

ОСОБЛИВОСТІ ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ АРТ-ЗАГРОЗ В ІНФРАСТРУКТУРІ KUBERNETES

Вінницький національний технічний університет

Анотація

У роботі досліджено еволюцію та специфіку атак класу Розвиненої тривалої загрози (APT) у середовищі оркестрації контейнерів Kubernetes. Проаналізовано ключові відмінності методів закріплення зловмисників у хмарній інфраструктурі порівняно з класичними мережами, зокрема використання контролерів (DaemonSets, CronJobs) та маніпуляції з RBAC. Визначено проблему «форензичного розриву», що виникає через ефемерність контейнерів та ускладнює розслідування інцидентів. На основі аналізу матриць загроз Microsoft та MITRE ATT&CK запропоновано комплексну стратегію захисту, що базується на принципах Zero Trust, мікросегментації мережі та безперервному runtime-моніторингу.

Ключові слова: Розвинена тривала загроза, APT-атака, Kubernetes, безпека контейнерів, форензичний розрив, RBAC, Zero Trust, матриця загроз, ефемерність, бічне переміщення.

Abstract

The paper explores the evolution and specificity of the Advanced Persistent Threat (APT) class in the Kubernetes orchestration container environment. It analyzes key differences in methods for attackers to establish themselves in cloud infrastructure through classical networks, including the use of controllers (DaemonSets, CronJobs) and RBAC manipulation. The problem of "forensic gap" is identified, which arises due to the ephemerality of containers and complicates incident investigation. Based on the analysis of Microsoft and MITRE ATT&CK threat matrices, a comprehensive protection strategy is proposed, based on the principles of Zero Trust, network micro-segmentation, and continuous runtime monitoring.

Keywords: Advanced persistent threat, APT attack, Kubernetes, container security, forensic breach, RBAC, Zero Trust, threat matrix, ephemerality, lateral movement.

Вступ

Фактичним стандартом для оркестрації контейнерних додатків, у зв'язку зі стрімким переходом критичної інфраструктури на хмарні платформи та контейнери, став Kubernetes. Це призвело до появи нового класу загроз – АРТ-атак, адаптованих під хмарні середовища. Ці АРТ-групи використовують специфічні архітектурні особливості Kubernetes, такі як ефемерність контейнерів та мікросервісна взаємодія, для тривалого прихованого шпигунства та саботажу.

Актуальність теми зумовлена тим, що класичні засоби захисту периметра виявляються неефективними проти зловмисників, які оперують на рівні оркестрації та внутрішніх комунікацій кластера.

Метою даної роботи є аналіз сутності АРТ-загроз у контексті контейнеризації, дослідження специфічних векторів атак та визначення ефективних методів захисту на основі підходу Zero Trust.

Результати дослідження

1. Advanced Persistent Threat як клас кіберзагроз: сутність та характеристики

Розвинена тривала загроза (Advanced Persistent Threat, APT) – це складна цілеспрямована кібератака, метою якої є отримання доступу до мережі та непомітність протягом тривалого часу, внаслідок ретельного планування дій.

Термін базується на трьох ключових характеристиках, що визначають природу цього класу загроз:

- advanced (розвинена). Така атака реалізується із використанням складних технік: від методів соціальної інженерії до використання вразливостей нульового дня (zero-day) та спеціалізованого шкідливого ПЗ;

- persistent (тривала). Така атака під час якої зловмисники прагнуть залишатися в системі непоміченими протягом місяців або навіть років (dwell time). Вони створюють безліч точок входу та резервних каналів, щоб повертатися до зламаної мережі навіть після часткового викриття;

– threat (загроза). Це керована людьми операція. Атакувальники мають чіткий план, конкретну мету та ресурси для її досягнення [1].

