

Article

Evil Twin Attack in Wi-Fi Networks: Evolution, Mutation Taxonomy, and Exposure Time Analysis (2005–2026)

Piotr Augustyniak  and Piotr Zwierzykowski * 

Institute of Communication and Computer Networks, Poznań University of Technology, 61-131 Poznań, Poland; piotr.augustyniak@put.poznan.pl

* Correspondence: piotr.zwierzykowski@put.poznan.pl

Abstract

The Evil Twin attack, which involves creating rogue Wi-Fi access points that impersonate legitimate networks, remains one of the most persistent and adaptive threats in cybersecurity, despite more than two decades having passed since its first public demonstration in 2005. This paper aims to provide a comprehensive analysis of the evolution of this attack, perceived as an “invisible enemy” due to its low detectability and systematic underestimation in incident reports. The study addresses key questions: how the Evil Twin attack has evolved, how its methods and tools have changed, where it currently stands, and where it may be heading in the future. The paper compiles evidence from conference presentations, academic publications, government reports, industry analyses, and media coverage, as well as selected defense mechanisms such as WIPS, WPA3, Protected Management Frames, ETGuard, and the Trusted Wireless Environment framework. An original taxonomy of Evil Twin attack mutations is proposed, along with a ten-stage Kill Chain model ([A]–[J]) mapped onto the MITRE ATT&CK framework, an exposure time metric T_e as a key evolutionary parameter, and models quantifying attack cost-effectiveness and efficiency. The analysis demonstrates that the Evil Twin remains a persistent and adaptive threat, whose effectiveness stems from the combination of technical vulnerabilities, user trust in familiar network names, and the difficulty of unambiguous attribution and classification of incidents.

Keywords: evil twin; rogue access point; Wi-Fi security; wireless networks; WIPS; WPA3; trusted wireless environment; man-in-the-middle; cybersecurity

1. Introduction

The Evil Twin attack involves the creation of a rogue wireless access point that impersonates a legitimate network by replicating its service set identifier (SSID) and configuration parameters, with the objective of intercepting network traffic or user credentials.

Although the term “Evil Twin” is occasionally used interchangeably with broader categories such as rogue access points or Wi-Fi honeypots in security literature, it strictly refers to a specific subclass of threats characterized by the deliberate and deceptive impersonation of an existing, legitimate network infrastructure.

Following its first public demonstrations in 2004–2005, the Evil Twin attack has undergone a profound transformation over the past two decades. It has evolved from rudimentary, proximity-dependent rogue access points into highly automated, ephemeral variants that leverage modern technologies, advanced social engineering, and process automation.

This paper presents a comprehensive narrative and conceptual review of the evolution of the Evil Twin attack from 2005 to 2026. Table 1 provides a chronological overview of key events.



Academic Editors: Hung-Yu Chien and Yu-an Tan

Received: 1 June 2026

Revised: 19 July 2026

Accepted: 29 July 2026

Published: 3 August 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Table 1. Chronology of key events related to the Evil Twin attack (2005–2025).

Year	Type	Event/Significance
2005	Demo	Black Hat USA—“Rogue Squadron” (Beetle, Potter); first public ET demonstration [1].
2007	Demo	DEF CON 15—“Multipot”; multi-point ET variant bypassing WIPS [2,3].
2008	Tool	KARMA—ET automation through probe request listening [4].
2011	Demo	Black Hat—Ramachandran workshops; practical ET training [5,6].
2013	Tool	MANA—KARMA extension incorporating WPA-Enterprise attacks [7].
2013	Case study	University of Santiago de Guayaquil—ET + SET + cloned captive portal [8,9].
2016	Incident	Avast at RNC, Cleveland—1200+ victims, 68.3% identities exposed [10,11].
2018	Incident	GRU vs. OPCW, The Hague—confirmed intelligence operation (close-access) [12–14].
2018	Standard	WPA3 + PMF (IEEE 802.11w)—management frame protection [15,16].
2018–2019	Incident	DOI OIG, USA—ET test across 91 government locations; no detection [17].
2018	Standard	Trusted Wireless Environment—6 Wi-Fi threat categories [18].
2019	Research	ETGuard (Jain et al.) —ET detection based on beacon fingerprinting [19].
2021–2023	Research	WatchGuard Threat Lab—tests across 45+ locations; 91% vulnerable [20].
2024	Incident	Australia—ET attacks at airports; 7-year and 4-month sentence [21,22].
2025	Incident	Brazil—media warnings against ET in public networks [23–25].

Research objectives. The primary objectives of this study are: (i) to provide a systematic chronological analysis of key incidents, demonstrations, and academic publications; (ii) to propose a mutation taxonomy of Evil Twin attacks; (iii) to introduce an exposure time metric T_e as a quantitative evolutionary parameter; (iv) to map these threats onto the MITRE ATT&CK framework using a proposed ten-stage Kill Chain model; and (v) to identify systemic gaps in detection, classification, and incident reporting practices.

Scope and delimitation. The scope of this work is restricted to the strict definition of the Evil Twin attack: the impersonation of a legitimate access point using an identical SSID. Related techniques, such as KARMA, MANA, or KRACK, are discussed only insofar as they contribute to the evolutionary context of Evil Twin attacks; they are not analyzed as primary attack models within this study.

Contribution. The main contributions of this paper include a novel mutation taxonomy, the introduction of the exposure time metric T_e along with its associated analytical models, and a complementary Kill Chain framework specifically tailored to the evolution of wireless attacks.

Organization of the paper. The remainder of this paper is organized as follows. Section 2 describes the narrative and conceptual methodology employed. Section 3 discusses challenges related to the documentation and misclassification of Evil Twin attacks. Section 4 provides a chronological analysis of key incidents and demonstrations. Section 5 presents the proposed conceptual frameworks, including the MITRE ATT&CK mapping, the ten-stage Kill Chain model, the exposure time metric T_e , and the mutation taxonomy. Section 6 outlines hypotheses regarding the future evolution of the attack, Section 7 discusses key methodological limitations, and Section 8 summarizes the findings and conclusions.

Table 1 presents a chronological overview of key events related to the Evil Twin attack. Events are classified into six categories according to their role in the evolution of the threat: *Demo*—public demonstrations and conference workshops (e.g., Black Hat, DEF CON); *Tool*—emergence of new offensive tools or frameworks; *Incident*—confirmed attacks, penetration tests (red team), field experiments, and their legal aftermath; *Standard*—introduction of technical standards or security frameworks; *Research*—scientific publications and research projects; and *Case study*—case studies of educational or documentary nature. This typology was adopted to ensure a consistent classification of events ranging from purely demonstrative to operational, while maintaining the readability of the chronology.

2. Methodology

This paper adopts the form of a **narrative and conceptual review**. This approach was deliberately chosen given the heterogeneous and fragmented nature of the available evidence on Evil Twin attacks. These attacks are documented across academic literature,

government reports, industry threat intelligence, conference presentations, and publicly reported incidents—many of which are not indexed in standard bibliographic databases and lack uniform reporting standards.

A strictly systematic protocol (e.g., PRISMA-style review) would not be optimal in this case, as it would fail to fully capture the heterogeneous evidence necessary to reconstruct the evolution of the attack across technical, operational, and incident-response domains. The narrative and conceptual approach enables a broader chronological and thematic synthesis, facilitating the identification of long-term trends and the formulation of proposed conceptual frameworks.

Sources were included based on the following explicit criteria: they had to contain either a description of a publicly reported incident, a technical description of the attack mechanism, an analysis of defense mechanisms, or threat intelligence observations directly related to Evil Twin attacks. Reliability was ensured through data triangulation and cross-verification between academic and institutional sources. Peer-reviewed journal and conference publications constitute the technical and analytical backbone of this review, whereas government and institutional reports, standardization documents, and primary incident records (including agency communications and contemporaneous press coverage) are used as primary evidence for specific real-world events rather than as analytical sources, and the two categories are weighted accordingly during triangulation. Key methodological and data-related limitations are discussed in the Limitations section.

A simplified source selection process, adapted from the PRISMA methodology for the purposes of this narrative review, is presented in Figure 1.

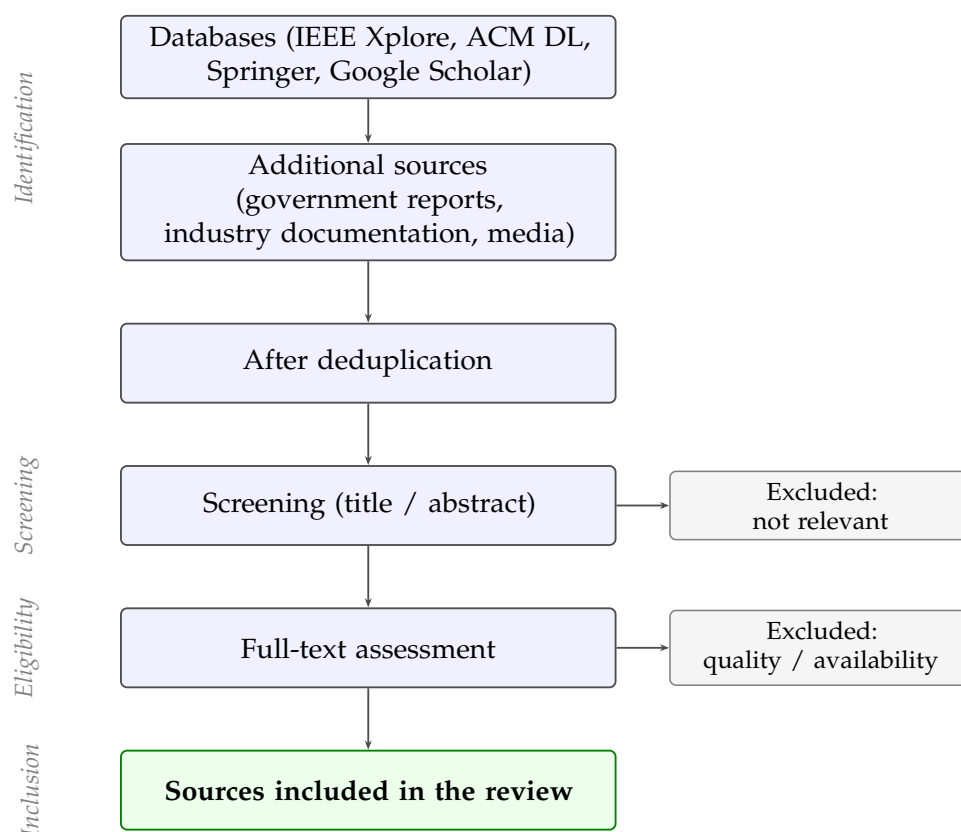


Figure 1. Simplified source selection diagram (adapted from PRISMA) for narrative review.

