Review

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

Piotr Augustyniak and Piotr Leszek Zwierzykowski *

Posted Date: 4 June 2026

doi: 10.20944/preprints202606.0325.v1

Keywords: Evil Twin; rogue access point; Wi-Fi security; wireless networks; WIPS; WPA3; trusted wireless environment; Man-in-the-Middle; cybersecurity

 doi:10.20944/preprints202606.0325.v1

Review

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

Piotr Augustyniak and Piotr Leszek Zwierzykowski *

Institute of Communication and Computer Networks, Poznań University of Technology, 61-131 Poznań, Poland
* 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 creating an unauthorized access point (*rogue access point*) with an identical SSID and configuration to a legitimate wireless network access point, for the purpose of intercepting network traffic or user credentials. It should be emphasized that the term Evil Twin is sometimes erroneously equated in the literature with the broader category of Rogue Access Point or Wi-Fi Honeypot [1], whereas in the strict sense, Evil Twin constitutes a specific subtype of these threats, characterized by the deliberate impersonation of a particular, existing network.

The first public demonstrations of the Evil Twin attack took place in 2004–2005. In its early phase, the attack required only a single device with a Wi-Fi card operating in monitor mode, appropriate software (e.g., AirSnort), and physical presence within range of the target network. Within a few minutes, it was possible to intercept network traffic, including passwords, session data, and login credentials.

Over the course of two decades, the Evil Twin attack has undergone a significant evolution – from a simple rogue access point in public venues, through advanced variants incorporating automation (KARMA, MANA) and social engineering integration, to contemporary, highly automated campaigns leveraging mobile technologies, artificial intelligence, and IoT infrastructure [2,3]. At present, the Evil

 doi:10.20944/preprints202606.0325.v1

Twin no longer constitutes an isolated incident but rather functions as a complex initialization vector for offensive campaigns, encompassing multiple tactics within the MITRE ATT&CK framework.

This paper provides a comprehensive review of the Evil Twin attack evolution over the period 2005–2026. The objectives of this article are: (1) a systematic chronological analysis of key incidents, demonstrations, and publications; (2) the development of an original taxonomy of attack mutations; (3) the introduction of an exposure time metric T_e as a quantitative evolutionary parameter; (4) mapping the attack onto the MITRE ATT&CK framework and an original Kill Chain model; and (5) the identification of gaps in existing classification systems and incident reporting frameworks.

The scope of this work is limited to the analysis of Evil Twin attack evolution in the strict sense, i.e., impersonation of a legitimate access point using an identical SSID. Related but distinct techniques have been intentionally excluded: KARMA (2008) and MANA (2013) are tools that automate the Evil Twin, but their detailed description falls outside the conceptual scope of this paper; the KRACK attack (Key Reinstallation Attack, 2017) [4] is a separate cryptographic threat, unrelated to access point impersonation. These techniques are mentioned in the context of evolution but do not constitute a subject of separate analysis.

Table 1 presents a chronological overview of key events related to the Evil Twin attack, and Figure 1 provides their graphical representation on a timeline. 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; *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.