2. Специфіка АРТ-загроз в екосистемі Kubernetes

Архітектура кластерів виконується на основі ефімерності та мікросервісній взаємодії контейнерів, тому методи зломисників для впровадження АРТ-атаки суттєво відрізняються. У класичних мережах АРТ-групи забезпечують свою присутність через зміни в реєстрі ОС або створення прихованих файлів. У Kubernetes контейнери можуть бути запущеними всього декілька хвилин або секунд, тому звичайні методи закріплення не працюватимуть. Тому зломисники зосереджені на компрометації рівня оркестрації:

- контейнер бекдору. Шкідливий код зломисника запускається у контейнері кластера, використовуючи контролери Kubernetes, такі як DaemonSets або Deployments. Таким чином, можливо забезпечувати постійну кількість контейнерів, що працюють на одному або всіх вузлах кластера;
- з можливістю запису монтування hostPath. Для отримання стійкості на базовому хості зломисник, що має дозвіл на створення нового контейнера в кластері, також має можливість створити контейнер із записуванням томом hostPath. Том hostPath монтує каталог або файл з хоста до контейнера;
- планувальник завдань Kubernetes (CronJob). Використання об'єктів CronJob дозволяє зломиснику планувати запуск шкідливого коду через визначені проміжки часу. Якщо шкідливий под буде виявлено і видалено службою безпеки, то контролер CronJob автоматично створить новий екземпляр згідно з розкладом, забезпечуючи відновлення доступу до кластера [2];
- використання дійсних облікових записів (Valid Accounts). Зломисники можуть отримати та зловживати скомпрометованими обліковими даними (наприклад, kubeconfig файли або токени Service Accounts) для підтримки постійного доступу та уникнення виявлення. Оскільки такі дії виглядають як легітимна активність користувача чи сервісу, це дозволяє обходити стандартні механізми захисту та використовувати надмірні права (через RBAC) для доступу до обмежених ресурсів мережі без застосування додаткового шкідливого ПЗ [3].

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed Dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

Рис. 1. Матриця загроз Microsoft [2]

Відповідно матриці загроз від Microsoft, зображені на рис. 1, ключовими векторами компрометації стають не зовнішні периметри, а внутрішні механізми оркестрації та конфігурації:

- втеча з контейнера (Privilege Escalation). Використання вразливості ядра або помилки конфігурації, щоб вийти за межі ізольованого контейнера. Це дозволяє отримати контроль над вузлом кластера і доступ до всіх запущених на ньому процесів [3];
- бічне переміщення (Lateral Movement). Використання "плоскої" мережевої моделі кластера, де за замовчуванням дозволений трафік між подами, дозволяє зломиснику безперешкодно переміщуватися від скомпрометованого веб-сервісу до внутрішніх баз даних або API-сервера [2].

Головною метою АРТ-атаки є довготривале приховане перебування в системі для збору даних, і в середовищі Kubernetes досягнення цієї мети значно полегшується специфікою роботи контейнерів. Контейнери є ефемерними та можуть існувати лише кілька хвилин, що створює критичний "форензичний розрив". Після завершення роботи або примусового перезапуску пода всі локальні логи та тимчасові файли автоматично знищуються. Така архітектурна особливість формує ідеальні умови для зловмисника, оскільки сліди вторгнення зникають разом із контейнером ще до того, як служба безпеки встигає відреагувати на інцидент.

Ситуацію ускладнює стратегія маскування під легітимні процеси. Оскільки АРТ-групи орієнтовані на абсолютну непомітність, вони активно використовують стандартні інструменти кластера, такі як `kubectl` або вбудовані дашборди, для проведення розвідки та експлуатації даних. Використання штатних засобів у поєднанні з постійною динамічною зміною IP-адрес робить зловмисну активність майже невидимою для класичних засобів моніторингу, які часто не здатні відрізнити дії атакуючих від легітимних операцій адміністраторів [2].

3. Методи виявлення та протидії АРТ-загрозам у середовищі Kubernetes

Архітектура Kubernetes, її специфіка та вектори атак, що наведені та описані в матриці загроз Microsoft, чітко демонструє, що задля захисту та безпеки системи необхідна комплексна стратегія. Для ефективного захисту від АРТ-атак захист повинен базуватись на Zero Trust та безперервного моніторингу, оскільки зловмисники використовують легітимні інструменти задля входження в систему.

Основним методом зловмисника для закріплення в системі є компрометація облікових записів, тому елементом захисту може виступати посилення політик RBAC (Role-Based Access Control). Сервісні акаунти не повинні мати прав адміністратора або дозволів на створення нових подів, якщо це не вимагається їх функціоналом. Для того, аби зменшити можливість використання викрадених облікових даних для тривалого доступу, потрібно проводити регулярну ротацію токенів та впровадити багатофакторну аутентифікацію для доступу до API-сервера [3].