Stage 1—Data collection. Data were collected from diverse, credible sources of academic, industry, and institutional character, covering the period from 2005 to January 2026. The main source categories were:

- **Scientific and conference literature:** a review of presentations and papers from key events such as Black Hat USA (2005, 2011, 2015, 2016), DEF CON (2007), and academic publications.
- **Security institution and government reports:** analysis of official documents, including the Office of Inspector General (OIG) report, OPCW statements, WatchGuard Threat Lab research, and CISA and ENISA reports.
- **Recent industry data from 2025 to 2026:** CVE vulnerability reports, vendor analyses, and data from NIST, Verizon DBIR, and IBM X-Force Threat Intelligence.

Source selection was based on the criteria of relevance (direct reference to Evil Twin or rogue AP), recency, and diversity. In total, over 100 sources were analyzed.

Stage 2—Data analysis. The analysis was conducted along two dimensions: chronological (tracking the attack evolution from 2005 to 2026) and thematic (classification of attack mutations). A data triangulation method was employed, involving cross-comparison of documented incidents with deployed defense mechanisms and identified gaps. In quantitative terms, a statistical analysis was conducted, focusing on the phenomenon of underestimation and misclassification of Evil Twin attacks in industry reports.

Stage 3—Synthesis and original contribution. Based on the conducted data analysis, a synthesis of key trends was developed: the gradual shortening of the rogue access point lifespan, the transition from attacks requiring prolonged physical presence to ephemeral variants, the hybridization of techniques, and the systematic underestimation of the attack in industry reports.

The primary contribution is the proposed mutation taxonomy, the exposure time metric T_e , the Kill Chain model, and the mapping onto the MITRE ATT&CK framework. Key methodological and data-related limitations of this synthesis are discussed in the Limitations section.

3. The Problem of Documentation and Classification of Evil Twin Attacks

Despite the technical feasibility and confirmed demonstrations, the number of publicly documented, real-world Evil Twin attacks resulting in legal proceedings remains small. A review of the literature and industry reports allows the identification of several systematic causes of this phenomenon.

3.1. Low Attack Detectability

The Evil Twin attack is characterized by a high degree of mimicry—the victim connects to a fake network with an identical SSID, observing no anomalies at the user interface level. Data interception occurs transparently (traffic sniffing or presentation of a fake login portal). The consequences of the attack often become apparent only after weeks or months (e.g., unauthorized banking transactions, account takeovers), which leads to systematic underreporting (i.e., incidents being reported to a lesser extent than they actually occur, deflating statistics) of the phenomenon.

Detection methods (packet timing analysis, signal triangulation, beacon fingerprinting) require specialized knowledge and tools unavailable to average users [7,26]. The disparity between the ease of preparing the attack (tools such as Wi-Fi Pineapple, hostapd-wpe, Wifiphisher [4]) and the complexity of its detection constitutes a significant factor contributing to the low reporting rate.

3.2. Difficulties in Identifying and Apprehending the Perpetrator

The Evil Twin attack is short-lived and mobile in nature—the attacker uses portable equipment (laptop, Raspberry Pi, Wi-Fi card), operates for a few minutes to several hours, and then leaves the location. The absence of permanent infrastructure (unlike botnets or

C2 servers) and the lack of traces in the victim's infrastructure logs significantly impede perpetrator identification. The physical proximity required to conduct the attack makes it targeted, yet simultaneously difficult to monitor at scale.

3.3. Misclassification in Industry Reports

In leading industry reports (Verizon DBIR, IBM X-Force, ENISA Threat Landscape), there is no separate category for "Evil Twin" or "Rogue Access Point". Incidents exhibiting characteristics of this attack vector are classified as phishing, Man-in-the-Middle [27], identity theft, or unauthorized access. At the level of analytical platforms, SIEM tools (Splunk, QRadar) and the MITRE ATT&CK framework do not possess a dedicated tag for Evil Twin attacks, resulting in their labeling as MitM or phishing by SOC (Security Operations Center) and DFIR (Digital Forensics and Incident Response) teams.

3.4. Impact of Protective Mechanisms on Attack Attractiveness

The development of transport layer protections such as HTTPS Everywhere (a browser extension enforcing encrypted HTTPS connections) and HSTS (HTTP Strict Transport Security, a server-side mechanism forcing HTTPS usage) has reduced the effectiveness of basic attack variants. At the same time, the absence of a central, global incident database distinguishing Evil Twin attacks further contributes to the underestimation of the phenomenon's scale in global statistics.

The issues described above are also reflected in the fragmented nature of existing survey and review literature. While multiple studies address individual aspects of Evil Twin attacks, including detection techniques, classification approaches, and WLAN security frameworks, they generally do not provide a unified model capturing temporal evolution, attack lifecycle, and structured adversarial adaptation. This fragmentation limits the ability of the existing literature to represent Evil Twin attacks as a coherent, evolving phenomenon across technical, operational, and empirical domains.

Existing survey and review studies on wireless LAN security and Evil Twin attacks can be broadly grouped into four categories. The first category focuses on detection techniques for rogue access points and Evil Twin attacks, including RSSI-based fingerprinting, MAC address verification, and anomaly detection methods. While effective in constrained environments, these works do not model temporal evolution or attack lifecycle progression.

The second category consists of wireless intrusion detection system (WIDS) surveys, which provide broad taxonomies of WLAN threats and defensive mechanisms using signature-based and anomaly-based approaches. However, these studies generally treat attacks as static events rather than dynamic and evolving processes.

The third category includes classification-oriented studies of rogue access points, which introduce structured taxonomies of attack types and mitigation strategies. These taxonomies are typically static and do not incorporate temporal dynamics, adversarial adaptation, or exposure-based modeling.

The fourth category comprises industry threat-classification frameworks and large-scale incident reports, which aggregate incidents at scale but provide no dedicated Evil Twin or rogue access point category, so that such events are recorded as phishing, Man-in-the-Middle, or unauthorized-access intrusions.

Table 2 summarizes the positioning of this work against representative categories of the existing survey literature.

Table 2. Positioning of this work within existing survey literature on WLAN security and Evil Twin attacks.

Literature Group	Scope	Methodology	Limitations Addressed by This Work
Evil Twin/Rogue AP detection studies	Detection mechanisms (RSSI, MAC filtering, anomaly detection)	Technical comparison of detection methods	No temporal modeling or attack lifecycle representation (e.g., [26,28–33])
Wireless intrusion detection surveys	WLAN threat classification and defense frameworks	Static taxonomy + ML/IDS methods	Lack of dynamic or evolutionary attack modeling (e.g., [34–38])
Rogue AP classification studies	Structural classification of attack types	Static taxonomies	No exposure-time modeling or adversarial adaptation (e.g., [39–41])
Industry frameworks and threat reports	Cyber threat classification and reporting standards	Large-scale incident aggregation reports	No dedicated Evil Twin category; misclassification into MitM/phishing (e.g., [42–45])
This work	Evil Twin attacks (2005–2026), mutation taxonomy, exposure-time model (T_e), kill-chain framework	Narrative + conceptual + temporal modeling	Unified structural and temporal representation of attack evolution

4. Chronological Analysis of Key Incidents and Demonstrations

This section presents a chronological review of key events related to the Evil Twin attack, encompassing conference demonstrations, confirmed incidents, scientific publications, and industry initiatives over the period 2005–2025. Each case study is described in a standardized format: context, method employed, outcome, and significance for the evolution of the attack.

4.1. Black Hat USA 2005: First Public Demonstration

The first publicly documented demonstration of the Evil Twin attack was conducted at the Black Hat USA conference in 2005. The presentation entitled “Rogue Squadron: Evil Twins, 802.11intel, Radical RADIUS, and Wireless Weaponry for Windows”, by Beetle and Bruce Potter (The Shmoo Group) [1], included a detailed discussion of the mechanism for creating a competing access point with an identical SSID and higher signal strength in order to intercept user connections.

The demonstration showcased the use of tools such as Airsnarf (SoftAP, DHCP, fake DNS server, Apache) for creating a rogue access point. Attacks on captive portals, web authentication, and EAP protocols (PEAP, TTLS, MSCHAPv2) were demonstrated, enabling credential interception even in WPA/Enterprise networks. This presentation established the Evil Twin as a viable threat vector for public and conference environments.

4.2. DEF CON 15 (2007): The Multipot Variant

At the DEF CON 15 conference in 2007, KN Gopinath presented the work “Multipot: A More Potent Variant of Evil Twin” [2,3], introducing a multi-point attack variant. Unlike the classic Evil Twin utilizing a single rogue access point, Multipot was based on the simultaneous operation of multiple access points on different channels (e.g., channels 3 and 10) with an identical SSID.

The significance of this demonstration lay in revealing the ineffectiveness of WIPS systems based on the deauthentication mechanism. In a multi-point configuration, after session interruption on one channel, the client automatically switched to an alternative access point, maintaining TCP/HTTP communication continuity. The demonstration showed that with an $N + 1$ access point configuration (where N denotes the number of channels simultaneously monitored by the WIPS sensor), the attack becomes resistant to session isolation.

4.3. Black Hat Workshops (2011–2016): Practical Training

During 2011–2016, a series of advanced workshops on wireless network security were conducted at Black Hat conferences, led by Vivek Ramachandran and Thomas d’Otreppe de Bouvette (Thomas d’Otreppe de Bouvette—creator of Aircrack-ng, the most popular Wi-Fi security auditing toolkit (first version: February 2006) and the OpenWIPS-ng wireless intrusion detection system) [6].

The 2011 workshops [5] covered the practical execution of Evil Twin attacks using hostapd and dnsmasq tools, forcing device reconnection to the rogue access point via deauthentication (aireplay-ng), and performing Man-in-the-Middle attacks on HTTP/HTTPS traffic. Subsequent editions (2015 [46], 2016 [47]) expanded the scope to include radio spectrum analysis and advanced key cracking techniques, confirming that despite the introduction of HTTPS and HSTS, the combination of deauthentication and a cloned captive portal continued to pose a real threat.

4.4. Case Study: University of Santiago de Guayaquil (2013)

Briones, Coronel, and Chavez-Burbano [8] described a practical case study of an Evil Twin attack conducted in the academic environment of the University of Santiago de Guayaquil (Ecuador). The paper documented a scenario in which the attacker created a rogue access point impersonating the university network protected by the WPA-EAP (802.1X) protocol, and subsequently used the Social Engineering Toolkit (SET) [9] to clone the login page (captive portal) and intercept user credentials.

Although the paper did not introduce a new detection or attack method, it constituted an important example of the Evil Twin’s transition from pure traffic sniffing to a variant based on phishing supported by a rogue access point. The study demonstrated that in environments with poorly configured radio authentication, the user is unable to distinguish the legitimate network from the fake one at the device interface level.

4.5. Republican National Convention in Cleveland (2016)

In July 2016, during the Republican National Convention (RNC) in Cleveland (Ohio), numerous rogue Wi-Fi networks were identified with names referencing the political context (e.g., “Vote Hillary”, “Vote Trump”, and “FBI Surveillance Van”) [10]. Journalists, including Glenn Greenwald [11] (The Intercept), identified at least a dozen rogue access points in the vicinity of the Quicken Loans Arena convention center.

The rogue networks were characterized by stronger signals than the legitimate access points, and upon connection, users were exposed to network traffic interception or redirected to cloned login pages. This incident constituted one of the most widely publicized cases of an Evil Twin attack in the context of a large-scale political event and highlighted the vulnerability of Wi-Fi infrastructure to social engineering attack variants in high-turnover user environments.

4.6. GRU Operation Against the OPCW in The Hague (2018)

In April 2018, four officers of the Russian military intelligence service (GRU, Unit 26165/APT28) conducted a close-access operation directed against the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague, which at that time was investigating the poisoning of Sergei Skripal [48] using the Novichok nerve agent [36] and the alleged chemical attack in Douma (Syria) [49].

Cyber operators Aleksei Morenets [50] and Yevgeny Serebriakov [51], along with HUMINT (Human Intelligence) support (Oleg Sotnikov [52], Aleksei Minin [53]) [54], placed Wi-Fi signal interception equipment (panel antennas, laptops, Wi-Fi Pineapple or an analogous device) in the trunk of a rental car parked near the OPCW headquarters. The

objective was to create a rogue access point impersonating the organization's legitimate network in order to intercept login credentials [12–14].

The operation was disrupted on 13 April 2018, by the Dutch military intelligence service MIVD in cooperation with allies. Analysis of the seized equipment confirmed earlier operations against WADA in Switzerland and Malaysia [55]. This incident constitutes one of the best-documented cases of the use of a close-access Evil Twin attack in an intelligence operation, confirming that this vector is employed by state-sponsored threat actors (APTs) in the context of espionage.

4.7. DOI OIG Penetration Tests (2018–2019)

In 2018–2019, the Office of Inspector General (OIG) of the U.S. Department of the Interior (DOI) conducted a series of ethical penetration tests using the Evil Twin attack, described in a report from September 2020 [17].

Tests were conducted across 91 locations representing all offices and organizational units of the DOI, using low-cost equipment (Raspberry Pi 2 with open-source Kali Linux software (<https://www.kali.org/>, accessed on 31 July 2026), cost below 200 USD per unit), controlled via a smartphone from publicly accessible places (e.g., park benches and visitor areas). The attacks were not detected by IT security systems or physical security at any of the tested locations. In the networks of four offices, user credentials were successfully obtained and used to gain access to wireless networks.

The report constitutes one of the best-documented examples of ethical use of the Evil Twin attack in a government environment, simultaneously demonstrating the low cost of conducting the attack, high effectiveness, and the absence of detection capabilities on the defenders' side.

4.8. ETGuard: D2D Attack Detection (2019)

Jain, Laxmi, Gaur, and Mosbah [19] proposed the ETGuard framework for detecting Evil Twin attacks in 802.11a/b/g networks, operating in pre-association mode based on beacon frame fingerprinting. The system, based on a client–server architecture, analyzed temporal sequences and beacon frame fields, demonstrating that the temporal emission profile is unique to each access point and can serve to distinguish a legitimate AP from a rogue one.

The research involved 12 attack scenarios using three types of rogue access point implementation: hardware (dedicated AP), software (laptop as soft AP), and mobile (phone as hotspot). Tests demonstrated high detection accuracy (no false negatives and one false positive). Furthermore, the authors demonstrated a new scenario in which the Evil Twin served as a temporary infection vector for mobile devices (particularly Android)—the rogue access point operated only until the malicious payload was delivered via the captive portal, after which it was deactivated.

The work demonstrated that most existing WIPS/WIDS systems (Cisco WLC, Aruba, and AirTight) are unable to detect short-lived, ephemeral Evil Twin variants, opening a new research direction in passive detection based on beacon frame analysis. Alternative approaches include the use of SDN architecture for centralized detection [40], client-side RTT analysis [33], and machine learning techniques on AWID3 datasets [56].

4.9. WatchGuard Threat Lab Research (2021–2023)

The WatchGuard Threat Lab team conducted an empirical verification of the security level of publicly available Wi-Fi networks across more than 45 facilities in multiple countries (including the USA, Poland, the United Kingdom, Germany, and Brazil), encompassing international airports, hotel chains, and restaurant chains [20].

The study was based on the verification of six threat categories defined within the Trusted Wireless Environment (TWE) standard [18], announced by WatchGuard Technologies in 2018. The TWE standard defines six Wi-Fi threat categories requiring automatic detection and blocking: (1) Rogue Access Point—an unauthorized access point connected to the LAN; (2) Evil Twin Access Point—an access point impersonating a legitimate network; (3) Neighbor Access Point—an unsecured neighboring network; (4) Rogue Client—a device carrying malware; (5) Ad Hoc Network—direct P2P connections bypassing security; and (6) Misconfigured Access Point—configuration errors facilitating attack. This classification became the basis for industry certifications (e.g., Security+) [57].

The researchers verified both the vulnerability to Evil Twin attacks and the depth of post-exploitation data access, encompassing Man-in-the-Middle attacks with code injection (traffic injection), HTTP data interception, and simulation of fake login prompts (credential harvesting).

Key findings indicate that: (a) none of the tested hotels passed the test successfully; (b) most locations had advanced firewalls but lacked protection at the radio layer (no WIPS systems); (c) only 9% of locations (exclusively in the United Kingdom) had active prevention systems capable of automatically blocking rogue access points; and (d) 91% of tested locations were vulnerable to the Evil Twin attack.

These results provided an argument for accelerating the deployment of the WPA3 standard and Protected Management Frames (PMF) functionality. Independent tests conducted by Miercom [58] demonstrated that most leading wireless infrastructure vendors (Cisco, Aruba, Ruckus, and Ubiquiti) without a dedicated WIPS module are unable to automatically block an Evil Twin attack. Furthermore, it was shown that only access points with a dedicated third radio for continuous band scanning are able to maintain the TWE standard without interrupting data transmission.

The TWE standard is sometimes criticized as “marketing packaging” for WIPS technology that existed previously. However, it should be noted that before the introduction of TWE, there was no unified, measurable definition of radio security requirements that went beyond connection encryption (WPA2/WPA3). TWE established a security threshold encompassing automatic detection and blocking of six threat categories, which influenced the development of requirements for the hospitality industry [20] and critical infrastructure.

Table 3 summarizes the discussed defense mechanisms, indicating their type, scope of operation, and key limitations in the context of protection against the Evil Twin attack. Mechanisms are ordered chronologically by year of introduction (or earliest publication), allowing the evolution of defensive approaches to be traced in parallel with the development of the attack itself.

4.10. Attacks at Airports in Australia (2024)

In April and May 2024, the Australian Federal Police arrested a man accused of conducting a series of Evil Twin attacks aboard domestic flights and at airports in Perth, Melbourne, and Adelaide [21,22]. The attacker used a portable Wi-Fi access point to create rogue networks with identical names (SSIDs) to the official airline hotspots (e.g., “Qantas Free Wi-Fi”). Upon connecting, passengers were redirected to cloned login pages where they submitted credentials for email and social media accounts.

Detection occurred when airline personnel reported a suspicious network. The perpetrator was charged with 9 cybercrime offences, carrying a maximum penalty of up to 10 years imprisonment. This case constitutes one of the few documented Evil Twin attacks in a mobile environment that resulted in criminal prosecution, confirming the effectiveness of this attack vector in high-turnover environments despite the widespread adoption of HTTPS and WPA3.

4.11. Attack Warnings in Brazil (2025)

In 2025, Brazilian technology media published a series of warnings regarding Evil Twin attacks on public networks in major metropolitan areas, particularly in São Paulo [23,24]. Reports by TechTudo [23], Olhar Digital [24], and Canaltech [25] documented scenarios in which attackers created rogue access points with SSIDs identical to legitimate networks in shopping centers and public transport stations, employing Man-in-the-Middle techniques and fake captive portals to intercept credentials and financial data.

Although these publications were primarily media warnings (without detailed police reports or victim statistics), they indicated a growing threat in countries experiencing rapid expansion of public Wi-Fi availability. Recommendations from security agencies (CISA, NCSC, CERT-FR) advising users to disable Wi-Fi in public spaces corroborated the continued relevance of this threat.

Table 3. Comparison of defense mechanisms against the Evil Twin attack.

Mechanism	Year	Protection Type	Scope of Operation	Limitations Against ET
WPA2-Enterprise (EAP-TLS)	2004	Mutual authentication	RADIUS certificate verification; encrypted transmission	Requires PKI; not for public networks; client may accept forged cert.
Clock skew/HW FP	2008–2014	Passive detection	AP ID via TSF clock skew [28,59] or HW traits [32]	Calibration needed; environmental sensitivity; limited scalability
PMF (802.11w)	2009/18	Frame protection	Blocks deauth/disassoc spoofing; mandatory in WPA3 [15]	No protection against ET without deauth (new clients, open nets, auto-connect) [16]
WIPS (dedicated radio)	2010+	Active det./blocking	Continuous scanning; rogue AP detection; containment frames	Dedicated HW with 3rd radio; ineffective for short ET (<60 s); cost
Cisco wIPS/CleanAir	2010+	Spectrum + WIPS	Interference and rogue AP detection at spectrum level [60,61]	Cisco HW only; no protocol-level attack detection
Client-side detection	2010–2018	Active/passive	Route analysis [31]; WiFiHop [62]; stats [30]; channel mon. [29]; TCP delay [63]	Network-dependent; limited in high-load networks
Aruba RFProtect	2012+	Multi-sensor	Threat classification; auto rogue AP containment [64]	Sensor density dependent; false positives in multi-tenant env.
Meraki Air Marshal	2014+	Cloud WIPS	Auto SSID spoof detection; cloud mgmt [65]	Requires cloud; limited local policy control
WPA3-SAE	2018	Encryption	No offline dictionary attacks; forward secrecy; per-session protection [66,67]	Does not verify AP identity—encrypted connection to rogue AP possible [68]
TWE (6 categories)	2018	Comprehensive standard	Auto detection and blocking of 6 Wi-Fi threat types; HW cert.	Single vendor (WatchGuard); certified HW required; no independent audit
ETGuard	2019	Passive fingerprinting	Beacon frame sequence analysis; real-time pre-assoc. detection	Academic prototype; 802.11a/b/g only; needs production validation
EvilScout (SDN)	2020	Detection + mitigation	SDN-based centralized ET detection and containment [40]	Requires SDN; not for traditional networks
ML-based WIDS	2022–2023	ML classification	Feature sel. + classifiers on AWID/AWID3 [56,69]; CSI FP [37]	Training data needed; limited cross-HW generalisability
Sig.-based MC-MitM IDS	2024	Passive signature-based	Distributed multi-ch. MitM detection [38,70]; TPR $\geq 90\%$	60 s delay; sensor deployment; known signatures only

5. Proposed Conceptual Frameworks: Analysis, Modeling, and Classification of the Evil Twin Attack

5.1. MITRE ATT&CK and the Evil Twin Attack

Within the MITRE ATT&CK framework, the Evil Twin attack does not appear as a distinct, standalone technique. It constitutes an example of a complex entry vector that, depending on its implementation, may realize multiple tactics and techniques simultaneously. From the MITRE ATT&CK perspective, Evil Twin represents a compelling example of threat evolution, having progressed from a simple, technical Wi-Fi attack to an advanced campaign initialization mechanism.

Within MITRE ATT&CK (In MITRE ATT&CK, the closest techniques are: T1557—Adversary-in-the-Middle and T1595—Active Scanning), Evil Twin is not a distinctly delineated technique but rather a complex attack vector. Fundamentally, Evil Twin corresponds to the Initial Access tactic (TA0001). As attack techniques evolved, the scope of applicable tactics expanded to include:

- Credential Access (TA0006)—credential theft through phishing on captive portals;
- Collection (TA0009)—passive and active network traffic eavesdropping;

- Defense Evasion (TA0005)—circumvention of HTTPS protections (e.g., SSL stripping);
- Command and Control (TA0011)—integration with command and control channels;
- Lateral Movement (TA0008)—leveraging obtained credentials for lateral movement within the network.

The evolution of the Evil Twin attack has been divided into successive phases, with particular emphasis on their characteristics and the corresponding scope of MITRE ATT&CK tactics.

Period 2004–2007: Classical Evil Twin and deauthentication attacks. The earliest form of the attack consisted of establishing a rogue access point with an SSID identical to that of the legitimate network. The primary objective was passive data collection through traffic sniffing. The attack aligned almost exclusively with the Initial Access and Collection tactics.

Period 2008–2013: Automation and captive portal phishing (KARMA/MANA). The KARMA and MANA techniques enabled active responses to probe requests, significantly increasing the effectiveness of connection hijacking. Evil Twin began to realize the Credential Access tactic.

Period 2014–2017: Active Man-in-the-Middle and HTTPS circumvention. The widespread adoption of HTTPS and HSTS necessitated further adaptation—SSL stripping techniques and traffic manipulation. Feng et al. [71] additionally demonstrated the feasibility of conducting a MitM attack without a rogue access point, utilizing ICMP redirects. The attack already encompassed elements of Defense Evasion.

Period 2018–2019: Close-access Evil Twin and short-lived variants. Attacks became short-lived, precisely targeted, and executed in close proximity to the victim. The scope of the attack expanded to include Lateral Movement.

Period 2020–2022: Ultra-short emissions and malware delivery. Further reduction of rogue AP activity time to several tens of seconds, facilitated by the circumvention of PMF mechanisms [15,16]. The objective increasingly shifted towards malware delivery—the Command and Control tactic.

Period 2023–2025: “Flash” Evil Twin and integration with offensive campaigns. The most recent phase is characterized by a high degree of automation. Evil Twin no longer functions as a standalone attack but rather as a module initiating a full kill chain, encompassing multiple MITRE ATT&CK tactics simultaneously.

Table 4 presents the evolution of the Evil Twin attack within the context of the MITRE ATT&CK framework.

Table 4. Evolution of the Evil Twin attack (2004–2025) in the context of MITRE ATT&CK.

Period	Variant/Platform	Data Theft	D./D.	MITRE Tactics	Cases
2004–2007	Classical ET + deauth; laptop + Wi-Fi card	Sniffing	V.L/V.L	TA0001, TA0009	—
2008–2013	KARMA/MANA + portal; Pineapple Mk4	Portal phish. + sniff.	L/L	TA0001, TA0006	Conf.
2014–2017	SSL strip/HSTS bypass; Pineapple + bettercap	MitM, cred. harv.	L–M/M	TA0006, TA0009, TA0005	RNC '16
2018–2019	Close-access ET, D2D; spec. HW/RPi	802.1X cred. theft	M–H/M	TA0001, TA0006, TA0008	OPCW, DOI
2020–2022	Ultra-short (<60 s), PMF bypass; RPi 4/Zero	Malware via portal	H/H	TA0001, TA0005, TA0011	Few publ.
2023–2025	Flash ET, AI portals; phone + Pineapple	AI phish., token theft	V.H/V.H	TA0001, TA0006, TA0009, TA0011	AU '24, BR '25

The evolution of the attack was accompanied by a systematic increase in the difficulty of detection and defense, as well as an expansion of the applicable MITRE ATT&CK tactics. As a result, Evil Twin has ceased to be merely a technical threat and has become a complex component of cyber operations, requiring multi-layered monitoring and response strategies.

5.2. Kill Chain of the Evil Twin Attack—A Conceptual Perspective

The Evil Twin attack implements a non-standard kill chain in which the initial access phase occurs at the radio layer, prior to any classical logical contact with the victim’s system.

The ET kill chain can be described as a physical/wireless/cyber hybrid, in which individual stages may proceed extremely rapidly or even in parallel.

- [A] **Reconnaissance** (radio reconnaissance)—identification of SSIDs, security types, client behavior, probe requests.
- [B] **Weaponization** (ET preparation)—a phase of the attack model (kill chain): preparation of the “attack payload”, i.e., development of tools, exploits, and fake portals. This is not yet an attack on the victim—it is the arming stage prior to logical contact. It is a configuration of the rogue AP, captive portal, and automation.
- [C] **Delivery** (vector delivery)—deauthentication, SSID spoofing, and forced connection.
- [D] **Initial Access** (TA0001)—the victim connects to the rogue AP.
- [E] **Credential Access** (TA0006)—credential phishing, and session token interception.
- [F] **Collection** (TA0009)—traffic sniffing, session hijacking, and data interception.
- [G] **Execution/Payload Delivery** (optional)—malware delivery via captive portal or MitM.
- [H] **Command and Control** (TA0011)—C2 communication initialization, beaconing.
- [I] **Lateral Movement** (TA0008)—lateral movement within the victim’s network.
- [J] **Impact** (TA0040)—further operational objectives of the campaign.

Table 5 provides a consolidated reference of all ten Kill Chain stages with their corresponding MITRE ATT&CK mappings and the layer at which each stage operates.

Table 5. Consolidated reference of Evil Twin Kill Chain stages.

Stage	Name	Layer	MITRE ATT&CK	Description
[A]	Reconnaissance	Radio	(pre-TA0001)	SSID scanning, probe request analysis, client behavior profiling
[B]	Weaponization	Radio	(pre-TA0001)	Rogue AP configuration, captive portal preparation, automation setup
[C]	Delivery	Radio	(pre-TA0001)	Deauthentication, SSID spoofing, forced client connection
[D]	Initial Access	Network	TA0001	Victim connects to rogue AP—critical inflection point
[E]	Credential Access	Application	TA0006	Phishing via captive portal, session token interception
[F]	Collection	Network	TA0009	Traffic sniffing, session hijacking, data interception
[G]	Execution/Payload Delivery	Application	TA0002	Malware delivery via portal or MitM (optional)
[H]	Command and Control	Network	TA0011	C2 channel initialization, beaconing
[I]	Lateral Movement	Network	TA0008	Movement within victim’s network using obtained credentials
[J]	Impact	Application	TA0040	Further campaign objectives, data exfiltration, disruption

Key observations indicate that Evil Twin shifts the beginning of the classical kill chain before the traditional Initial Access stage. The Reconnaissance and Delivery processes are executed at the radio layer. Modern variants significantly reduce the duration of the entire kill chain to merely a few seconds. A review of mitigation techniques for individual kill chain stages is presented in [41].

The MITRE ATT&CK ↔ Kill Chain diagram demonstrates that the Evil Twin attack cannot be unambiguously assigned to a single framework tactic. It constitutes a complex initialization vector that realizes multiple tactics in parallel, with its initial phases occurring beyond the classical Initial Access moment, at the radio and behavioral layers.

Table 6 presents a comprehensive mapping of the proposed mutation taxonomy of the Evil Twin attack onto the Kill Chain (stages [A]–[J]) and the MITRE ATT&CK framework.

Table 6. Comprehensive mapping: Evil Twin—Kill Chain—MITRE ATT&CK.

Period/Mutation	Dominant Char.	Kill Chain	MITRE Tactics	Notes
2004–07 Classical ET	AP spoof, sniffing	A→B→C→D→F	TA0001, TA0009	Simple, passive
2008–13 KARMA/MANA	SSID auto, captive portal	A→...→E→F	TA0001, TA0006, TA0009	Active credential theft
2014–17 SSL stripping	Active MitM, HTTPS bypass	A→...→F→G	+TA0005	Increased complexity
2018–19 Close-access	Short-lived, prepayload	A→...→G→H	+TA0011	ET as campaign initiator
2020–22 Ultra-short ET	PMF bypass, mobile D2D	A→...→I	+TA0008	Lateral movement
2023–25 Flash ET + AI	AI phishing, cred. stuffing	A→...→J	+TA0040	Full kill chain

The compiled data reveal several key evolutionary trends: a systematic extension of the kill chain (from stages [D]–[F] to the full range [A]–[J]), an increase in the number of MITRE

ATT&CK tactics realized in each successive attack generation, and the transformation of the Evil Twin role from a standalone vector to an offensive campaign initialization module.

5.3. Evil Twin as a Campaign Initialization Vector

In the existing literature, the Evil Twin attack is most commonly described as a standalone technique consisting of impersonating a legitimate access point. This paper proposes an alternative interpretation: the Evil Twin attack should not be treated as a discrete technique but rather as a specialized campaign initialization vector, analogous to email phishing, watering hole attacks (watering hole attacks are sophisticated cyberattacks in which adversaries compromise legitimate, niche websites frequently visited by a specific target group), or malicious USB drives.

Classifying the Evil Twin attack as a standalone technique leads to several significant oversimplifications. First, such an approach focuses exclusively on the access point impersonation mechanism, overlooking the preceding radio reconnaissance phases. Second, it reduces the analysis of the attack to a single stage within frameworks such as MITRE ATT&CK, disregarding the fact that contemporary Evil Twin implementations realize multiple tactics in parallel.

Analysis of the Evil Twin attack chain proposed in this paper (stages [A]–[J]) demonstrates that its operation commences prior to the classical Initial Access moment. The reconnaissance ([A]), preparation ([B]), and delivery ([C]) phases are executed at the radio layer and are not unambiguously mapped to MITRE ATT&CK tactics.

The moment the victim connects to the rogue access point ([D]) does not constitute the conclusion of the attack but rather its critical inflection point, enabling the activation of subsequent kill chain stages. Evil Twin serves as an initiating mechanism, analogously to other campaign initialization vectors.

A comparison of Evil Twin with classical initialization vectors reveals significant functional similarities. At the same time, Evil Twin is distinguished by several characteristics: it exploits user trust in the network infrastructure (rather than in message content), operates at the radio layer (which is less extensively monitored), and modern mutations are characterized by very short exposure times.

Adopting the perspective of Evil Twin as a campaign initialization vector necessitates extending classical MITRE ATT&CK-based models to incorporate the phases preceding Initial Access, as well as monitoring the radio layer as an integral part of threat detection systems.

5.4. Proposed Metric: Exposure Time T_e

The MITRE ATT&CK framework classifies adversary actions by answering the questions of *what was executed* and *for what purpose*. However, this model does not account for the temporal dimension, which in the case of attacks operating at the radio layer has critical operational significance.

In this paper, we introduce a new analytical metric—the Evil Twin attack exposure time—defined as the time interval during which the rogue access point remains active and generates detectable artifacts.

One of the significant limitations of the MITRE ATT&CK framework is the absence of a built-in mechanism enabling the formal description of the temporal dynamics of individual attack technique execution. The model relies on a binary classification in which a given technique is marked as either utilized or not utilized, without accounting for parameters such as duration. In the context of Evil Twin attacks, the absence of the temporal dimension becomes particularly problematic, as short-lived emissions exhibit significantly lower radio detectability despite achieving the same tactical objectives. Louca et al. [72]

additionally demonstrated the feasibility of conducting an Evil Twin attack using the 802.11v protocol, which further complicates temporal analysis.

Formalization of exposure time. To quantitatively capture the dynamics of the Evil Twin attack, we propose defining the exposure time as the total period during which the attack remains active and potentially detectable:

$$T_e = T_a + T_i + T_d \quad (1)$$

where T_e —attack exposure time [s]; T_a —attack preparation and initialization time on the attacker’s side [s] (from the emission of the first frame to the achievement of operational readiness); T_i —victim interaction time with the attack infrastructure [s]; and T_d —detectable radio artifact generation time [s].

Representative ranges enable the estimation of the total T_e in typical scenarios: T_a : 1–10 [s], T_i : 5–30 [s], T_d : 5–15 [s], yielding $T_e \approx 11$ –55 [s] for contemporary attacks.

Exposure time scale. To enable a comparable assessment of the profitability and detectability of Evil Twin attacks, we propose a scale based on exposure time (Table 7).

Table 7. Proposed exposure time scale categories (T_e).

T_e Range	Level	Typical Attack Character	Detectability	Profitability
0–10 s	Very short	Flash/fully automated (PMKID, rapid KARMA/MANA)	Very low	Very high
10–30 s	Short	Automated ET + deauth/probe response spoofing	Low	High
30–60 s	Medium	Contemporary automated ET (full beacon/probe/deauth emission)	Medium	Moderate
60–120 s	Long	Classical ET with captive portal or manual interaction	High	Low
>120 s	Very long	Persistent rogue AP (presence maintenance)	Very high	Very low

The scale illustrates the inverse relationship between exposure time and attack profitability: the shorter T_e , the greater the asymmetry in favor of the attacker.

Attack profitability model. To quantitatively assess the attractiveness of the attack from the adversary’s perspective, we propose a profitability function:

$$O(T_e) = \frac{1 - P_x(T_e)}{T_e}, \quad T_e > 0 \quad (2)$$

where $O(T_e)$ is the profitability of the Evil Twin attack as a function of exposure time, and $P_x(T_e)$ is the probability of attack detection by defensive mechanisms (WIDS/WIPS/SOC) as a function of time, $0 \leq P_x \leq 1$.

The denominator T_e reflects inverse proportionality: the shorter the exposure time, the greater the profitability. The numerator $(1 - P_x)$ represents the “safety” of the attack. The model demonstrates that each additional second of attack duration is “more expensive” than the previous one—reducing the attack from 20 [s] to 10 [s] doubles the profitability, whereas reducing it from 120 [s] to 110 [s] constitutes a marginal change.

Attack effectiveness model—the “compromise window”. As an extension of the profitability model, we introduce an attack effectiveness metric (E_{eff}), accounting for the dynamics of data exfiltration (The function $D(t)$ was intentionally employed rather than a simple product $D \times T$ —one cannot assume that data are exfiltrated at a constant rate. For example, at the onset of the attack, $D(t)$ may be low (observation phase), but when the user logs into their bank, $D(t)$ increases dramatically):

$$E_{\text{eff}} = P_{\text{succ}} \times \int_0^{T_e} D(t) dt \times (1 - P_x(T_e)) \quad (3)$$

where P_{succ} —probability of initial connection establishment by the victim ($0 \leq P_{\text{succ}} \leq 1$); $D(t)$ —data exfiltration intensity function over time t ; and $P_x(T_e)$ —probability of attack detection.

Table 8 presents typical modeling assumptions for P_{succ} .

Table 8. Assumptions for the estimated value of P_{succ} .

Scenario/Attack Mutation	P_{succ} Range	Ref. Value
Aggressive variants with KARMA/MANA + auto-connect	0.70–0.90	0.85
Flash mutation without deauthentication (strong signal + roaming)	0.10–0.40	0.35
Classical/hybrid with captive portal	0.20–0.50	0.25–0.35
Mass deauthentication (pre-PMF)	0.80–0.95	0.90
Enterprise environments WPA3-Enterprise + certificates	0.05–0.20	0.10

Sensitivity analysis with fixed $T_e = 20$ [s], $\int D(t) dt = 25$ units, $P_x = 0.15$ yields: $P_{\text{succ}} = 0.85 \Rightarrow E_{\text{eff}} \approx 18.1$; $P_{\text{succ}} = 0.35 \Rightarrow E_{\text{eff}} \approx 7.4$; $P_{\text{succ}} = 0.10 \Rightarrow E_{\text{eff}} \approx 2.1$ —variants exploiting auto-connect achieve up to 8–9× higher effectiveness.

It should be emphasized that the presented models (T_e , $O(T_e)$, E_{eff}) are conceptual–analytical in nature and constitute a proposal of theoretical frameworks for further validation. The principal limitation is the assumption of additivity of the T_e components—in real-world scenarios, the phases T_a , T_i , and T_d may partially overlap. Furthermore, the linear approximation of $P_x(T_e)$ is a simplification; the actual detectability function depends on the configuration of WIDS/WIPS systems, sensor density, and the network traffic profile. Empirical validation in controlled test environments, utilizing tools such as Wi-Fi Pineapple Mk VII or hostapd-mana, constitutes a key direction for future research.

5.5. Proposed Mutation Taxonomy of the Evil Twin Attack

In the scientific literature, the Evil Twin attack is most commonly classified as a variant or technique within broader categories. In this paper, we propose a new classification in which the Evil Twin attack is treated not as a simple “variant” or “technique”, but as an evolutionary mutation. This perspective enables us to capture changes in the attack’s function, its role within larger campaigns, and its relationship to other stages of the kill chain.

Traditional classifications focus mainly on tools and technical implementations. In contrast, the proposed mutation taxonomy emphasizes the adaptive process of the attack in response to changing technologies, defensive measures, and adversary objectives.

The taxonomy divides Evil Twin attacks into four main categories based on their dominant characteristics as summarized in Table 9.

Table 9. Operationalization of the Evil Twin mutation taxonomy.

Mutation	Period	T_e	Auto.	SE	Dominant Features	Examples
Classical	2005–2013	>120 s	Low	Low	Persistent AP, deauth, sniffing	BH 2005, Multipot
Hybrid	2014–2019	60–120 s	Med.	Med./High	Captive portal, D2D, phishing	Univ. Guayaquil
Flash	2020–2026	10–60 s	High	Low/Med.	PMF bypass, roaming, short emission	WatchGuard tests
Opportunistic-Hybrid	2026+	<10 s	V.High	High	AI-driven, IoT, adaptive	WatchGuard tests (Hypothetical)

The proposed taxonomy is primarily *feature based*, with the periods of dominant observability serving only as historical context for the prevalence of each mutation type. The exposure time intervals (T_e) should be treated as heuristic analytical boundaries derived from recurring temporal patterns observed in historical incident reports, rather than as fixed or universally applicable numerical constants. The *Opportunistic-Hybrid* category is prospective and represents the anticipated future direction of the threat’s evolution.

This taxonomy provides a structured framework for classifying current and future Evil Twin variants, supporting a more precise analysis of their development over time.

5.6. Mapping the Evil Twin Attack Beyond MITRE ATT&CK

The MITRE ATT&CK framework commences at the Initial Access stage (TA0001). However, the Evil Twin attack executes actions that begin at the radio layer and may be exploited to acquire information even before the classical TA0001. This layer is not

accounted for in the classical MITRE ATT&CK model, which creates a gap in the context of comprehensive classification of wireless attack vectors.

The radio layer as an attack domain.

- **Reconnaissance [A]:** interception of information on available APs, SSIDs, channels—a phase not covered by ATT&CK, pertaining exclusively to the radio layer.
- **Weaponization [B]:** configuration of the rogue AP—preparation of conditions for obtaining Initial Access.
- **Delivery [C]:** access point impersonation and forcing the victim’s connection—a technique not described in ATT&CK in the radio context.

The problem of incomplete coverage of attack domains within MITRE ATT&CK is not unique to the radio layer. The MITRE organization has already developed framework extensions for specific environments: ATT&CK for ICS (Industrial Control Systems) encompasses tactics and techniques dedicated to industrial control systems, including manipulation of physical processes (Impact—T0831 Manipulation of Control) and techniques specific to protocols such as Modbus and OPC UA. Analogously, ATT&CK for Mobile extends the model with techniques characteristic of mobile devices, such as T1437 (Standard Application Layer Protocol) and T1430 (Location Tracking).

Both extensions confirm the validity of creating specialized domains when the classical Enterprise model does not cover key attack vectors. In the case of the Wi-Fi radio layer, the situation is analogous: phases [A]–[C] of the proposed Kill Chain (Reconnaissance, Weaponization, and Delivery at the radio layer) have no counterparts in any existing MITRE extensions. ATT&CK for Mobile does include technique T1465 (Rogue Wi-Fi Access Points); however, its description is limited to a conceptual level and does not encompass a detailed mutation taxonomy or a temporal dimension.

The MITRE ATT&CK framework does not encompass adversary actions at the radio layer as a separate domain, which constitutes a significant gap in the classification of Wi-Fi attacks. The Evil Twin attack commences before the classical Initial Access and involves actions in phases [A]–[C] executed at the radio layer. Vanhoef [73] demonstrated that vulnerabilities at the Wi-Fi frame aggregation and fragmentation level (FragAttacks) extend beyond the MITRE ATT&CK classification. Existing extensions (ICS and Mobile) confirm the feasibility and value of creating specialized domains. We propose considering an analogous extension, “ATT&CK for Wireless”, encompassing: radio reconnaissance (SSID scanning, probe request analysis), radio layer weaponization (rogue AP configuration, beacon spoofing), and radio layer delivery (forced connection through deauthentication or roaming manipulation). Such an extension would enable more comprehensive modeling of Wi-Fi attacks and their role in APT campaigns.

6. Hypotheses on the Evolution of the Evil Twin Attack

The observed evolution of Evil Twin attacks suggests a trend toward increased automation, reduced exposure time (T_e), and tighter integration with heterogeneous wireless environments. However, the following statements should be interpreted as *research hypotheses*, derived from existing empirical and experimental findings, rather than confirmed future outcomes. They are intended to guide further investigation rather than provide predictive certainty.

6.1. Hypothesis 1—Toward Near-Zero Exposure Attacks

Hypothesis 1. *The continued development of Evil Twin attack implementations may lead to ultra-short exposure-time scenarios, in which attacker presence is minimized through automation and rapid deployment mechanisms.*

Recent studies on rogue access point detection and wireless attack automation demonstrate a progressive reduction in attacker interaction time due to pre-configured toolchains and scripted deployment environments [26,28,29,33]. Furthermore, advancements in automated penetration testing frameworks and mobile attack platforms indicate that deployment latency can be significantly reduced in controlled conditions [9,47].

In this context, the concept of near-zero exposure should be interpreted as an extrapolation of observed trends in attack automation rather than an empirically validated state.

6.2. Hypothesis 2—Artificial Intelligence-Augmented Attack Automation

Hypothesis 2. *Future Evil Twin attack variants may incorporate machine learning techniques to enhance target selection, adapt SSID behavior, and optimize attack timing.*

While there is currently limited direct evidence of fully autonomous AI-driven Evil Twin deployments, research in AI-based intrusion systems and adaptive wireless attack detection demonstrates the feasibility of learning-based adaptation in wireless environments [34,69,74]. Additionally, AI-assisted offensive security tooling is increasingly discussed in the context of automated penetration testing and adversarial adaptation.

Therefore, AI integration is treated here as an emerging capability extrapolated from defensive and dual-use security research.

6.3. Hypothesis 3—Expansion Through IoT-Enabled Attack Surfaces

Hypothesis 3. *The increasing prevalence of IoT devices may expand the potential attack surface for Evil Twin-style attacks by enabling additional propagation vectors and relay points.*

Existing literature on IoT security highlights the limited authentication and update mechanisms in many deployed devices, which can be leveraged in wireless attack chains [35,74]. Although direct IoT-mediated Evil Twin implementations remain underexplored, the combination of weakly secured IoT endpoints and wireless bridging mechanisms may facilitate more distributed attack topologies.

6.4. Hypothesis 4—5G-Enhanced Attack Dynamics

Hypothesis 4. *The adoption of 5G networks may influence Evil Twin attack dynamics by increasing network density, reducing latency, and enabling faster data exfiltration once initial compromise occurs.*

Research on modern wireless security protocols (WPA3, 802.11 enhancements) and high-speed mobile environments indicates that increased connectivity density may amplify the impact of proximity-based attacks [4,67,68]. However, there is currently no direct empirical evidence linking 5G deployment to Evil Twin effectiveness; thus, this hypothesis represents a structural extrapolation of known wireless risk factors.

Summary. All hypotheses presented above are derived from observed trends in wireless security research, including attack automation, protocol evolution, and increasing network heterogeneity. They should be interpreted as directions for future empirical validation rather than confirmed projections.

7. Limitations

This study is subject to several limitations inherent to the nature of a narrative and conceptual review. First, the analysis relies heavily on *grey literature*—including industry threat intelligence, security advisories, and conference presentations. While this reliance is

unavoidable when investigating highly dynamic and evolving cyber threats that lack uniform reporting standards, it necessitates a cautious interpretation of the synthesized trends.

Second, the proposed mutation taxonomy and the frameworks derived from the exposure time metric T_e are primarily conceptual and theoretical in nature. Consequently, they have not yet been subjected to empirical validation in controlled laboratory settings or within diverse, large-scale production network environments. These models serve as an analytical foundation rather than an experimentally verified solution.

Third, the proposed ten-stage Kill Chain model represents an effort to explicitly formalize the phases preceding *Initial Access* at the radio layer—stages that are currently only partially addressed or abstracted within existing industry frameworks.

The authors acknowledge these methodological constraints and present the proposed frameworks as initial contributions intended to stimulate further scholarly discourse and facilitate future empirical assessment.

8. Summary and Conclusions

This study provides a comprehensive narrative and conceptual review of the evolution of the Evil Twin attack in Wi-Fi networks throughout the 2005–2026 period. Since its initial public demonstration in 2005, this threat has undergone a profound transformation—evolving from rudimentary rogue access point impersonation into highly adaptive, ephemeral, and hybrid variants that integrate social engineering, process automation, and emerging technologies.

Through a chronological analysis and data triangulation across academic, governmental, and industry sources, this research identifies a systematic reduction in the attack's exposure time, a trend toward increasing technical hybridization, and persistent underreporting or misclassification within mainstream security assessments. The primary contributions of this work are as follows:

- A novel mutation taxonomy for Evil Twin attacks (comprising Classical, Hybrid, Flash, and prospective Opportunistic-Hybrid variants);
- A specialized ten-stage Kill Chain model tailored to wireless-layer threats;
- The exposure time metric T_e , supported by associated analytical models;
- A conceptual mapping that augments the MITRE ATT&CK framework with radio-layer specificities.

This study underscores the “invisible enemy” nature of Evil Twin attacks, characterized by high-fidelity mimicry, low detectability, and inherent challenges in unambiguous attribution. Despite significant advancements in cryptographic and architectural defenses (such as WPA3, Protected Management Frames, and WIPS), the attack vector remains highly viable, particularly in high-turnover public and enterprise environments.

The methodological and conceptual constraints of this review are addressed in Section 7. We propose the frameworks presented herein as analytical foundations designed to stimulate further scholarly discourse, facilitate empirical validation, and support the development of detection mechanisms better adapted to flash and opportunistic attack variants.

Future research should prioritize the operational validation of the proposed taxonomy and T_e metric, the extension of these frameworks into 5G and IoT ecosystems, and advocacy for enhanced incident classification standards that more accurately categorize Wi-Fi spoofing phenomena.

In conclusion, the Evil Twin attack is not diminishing; rather, it is mutating in direct response to defensive advancements. Its persistence reinforces the necessity for the continuous evolution of both technical countermeasures and conceptual security models within the wireless domain.

Author Contributions: Conceptualization, P.A.; methodology, P.A.; investigation, P.A.; formal analysis, P.Z.; resources, P.A.; data curation, P.A.; writing—original draft preparation, P.A. and P.Z.; writing—review and editing, P.A. and P.Z.; supervision, P.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Polish Ministry of Science and Higher Education under Grant 0313/SBAD/1315.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new datasets were created or analyzed during the current study. All information discussed in this review is based on publicly available sources, technical reports, scientific publications, conference materials, and governmental documentation cited in the References section.

Acknowledgments: During the preparation of this manuscript, the authors used Claude (Anthropic 2025) to support language editing and improve the clarity, style, and readability of the text. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Beetle; Potter, B. Rogue Squadron: Evil Twins, 802.11intel, Radical RADIUS, and Wireless Weaponry for Windows. In Proceedings of the Black Hat, Las Vegas, NV, USA, 27–28 July 2005. Available online: <https://blackhat.com/presentations/bh-usa-05/bh-us-05-beetle-update.pdf> (accessed on 6 May 2026).
2. Gopinath, K.N. Multipot: A More Potent Variant of Evil Twin. In Proceedings of the DEF CON 15, Las Vegas, NV, USA, 3–5 August 2007. Available online: <https://www.youtube.com/watch?v=1dbj50CiOPk> (accessed on 6 May 2026).
3. Gopinath, K.N. Multipot: A More Potent Variant of Evil Twin—Whitepaper. 2007. Available online: <https://media.defcon.org/DEF%20CON%202015/DEF%20CON%202015%20presentations/DEF%20CON%202015%20-%20gopinath-WP.pdf> (accessed on 6 May 2026).
4. Chatzisofroniou, G.; Kotzanikolaou, P. Exploiting WiFi Usability Features for Association Attacks in IEEE 802.11: Attack Analysis and Mitigation Controls. *J. Comput. Secur.* **2022**, *30*, 357–380. [CrossRef]
5. Black Hat USA 2011 Archives. 2011. Available online: <https://blackhat.com/html/bh-us-11/bh-us-11-archives.html> (accessed on 6 May 2026).
6. d’Otrepe de Bouvette, T. Aircrack-ng, 2006. Official Project Website. Available online: <https://www.aircrack-ng.org/> (accessed on 6 May 2026).
7. Wakhloo, A.; Ghergulescu, I.; Moldovan, A.N. Investigation of WiFi Security Auditing Tools for Evil Twin Attacks and Detection. In *Proceedings of the Hybrid Intelligent Systems (HIS 2023)*; LNNS; Springer: Berlin/Heidelberg, Germany, 2024; Volume 1060. [CrossRef]
8. Briones, J.M.; Coronel, M.A.; Chavez-Burbano, P. Case of Study: Identity Theft in a University WLAN, Evil Twin and Cloned Authentication Web Interface. *Int. J. Wirel. Hoc Commun.* **2013**. [CrossRef]
9. TrustedSec. Social Engineer Toolkit. 2026. GitHub Repository. Available online: <https://github.com/trustedsec/social-engineer-toolkit> (accessed on 6 May 2026).
10. Shinal, J. Fake Wi-Fi Hotspots Lure RNC Attendees. USA Today. 2016. Available online: <https://eu.usatoday.com/story/tech/columnist/shinal/2016/07/21/vote-hillary-other-fake-wi-fi-hotspots-lure-rnc-attendees/87415654/> (accessed on 6 May 2026).
11. Avast. Republican National Convention Delegates Unknowingly Use Fake Wi-Fi Networks, 2016. Avast Security Experiment at the 2016 RNC. Available online: <https://blog.avast.com/republican-national-convention-delegates-unknowingly-use-fake-wi-fi-networks> (accessed on 6 May 2026).
12. Government of the United Kingdom. Minister for Europe Statement: Attempted Hacking of the OPCW by Russian Military Intelligence. 2018. Available online: <https://www.gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence> (accessed on 6 May 2026).
13. OPCW. EC-89 United States National Statement. 2018. Available online: <https://www.opcw.org/sites/default/files/documents/2018/10/EC-89%20US%20NATIONAL%20STATEMENT%20-%20%28AS%20DELIVERED%29.pdf> (accessed on 6 May 2026).
14. BBC News. Russia Cyber-Plots: US, UK and Netherlands Allege Attacks. 2018. Available online: <https://www.bbc.com/news/world-europe-45747472> (accessed on 6 May 2026).

15. Schepers, D.; Ranganathan, A.; Vanhoef, M. On the Robustness of Wi-Fi Deauthentication Countermeasures. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22)*; ACM: New York, NY, USA, 2022; pp. 245–256. [\[CrossRef\]](#)
16. Lounis, K.; Ding, S.H.H.; Zulkernine, M. Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3. In *Proceedings of the Foundations and Practice of Security (FPS 2021)*; LNCS; Springer: Berlin/Heidelberg, Germany, 2022; Volume 13291, pp. 235–251. [\[CrossRef\]](#)
17. U.S. Department of the Interior Office of Inspector General. Evil Twins, Eavesdropping, and Password Cracking: How OIG Successfully Attacked the U.S. Department of the Interior's Wireless Networks. 2020. Available online: https://www.doioig.gov/sites/default/files/2021-migration/FinalAudit_WirelessNetworkSecurity_Public.pdf (accessed on 6 May 2026).
18. WatchGuard Technologies. Trusted Wireless Environment. 2026. Available online: <https://www.watchguard.com/wgrd-solutions/security-trends/trusted-wireless-environment> (accessed on 6 May 2026).
19. Jain, V.; Laxmi, V.; Gaur, M.S.; Mosbah, M. ETGuard: Detecting D2D Attacks Using Wireless Evil Twins. *arXiv* **2019**, arXiv:1903.05843.
20. WatchGuard Technologies. Six Wi-Fi Attacks Impacting Hotel Guests. 2026. Available online: <https://web.archive.org/web/20240223011322/https://www.watchguard.com/wgrd-news/blog/six-wi-fi-attacks-impacting-hotel-guests> (accessed on 21 July 2026).
21. Australian Federal Police. Man Charged Over Creation of Evil Twin Free Wi-Fi Networks to Access Personal Data. 2024. Available online: <https://www.afp.gov.au/news-centre/media-release/man-charged-over-creation-evil-twin-free-wifi-networks-access-personal> (accessed on 6 May 2026).
22. Security Affairs. Evil Twin WiFi Attack on Plane. 2024. Available online: <https://securityaffairs.com/165108/cyber-crime/evil-twin-wifi-attack-plane.html> (accessed on 6 May 2026).
23. TechTudo. Depois que Conheci Esse Golpe, Nunca Mais Usei Redes de Wi-Fi Públicas. 2025. Available online: <https://www.techtudo.com.br/noticias/2025/07/depois-que-conheci-esse-golpe-nunca-mais-usei-redes-de-wi-fi-publicas-edsoftwares.ghtml> (accessed on 6 May 2026). (In Portuguese)
24. Olhar Digital. Cuidado com o Evil Twin! Conheça o Golpe do Wi-Fi Falso e Veja Como se Prevenir. 2025. Available online: <https://olhardigital.com.br/2025/07/30/seguranca/cuidado-com-o-evil-twin-conheca-o-golpe-do-wi-fi-falso-e-veja-como-se-prevenir/> (accessed on 6 May 2026). (In Portuguese)
25. Canaltech. Agências dos EUA e Europa Recomendam Desligar Wi-Fi ao Sair de Casa; Entenda. 2025. Available online: <https://canaltech.com.br/seguranca/agencias-dos-eua-e-europa-recomendam-desligar-wi-fi-ao-sair-de-casa-entenda/> (accessed on 6 May 2026). (In Portuguese)
26. Banakh, R.; Nyemkova, E.; Justice, C.; Piskozub, A.; Lakh, Y. Data Mining Approach for Evil Twin Attack Identification in Wi-Fi Networks. *Data* **2024**, *9*, 119. [\[CrossRef\]](#)
27. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [\[CrossRef\]](#)
28. Jana, S.; Kasera, S.K. On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom)*; ACM: New York, NY, USA, 2008; pp. 104–115. [\[CrossRef\]](#)
29. Nakhila, O.; Zou, C. User-Side Wi-Fi Evil Twin Attack Detection Using Random Wireless Channel Monitoring. In *Proceedings of the 2016 IEEE Military Communications Conference (MILCOM)*; IEEE: Piscataway, NJ, USA, 2016; pp. 1243–1248. [\[CrossRef\]](#)
30. Yang, C.; Song, Y.; Gu, G. Active User-Side Evil Twin Access Point Detection Using Statistical Techniques. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1638–1651. [\[CrossRef\]](#)
31. Cheng, Y.; Liao, X.; Wu, B. Who is Peeping at Your Passwords at Starbucks?—To Catch an Evil Twin Access Point. In *Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*; IEEE: Piscataway, NJ, USA, 2010; pp. 323–332. [\[CrossRef\]](#)
32. Lanze, F.; Panchenko, A.; Ponce-Alcaide, I.; Engel, T. Undesired Relatives: Protection Mechanisms Against the Evil Twin Attack in IEEE 802.11. In *Proceedings of the 10th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet)*; ACM: New York, NY, USA, 2014; pp. 87–98. [\[CrossRef\]](#)
33. Kitisriworapan, S.; Jansang, A.; Phonphoem, A. Client-Side Rogue Access-Point Detection Using a Simple Walking Strategy and Round-Trip Time Analysis. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 252. [\[CrossRef\]](#)
34. Kumar, Y.; Kumar, V. A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications. *Wirel. Pers. Commun.* **2023**, *133*, 395–452. [\[CrossRef\]](#)
35. Nazir, R.; Laghari, A.A.; Kumar, K.; David, S.; Ali, M. Survey on Wireless Network Security. *Arch. Comput. Methods Eng.* **2022**, *29*, 1591–1610. [\[CrossRef\]](#)

36. Organisation for the Prohibition of Chemical Weapons. Summary of the Report on Activities Carried Out in Support of a Request for Technical Assistance by the United Kingdom. Technical Report S/1612/2018, OPCW, 2018. Technical Report Confirming Nerve Agent Identification. Available online: https://www.opcw.org/sites/default/files/documents/S_series/2018/en/s-1612-2018_e__1_.pdf (accessed on 6 May 2026).
37. Yan, D.; Yan, Y.; Yang, P.; Song, W.Z.; Li, X.Y.; Liu, P. Real-Time Identification of Rogue WiFi Connections in the Wild. *IEEE Internet Things J.* **2022**, *10*, 6042–6058. [CrossRef]
38. Thankappan, M.; Rifa-Pous, H.; Garrigues, C. A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks. *IEEE Access* **2024**, *12*, 23096–23121. [CrossRef]
39. Alotaibi, B.; Elleithy, K. Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions. *Wirel. Pers. Commun.* **2016**, *90*, 1261–1290. [CrossRef]
40. Shrivastava, P.; Jamal, M.S.; Kataoka, K. EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 89–102. [CrossRef]
41. Muthalagu, R.; Sanjay, S. Evil Twin Attack Mitigation Techniques in 802.11 Networks. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2021**, *12*, 38–41. [CrossRef]
42. Verizon. Data Breach Investigations Report (DBIR). 2025. Available online: <https://www.verizon.com/business/resources/reports/dbir/> (accessed on 15 January 2026).
43. Verizon. 2025 Data Breach Investigations Report. Technical Report, Verizon Business. 2025. Available online: <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf> (accessed on 15 January 2026).
44. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2025*; Technical Report; ENISA (Publications Office of the European Union): Luxembourg, 2025; ISBN 978-92-9204-723-8. Available online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025> (accessed on 15 January 2026).
45. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2025—Booklet*; Technical Report; Catalogue no. TP-01-25-025-EN-N; ENISA (Publications Office of the European Union): Luxembourg, 2025; ISBN 978-92-9204-721-4. [CrossRef]
46. Advanced Wi-Fi Pentesting. Black Hat USA 2015 Training, 2015. Available online: <https://blackhat.com/us-15/training/advanced-wi-fi-pentesting.html> (accessed on 6 May 2026).
47. Advanced Wi-Fi Attack and Defense for Hackers and Pentesters. Black Hat USA 2016 Training. 2016. Available online: <https://blackhat.com/us-16/training/advanced-wi-fi-attack-and-defense-for-hackers-and-pentesters.html> (accessed on 6 May 2026).
48. Government of the United Kingdom. Novichok Nerve Agent Use in Salisbury: UK Government Response, March to April 2018; Official UK Government Response: London, UK, 2018. Available online: <https://www.gov.uk/government/news/novichok-nerve-agent-use-in-salisbury-uk-government-response> (accessed on 6 May 2026).
49. Organisation for the Prohibition of Chemical Weapons. *Report of the OPCW Fact-Finding Mission in Syria Regarding the Incident of Alleged Use of Chemical Weapons in Douma*; Technical Report S/1731/2019; OPCW: The Hague, The Netherlands, 2019. Final Report. Available online: [https://www.opcw.org/sites/default/files/documents/2019/03/s-1731-2019\(e\).pdf](https://www.opcw.org/sites/default/files/documents/2019/03/s-1731-2019(e).pdf) (accessed on 6 May 2026).
50. Federal Bureau of Investigation. Aleksei Sergeyevich Morenets. 2026. Available online: <https://www.fbi.gov/wanted/cyber/aleksei-sergeyevich-morenets> (accessed on 6 May 2026).
51. Federal Bureau of Investigation. Evgenii Mikhaylovich Serebriakov. 2026. Available online: <https://www.fbi.gov/wanted/cyber/evgenii-mikhaylovich-serebriakov> (accessed on 6 May 2026).
52. Federal Bureau of Investigation. Oleg Mikhaylovich Sotnikov. 2026. Available online: <https://www.fbi.gov/wanted/cyber/oleg-mikhaylovich-sotnikov> (accessed on 6 May 2026).
53. Federal Bureau of Investigation. Alexey Valerevich Minin. 2026. Available online: <https://www.fbi.gov/wanted/cyber/alexey-valerevich-minin> (accessed on 6 May 2026).
54. Lowenthal, M.M. *Intelligence: From Secrets to Policy*, 8th ed.; CQ Press: Washington, DC, USA, 2020; ISBN 978-1544369174. Available online: <https://books.google.com/books/about/Intelligence.html?id=Fk6YDwAAQBAJ> (accessed on 6 May 2026).
55. CrowdStrike Intelligence. *FANCY BEAR (APT28): A Window into Russia's Cyber Espionage Operations*; Technical Report; Threat Intelligence Report; CrowdStrike: Austin, TX, USA, 2016. Available online: <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/> (accessed on 6 May 2026).
56. da Silva, L.M.; Andregghetti, V.M.; Romero, R.A.F.; Branco, K.R.L.J.C. Analysis and Identification of Evil Twin Attack through Data Science Techniques Using AWID3 Dataset. In *Proceedings of the 6th International Conference on Machine Learning and Machine Intelligence (MLMI 2023)*; ACM: New York, NY, USA, 2023; pp. 168–175. [CrossRef]
57. Messer, P. Rogue Access Points. 2026. Available online: <https://www.professormesser.com/security-plus/sy0-501/rogue-access-points/> (accessed on 6 May 2026).
58. Miercom. Miercom. 2026. Available online: <https://miercom.com/> (accessed on 6 May 2026).
59. Han, H.; Sheng, B.; Tan, C.C.; Li, Q.; Lu, S. A Timing-Based Scheme for Rogue AP Detection. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *22*, 1912–1925. [CrossRef]

60. Cisco Systems. Cisco Adaptive Wireless Intrusion Prevention System. 2026. Available online: <https://www.cisco.com/c/en/us/products/wireless/adaptive-wireless-ips-software/index.html> (accessed on 7 May 2026).
61. Cisco Systems. Cisco CleanAir Technology. 2026. Available online: <https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/112139-cleanair-ugn-guide-00.html> (accessed on 7 May 2026).
62. Monica, D.; Ribeiro, C. WiFiHop—Mitigating the Evil Twin Attack through Multi-hop Detection. In *Proceedings of the 16th European Symposium on Research in Computer Security (ESORICS 2011)*; LNCS; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6879, pp. 21–39. [\[CrossRef\]](#)
63. Kuo, E.C.; Chang, M.S.; Kao, D.Y. User-Side Evil Twin Attack Detection Using Time-Delay Statistics of TCP Connection Termination. In *Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT)*; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6. [\[CrossRef\]](#)
64. Hewlett Packard Enterprise. Aruba RFProtect Wireless Intrusion Protection. 2026. Available online: <https://www.hpe.com/psnow/doc/c05272726> (accessed on 21 July 2026).
65. Cisco Systems. Cisco Meraki Air Marshal. 2026. Available online: https://documentation.meraki.com/MR/Monitoring_and_Reporting/Air_Marshal (accessed on 7 May 2026).
66. Vanhoef, M.; Ronen, E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP)*, Virtual, 8–20 May 2020; pp. 517–533. [\[CrossRef\]](#)
67. Halbouni, A.; Ong, L.Y.; Leow, M.C. Wireless Security Protocols WPA3: A Systematic Literature Review. *IEEE Access* **2023**, *11*, 112438–112450. [\[CrossRef\]](#)
68. Chatzoglou, E.; Kampourakis, G.; Kolias, C. How is Your Wi-Fi Connection Today? DoS Attacks on WPA3-SAE. *J. Inf. Secur. Appl.* **2022**, *64*, 103058. [\[CrossRef\]](#)
69. Kamble, A.; Kshirsagar, D. Feature Selection in Wireless Intrusion Detection System for Evil Twin Attack Detection. In *Proceedings of the 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6. [\[CrossRef\]](#)
70. Thankappan, M.; Rifa-Pous, H.; Garrigues, C. A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. *Int. J. Inf. Secur.* **2024**, *23*, 3457–3479. [\[CrossRef\]](#)
71. Feng, X.; Li, Q.; Sun, K.; Yang, Y.; Xu, K. Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 22–25 May 2023; pp. 694–709. [\[CrossRef\]](#)
72. Louca, C.; Peratikou, A.; Stavrou, S. A Novel Evil Twin MiTM Attack through 802.11v Protocol Exploitation. *Comput. Secur.* **2023**, *130*, 103261. [\[CrossRef\]](#)
73. Vanhoef, M. Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation. In *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*, Virtual, 11–13 August 2021; pp. 161–178. Available online: <https://www.usenix.org/conference/usenixsecurity21/presentation/vanhoef> (accessed on 6 May 2026).
74. Nivaashini, M.; Thangaraj, P. Computational Intelligence Techniques for Automatic Detection of Wi-Fi Attacks in Wireless IoT Networks. *Wirel. Netw.* **2021**, *27*, 2761–2784. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.