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

 doi:10.20944/preprints202606.0325.v1

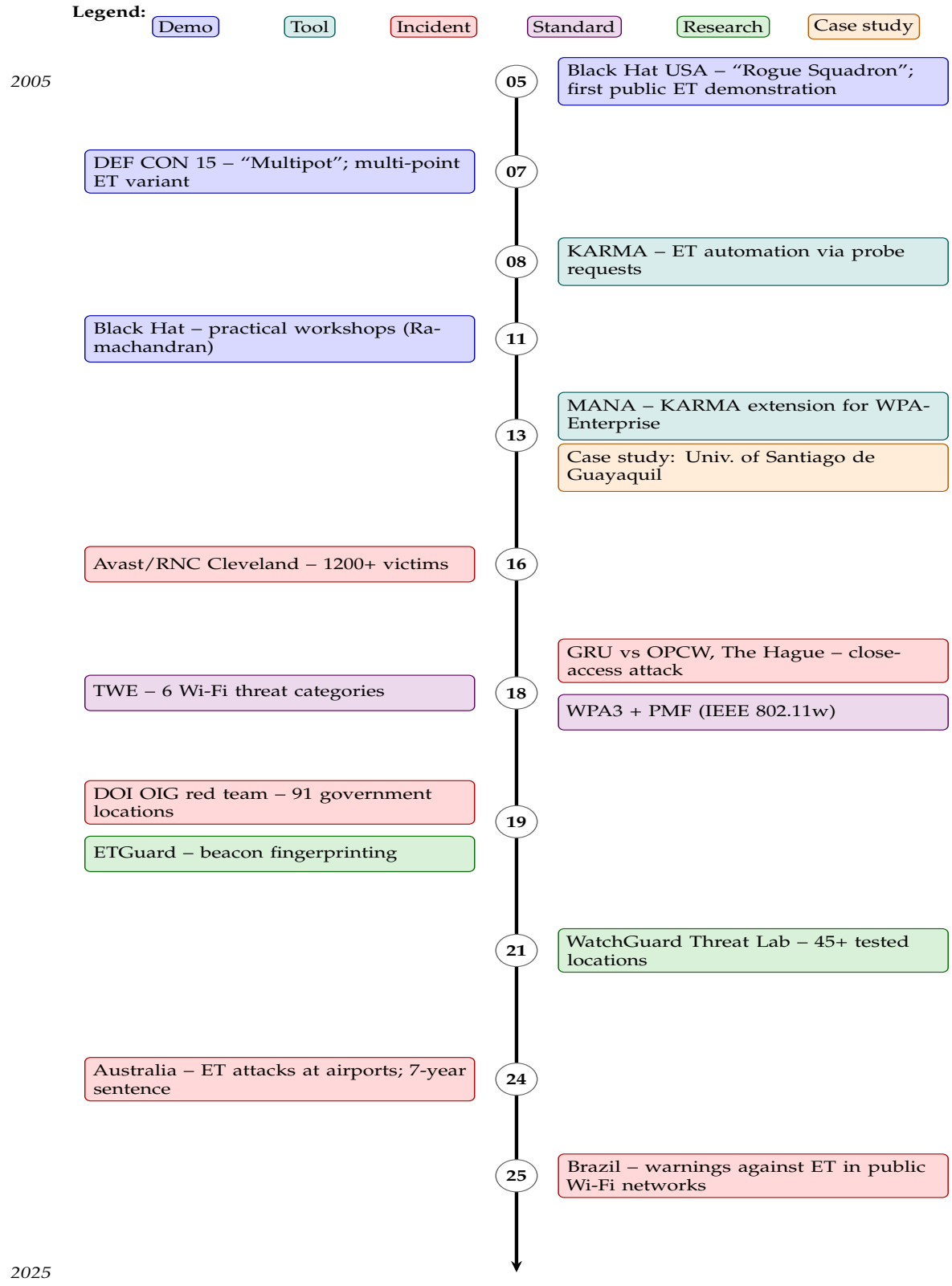

Figure 1. Evolution of the Evil Twin attack – timeline of key events (2005–2025).

2. Methodology

This paper takes the form of a narrative review, which is justified by the specificity of the subject under study: Evil Twin attacks are documented across heterogeneous sources (scientific literature, government reports, industry documentation, conference materials, media coverage), a significant portion of which is not indexed in standard bibliographic databases. A systematic review following the

 doi:10.20944/preprints202606.0325.v1

PRISMA methodology would be inadequate given the dominance of grey literature and the absence of standardized protocols for Evil Twin incident reporting. The adopted approach combines elements of qualitative and quantitative analysis in order to reconstruct the evolution of the attack and develop original conclusions regarding its mutations. The methodology was designed to ensure reliability, reproducibility, and objectivity, while accounting for limitations arising from the underestimation of incidents in available sources. The research process was divided into three main stages: data collection, analysis, and synthesis incorporating original contributions.

2.1. 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 (e.g., *Case of Study: Identity Theft in a University WLAN* from 2013 and *ETGuard: Detecting D2D Attacks using Wireless Evil Twins* from 2019).
- Security institution and government reports: analysis of official documents, including the Office of Inspector General (OIG) report of the U.S. Department of the Interior from 2020, OPCW statements from 2018, WatchGuard Threat Lab research (2021–2023), and CISA and ENISA reports from 2025–2026.
- Recent industry data from 2025–2026: CVE vulnerability reports[1], vendor analyses, and data from NIST (SP 800-97), Verizon DBIR (2023–2026), and IBM X-Force Threat Intelligence.

Source selection was based on the criteria of: relevance (direct reference to evil twin or rogue AP), recency (priority given to data from the last decade), and diversity (a mix of academic, government, and industry sources). The databases searched included IEEE Xplore, ACM Digital Library, Springer Link, Google Scholar, and institutional repositories (NIST, ENISA, CISA), using the following search phrases: “evil twin”, “rogue access point”, “Wi-Fi spoofing”, “wireless MitM”. In total, over 100 sources were analyzed, encompassing scientific publications, industry reports, technical documentation, and conference materials. A simplified source selection diagram, adapted from the PRISMA methodology for the purposes of this narrative review, is presented in Figure 2.

[1] E.g., CVE-2018-6402: the possibility of forcing Ecobee 4 devices to deauthorize and connect to an unencrypted Wi-Fi network with the same SSID, even if the device settings specify WPA2 encryption, provided the competing network has a stronger signal.

 doi:10.20944/preprints202606.0325.v1

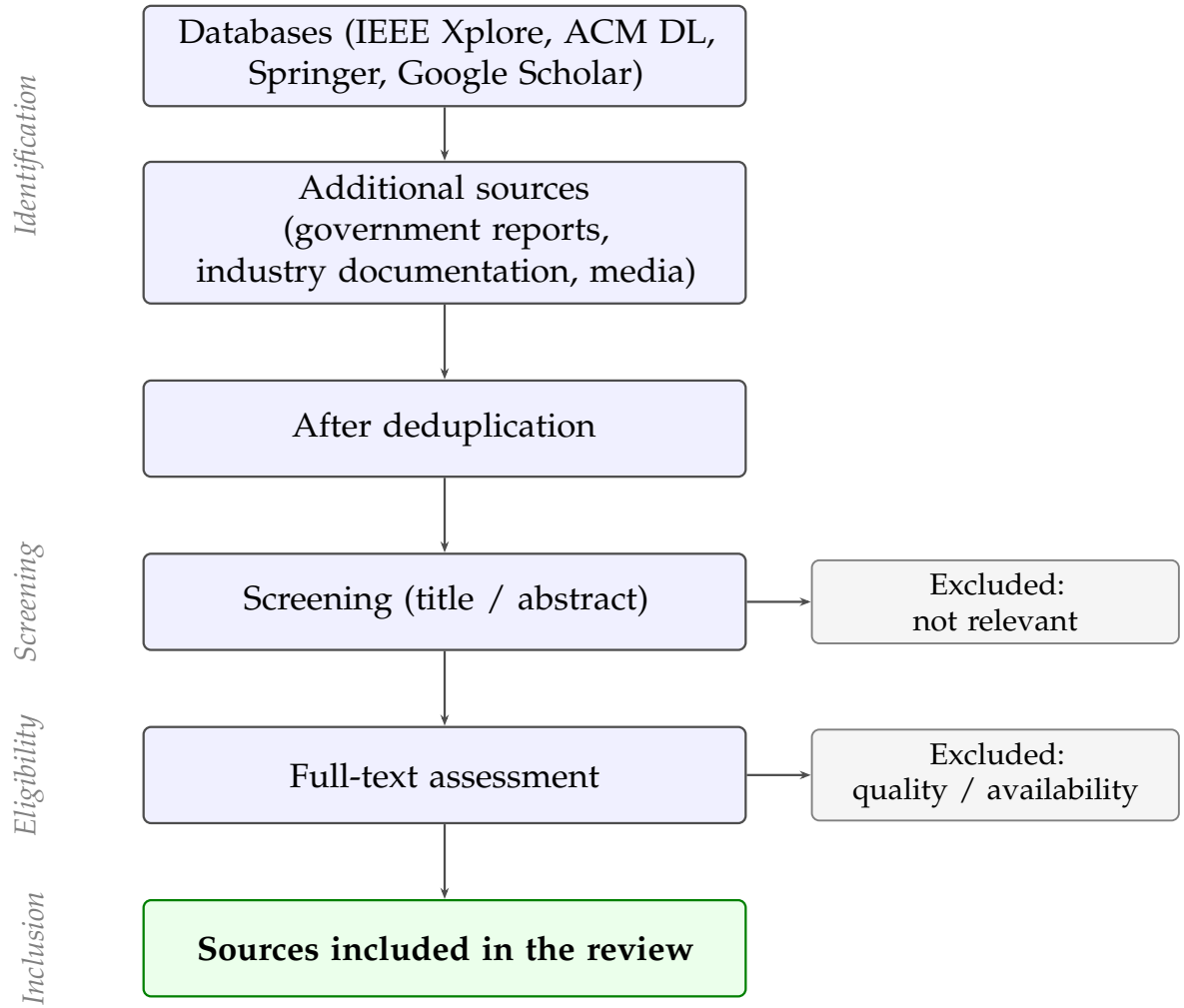

Figure 2. Simplified source selection diagram (adapted from PRISMA) for narrative review.

2.2. 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. In leading reports such as the Verizon DBIR editions 2023–2026 [5,6], the Evil Twin attack does not appear as a separate category. Incidents exhibiting characteristics of this attack vector are absorbed into broader groups:

- Credential abuse – accounts for approximately 22% of initial attack vectors in DBIR 2025 [6,7],
- Phishing – constitutes 16–19% of initial vectors [6,8,9],
- Social engineering – combined with human error, accounts for approximately 60% of all incidents [10–12],
- Adversary-in-the-Middle (MitM) – appears as a category but without distinguishing the specifics of wireless attacks [6,8,13].

Limitations of the analysis included, among others, the lack of full access to confidential reports and potential biases in industry sources. To minimize these, data were cross-verified against inde-

 doi:10.20944/preprints202606.0325.v1

pendent institutional sources, e.g., by comparing NIST SP 800-97 recommendations[2] [14,15] with the ENISA Threat Landscape[3] 2025 reports [16,17].

2.3. 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 an original, extended taxonomy of Evil Twin attack mutations – a comprehensive classification developed on the basis of data synthesis from 2005–2026, systematizing the attack evolution in a manner not previously presented in scientific literature or industry reports. The taxonomy divides mutations into four main categories:

- Classical mutation (2005–2013): long-lived rogue APs with active deauthentication and traffic sniffing.
- Hybrid mutation (2014–2019): technical integration with social engineering – phishing captive portals and D2D (Device-to-Device, i.e., direct communication between devices without infrastructure mediation), where the rogue AP serves solely for initial infection and then disappears.
- Flash mutation (2020–2026): ultra-short-lived attacks, often without the use of deauthentication (bypassing PMF), based on natural client roaming.
- Opportunistic-hybrid mutation (projected 2026+): combination of flash mutation with contextual elements and automation.

The second contribution is original mathematical modeling of attack dynamics, centered on the concept of exposure time (T_e). The third contribution is a proposal to extend incident reporting policies with a mandatory, separate category of "Wi-Fi Spoofing / Rogue AP Impersonation" in global reports.

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 [18,19]. The disparity between the ease of preparing the attack (tools such as Wi-Fi Pineapple, hostapd-wpe, Wifiphisher [20]) 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

[2] NIST SP 800-97 is a key document on Wi-Fi security – it discusses rogue AP detection, beacon fingerprinting, and mutual authentication as defenses against the Evil Twin.

[3] An annual ENISA threat report – in the 2024–2025 editions, attacks on Wi-Fi/5G are classified as MitM/network interception.

 doi:10.20944/preprints202606.0325.v1

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 [13], 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.

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) [21], 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" [22–24], 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.

 doi:10.20944/preprints202606.0325.v1

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 [25,26] and Thomas d'Otreppe de Bouvette[4] (creator of Aircrack-ng [27]).

The 2011 workshops [28] 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 [29], 2016 [30]) 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 [31] 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) [32,33] 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", "FBI Surveillance Van") [34]. Journalists, including Glenn Greenwald [35,36] (The Intercept [37,38]), 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) [39,40] in The Hague, which at that time was investigating the poisoning of Sergei Skripal [41] using the Novichok nerve agent [42] and the alleged chemical attack in Douma (Syria) [43].

Cyber operators Aleksei Morenets [44,45] and Yevgeny Serebriakov [46,47], along with HUMINT (Human Intelligence) support (Oleg Sotnikov [48,49], Aleksei Minin [50,51]) [52], 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 [53–55].

The operation was disrupted on April 13, 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 [56]. This incident constitutes one of the best-documented cases of the use

[4] 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.

 doi:10.20944/preprints202606.0325.v1

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 [57,58].

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, cost below 200 USD per unit), controlled via a smartphone from publicly accessible places (e.g., park benches, 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 [59] 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, 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, 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 [60], client-side RTT analysis [61], and machine learning techniques on AWID3 datasets [62].

4.9. WatchGuard Threat Lab Research (2021–2023)

The WatchGuard Threat Lab team [63] 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, United Kingdom, Germany, Brazil), encompassing international airports, hotel chains, and restaurant chains [64,65].

The study was based on the verification of six threat categories defined within the Trusted Wireless Environment (TWE) standard [66], 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; (6) Misconfigured Access Point – configuration errors facilitating attack. This classification became the basis for industry certifications (e.g., Security+) [67].

 doi:10.20944/preprints202606.0325.v1

4.9.1. Research Results

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; (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 [68] demonstrated that most leading wireless infrastructure vendors (Cisco, Aruba, Ruckus, 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.

4.9.2. Critical Assessment of the TWE Standard

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 [64] and critical infrastructure.

Table 2 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 [69,70]. 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 [71,72]. Reports by TechTudo [71], Olhar Digital [72], and Canaltech [73] documented scenarios in which attackers created rogue access points with SSIDs identical to legitimate networks in shopping centres 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.

 doi:10.20944/preprints202606.0325.v1

Table 2. 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	2008–14	Passive detection	AP ID via TSF clock skew [74,75] or HW traits [76]	Calibration needed; environmental sensitivity; limited scalability
PMF (802.11w)	2009/18	Frame protection	Blocks deauth/disassoc spoofing; mandatory in WPA3 [77]	No protection against ET without deauth (new clients, open nets, auto-connect) [78]
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 [79,80]	Cisco HW only; no protocol-level attack detection
Client-side detection	2010–18	Active/passive	Route analysis [81]; WiFi-Hop [82]; stats [83]; channel mon. [84]; TCP delay [85]	Network-dependent; limited in high-load networks
Aruba RFProtect	2012+	Multi-sensor	Threat classification; auto rogue AP containment [86]	Sensor density dependent; false positives in multi-tenant env.
Meraki Air Marshal	2014+	Cloud WIPS	Auto SSID spoof detection; cloud mgmt [87]	Requires cloud; limited local policy control
WPA3-SAE	2018	Encryption	No offline dictionary attacks; forward secrecy; per-session protection [88,89]	Does not verify AP identity — encrypted connection to rogue AP possible [90]
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 centralised ET detection and containment [60]	Requires SDN; not for traditional networks
ML-based WIDS	2022–23	ML classification	Feature sel. + classifiers on AWID/AWID3 [62,91]; CSI FP [92]	Training data needed; limited cross-HW generalisability
Sig.-based MC-MitM IDS	2024	Passive signature-based	Distributed multi-ch. MitM detection [93,94]; TPR≥90%	60 s delay; sensor deployment; known signatures only

5. Authors' Contribution: Analysis, Modelling, 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 realise 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 initialisation mechanism.

5.1.1. Position of the Evil Twin Attack in the MITRE ATT &CK Framework

Within MITRE ATT&CK[5], 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.

5.1.2. Chronological Evolution of the Evil Twin Attack

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.

[5] In MITRE ATT&CK, the closest techniques are: T1557 – Adversary-in-the-Middle, T1595 – Active Scanning.

 doi:10.20944/preprints202606.0325.v1

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 realise 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. [95] additionally demonstrated the feasibility of conducting a MitM attack without a rogue access point, utilising 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 [77,78]. 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 characterised 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 3 presents the evolution of the Evil Twin attack within the context of the MITRE ATT&CK framework.

Table 3. 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
2004–07	Classical ET + deauth; laptop + Wi-Fi card	Sniffing	V.L/V.L	TA0001, TA0009	—
2008–13	KARMA/MANA + portal; Pineapple Mk4	Portal phish. + sniff.	L/L	TA0001, TA0006	Conf.
2014–17	SSL strip / HSTS bypass; Pineapple + bettercap	MitM, cred. harv.	L–M/M	TA0006, TA0009, TA0005	RNC '16
2018–19	Close-access ET, D2D; spec. HW / RPi	802.1X cred. theft	M–H/M	TA0001, TA0006, TA0008	OPCW, DOI
2020–22	Ultra-short (<60 s), PMF bypass; RPi 4/Zero	Malware via portal	H/H	TA0001, TA0005, TA0011	Few publ.
2023–25	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 defence, 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.

5.2.1. Evil Twin Kill Chain Stages

[A] Reconnaissance (radio reconnaissance) – identification of SSIDs, security types, client behaviour, probe requests.

 doi:10.20944/preprints202606.0325.v1

[B] Weaponization (ET preparation)[6] – configuration of the rogue AP, captive portal, and automation.

[C] Delivery (vector delivery) – deauthentication, SSID spoofing, forced connection.

[D] Initial Access (TA0001) – the victim connects to the rogue AP.

[E] Credential Access (TA0006) – credential phishing, session token interception.

[F] Collection (TA0009) – traffic sniffing, session hijacking, data interception.

[G] Execution / Payload Delivery (optional) – malware delivery via captive portal or MITM.

[H] Command and Control (TA0011) – C2 communication initialisation, beaconing.

[I] Lateral Movement (TA0008) – lateral movement within the victim's network.

[J] Impact (TA0040) – further operational objectives of the campaign.

Table 4 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 4. 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 behaviour 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 & Control	Network	TA0011	C2 channel initialisation, 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 [96].

5.2.2. Kill Chain – MITRE ATT &CK Mapping

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 initialisation vector that realises multiple tactics in parallel, with its initial phases occurring beyond the classical Initial Access moment, at the radio and behavioural layers.

Table 5 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 5. 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

[6] Weaponization – 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.

 doi:10.20944/preprints202606.0325.v1

tactics realised in each successive attack generation, and the transformation of the Evil Twin role from a standalone vector to an offensive campaign initialisation module.

5.3. Evil Twin as a Campaign Initialisation Vector

5.3.1. Introduction and Concept Redefinition

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 specialised campaign initialisation vector, analogous to email phishing, watering hole attacks[7], or malicious USB drives.

5.3.2. Evil Twin and the Limitations of the Classical Technical Perspective

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 realise multiple tactics in parallel.

5.3.3. Evil Twin as a Kill Chain Initialisation Vector

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 initialisation vectors.

5.3.4. Comparison with Other Initialisation Vectors

A comparison of Evil Twin with classical initialisation 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 characterised by very short exposure times.

5.3.5. Implications for Threat Modelling and Defence

Adopting the perspective of Evil Twin as a campaign initialisation 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

5.4.1. Introduction and Motivation

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 artefacts.