Для протидії бічному переміщенню, необхідно відмовитися від плоскої мережевої моделі. Використання Network Policies дозволяє ізолювати простори імен та мікросервіси один від одного, залишаючи лише явно дозволений трафік (whitelisting). Це створює бар'єри для зловмисника, тому навіть у разі зламу одного контейнера, доступ до баз даних або інших критичних вузлів буде заблоковано на рівні мережі.

Для вирішення проблеми форензичного розриву та виявлення бекдорів необхідно впроваджувати засоби безпеки на етапі виконання. Слід аналізувати поведінку процесів у реальному часі, виявляти спроби запуску оболонки (shell) всередині контейнера, нетипові мережеві з'єднання або спроби монтування чутливих директорій хоста. Такий підхід дозволяє ідентифікувати АРТ-активність навіть якщо зловмисник використовує методи маскування під легітимні системні процеси [1].

Налаштування та збереження журналів аудиту (Kubernetes Audit Logs) також є важливим аспектом в захисті. Оскільки АРТ-атаки часто розтягнуті у часі, наявність історичних даних про всі запити до API-сервера дозволяє виявити аномальну поведінку легітимних користувачів ще до того, як буде завдано критичної шкоди. Це дає змогу реконструювати ланцюжок дій зловмисника навіть після знищення слідів у контейнерах, ефективно закриваючи питання форензичного розриву.

Ефективна протидія АРТ-атакам у Kubernetes неможлива без переходу від статичного захисту периметра до ешелонованої оборони. Поєднання суворого контролю доступу (RBAC), мікросегментації мережі та глибокого аналізу поведінки в реальному часі дозволяє нівелювати переваги зловмисників, які надає їм ефемерність контейнерів. Реалізація цих заходів створює середовище "нульової довіри", де успішний злам одного компонента не гарантує зловмиснику контроль над усім кластером.

Побудова безпеки у Kubernetes – це не статичний стан, а безперервний та динамічний процес адаптації. Комплексне застосування RBAC, мережевої ізоляції, Runtime-захисту та аудиту створює глибоко ешелоновану оборону, яка робить економічно не вигідним і технічно надскладним тривале приховане перебування зловмисника в кластері.

Висновки

У роботі проаналізовано природу та специфіку Advanced Persistent Threats у середовищі Kubernetes. Встановлено, що ключовою проблемою виявлення таких загроз є «форензичний розрив», зумовлений ефемерністю контейнерів. Знищення пода призводить до втрати цифрових логів, тимчасових файлів, що дозволяє зловмисникам уникати відповідальності.

Дослідження векторів атак (згідно з матрицею Microsoft та MITRE) показало, що сучасні АРТ зосереджені не на зовнішньому зламі, а на компрометації ланцюга постачання, використанні легітимних інструментів адміністрування та зловживаннями правами доступу (RBAC) для забезпечення стійкості у кластері.

На основі проведеного дослідження визначено, що ефективна протидія АРТ-загрозам вимагає відмови від традиційного захисту периметра на користь комплексної стратегії. Вона має включати сувору мінімізацію привілеїв, мережеву мікросегментацію для блокування бічного переміщення та впровадження засобів runtime-безпеки. Лише такий підхід дозволяє виявляти аномальну поведінку в реальному часі та нівелювати переваги, які надає зловмисникам динамічна природа хмарного середовища.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. APT Attacks: What Is an Advanced Persistent Threat? [Електронний ресурс]. – Режим доступу: <https://datami.ee/ua/blog/apt-attacks-what-is-an-advanced-persistent-threat/> (дата звернення: 14.12.2025).
2. Attack matrix for Kubernetes / Microsoft Security Blog [Електронний ресурс]. – Режим доступу: <https://www.microsoft.com/en-us/security/blog/2020/04/02/attack-matrix-kubernetes/> (дата звернення: 14.12.2025).
3. MITRE ATT&CK® Technique T1078: Valid Accounts [Електронний ресурс]. – Режим доступу: <https://attack.mitre.org/techniques/T1078/> (дата звернення: 14.12.2025).

Крістіна Вікторівна Пугачева – студентка групи 2KITC-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: kristipref@gmail.com;

Науковий керівник: Анатолій Васильович Грицак – доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Kristina V. Puhacheva – student of group 2KITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: kristopref@gmail.com;

Supervisor: Anatolii V. Hrytsak – Assistant Professor of the Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia.