DF87A7E84
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Azure CLI
	HKEY_USERS\S-1-5-21-2665380886-1368437490-2271808297-1001\Environment	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer
		HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Environment	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Environment
			HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\bam\State\UserSettings
			HKEY_USERS\S-1-5-21-2665380886-1368437490-2271808297-1001\SOFTWARE\Microsoft\Microsoft Azure CLI

Отримані результати свідчать, що сліди використання хмарних сервісів через вебінтерфейс утворюються в каталогах історії відвідувань сайтів, сесій, cookie та тимчасових даних (кеш). При використанні командних інтерфейсів утворюються каталоги, файли та записи в реєстрі Windows, що містять дані про налаштування та виконані команди.

Бібліографія

1. Cloud Computing | CSRC. URL: https://csrc.nist.gov/projects/cloud-computing (дата звернення: 18.11.2024).
2. Chart: Amazon Maintains Cloud Lead as Microsoft Edges Closer | Statista. URL: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/ (дата звернення: 18.11.2024).
3. Desktop Windows Version Market Share Worldwide | Statcounter Global. URL: https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide (дата звернення: 18.11.2024).
4. Process Monitor – Sysinternals. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon (дата звернення: 18.11.2024).
5. Browser Market Share Worldwide | Statcounter Global Stats. URL: https://gs.statcounter.com/browser-market-share/ (дата звернення: 18.11.2024).