[7] Watering hole attacks are sophisticated cyberattacks in which adversaries compromise legitimate, niche websites frequently visited by a specific target group.

 doi:10.20944/preprints202606.0325.v1

5.4.2. Absence of the Temporal Dimension in MITRE ATT &CK

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 utilised or not utilised, 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. [97] additionally demonstrated the feasibility of conducting an Evil Twin attack using the 802.11v protocol, which further complicates temporal analysis.

5.4.3. Formalisation 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:

$$T_e = T_a + T_i + T_d \tag{1}$$

where: T_e – attack exposure time [s]; T_a – attack preparation and initialisation 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]; T_d – detectable radio artefact 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.

5.4.4. 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 6).

Table 6. 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 favour of the attacker.

5.4.5. Attack Profitability Model

To quantitatively assess the attractiveness of the attack from the adversary's perspective, we propose a profitability function:

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

where: $O(T_e)$ – profitability of the Evil Twin attack as a function of exposure time; $P_x(T_e)$ – 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

 doi:10.20944/preprints202606.0325.v1

the attack from 20 [s] to 10 [s] doubles the profitability, whereas reducing it from 120 [s] to 110 [s] constitutes a marginal change.

5.4.6. Attack Effectiveness Model: The "Compromise Window" Concept

As an extension of the profitability model, we introduce an attack effectiveness metric (E_{eff}), accounting for the dynamics of data exfiltration[8]:

$$E_{\text{eff}} = P_{\text{succ}} \times \int_0^{T_e} D(t)\,\mathrm{d}t \times \left(1 - P_x(T_e)\right) \tag{3}$$

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; $P_x(T_e)$ – probability of attack detection.

Table 7 presents typical modelling assumptions for P_{succ}.

Table 7. 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], $\int D(t)\,\mathrm{d}t = 25$ 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 emphasised 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, utilising 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

5.5.1. Introduction and Concept Redefinition

In the scientific literature, the Evil Twin attack is most commonly classified as a variant or technique within broader categories. In this paper, the authors propose a new classification in which the Evil Twin attack is treated not as a "variant" or "technique," but as an evolutionary mutation. This perspective enables capturing: changes in the attack's function, changes in the attack's role within full campaigns, and changes in the attack's relationship to other kill chain stages.

5.5.2. Variants Vs. Mutations

Traditional classification focuses on tools (classical Evil Twin, KARMA/MANA, MITM with SSL stripping, Wi-Fi Pineapple variants) but does not encompass the changing function of the attack or its transformations within larger operations.

Evolutionary mutations, by contrast, represent the process of attack adaptation in response to changing technologies, defence methods, and the operational objectives of adversaries. Each mutation is not simply a version of the previous one but constitutes a response to new challenges.

[8] 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.

 doi:10.20944/preprints202606.0325.v1

5.5.3. Key Findings

- **Functional transformation**: the changing function of the attack, from a simple technique to a multi-stage vector, demonstrates the mutational character of this threat.
- **Attack role**: the changing role in offensive campaigns enables multifunctional utilisation – not only as an Initial Access vector but as a tool initiating further techniques.
- **New classification**: the mutation taxonomy enables a more precise capture of the Evil Twin attack's evolution and its adaptation to new technological challenges.

The temporal boundaries of individual mutations were established based on pivotal changes in attack characteristics: the year 2013 marks the emergence of the MANA framework, which automated impersonation of WPA-Enterprise networks and initiated the integration of Evil Twin with social engineering (captive portal phishing); the year 2019 denotes the transition to short-lived (flash) variants, driven by the widespread adoption of PMF (IEEE 802.11w) and the necessity to circumvent deauthentication; the year 2026 represents the projected boundary beyond which opportunistic-hybrid mutations leveraging AI and IoT may dominate the threat landscape.

Figure 3 presents a graphical representation of the proposed Evil Twin attack mutation taxonomy, illustrating the relationships between individual categories, their temporal scope, and key distinguishing characteristics.

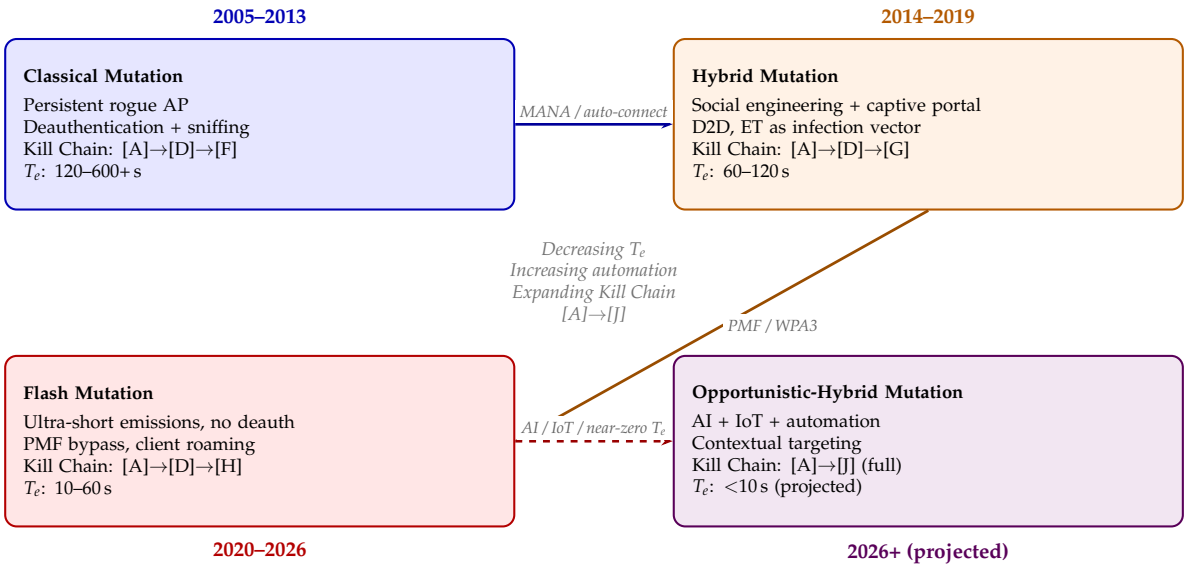

Figure 3. Proposed Evil Twin attack mutation taxonomy – four evolutionary categories with key distinguishing characteristics.

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

5.6.1. Introduction and Problem Definition

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.

5.6.2. 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.

 doi:10.20944/preprints202606.0325.v1

- **Delivery [C]**: access point impersonation and forcing the victim's connection – a technique not described in ATT&CK in the radio context.

5.6.3. Comparison with Existing MITRE ATT &CK Extensions

The problem of incomplete coverage of attack domains within MITRE ATT&CK is not unique to the radio layer. The MITRE organisation 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 specialised 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, 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.

5.6.4. Implications and Conclusions

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 [98] demonstrated that vulnerabilities at the Wi-Fi frame aggregation and fragmentation level (FragAttacks) extend beyond the MITRE ATT&CK classification. Existing extensions (ICS, Mobile) confirm the feasibility and value of creating specialised domains. We propose considering an analogous extension, "ATT&CK for Wireless," encompassing: radio reconnaissance (SSID scanning, probe request analysis), radio layer weaponisation (rogue AP configuration, beacon spoofing), and radio layer delivery (forced connection through deauthentication or roaming manipulation). Such an extension would enable more comprehensive modelling of Wi-Fi attacks and their role in APT campaigns.

6. Hypotheses on the Evolution of the Evil Twin Attack

6.1. Introduction

The evolution of Evil Twin attacks exhibits a clear tendency towards increasing effectiveness, reducing exposure time, and automation. The objective of this section is to present hypotheses regarding further development – propositions for verification that may serve as inspiration for new empirical research.

6.2. Hypothesis 1 – Near-Zero Exposure Attacks

H1: The further evolution of the Evil Twin attack will trend towards near-zero exposure attacks, executed in a fully automated manner by mobile devices, with minimal user involvement.

Contemporary mutations are characterised by very short T_e values, which in the most recent variants amount to merely several tens of seconds. Automation and the advancement of 5G/AI may lead to a complete reduction of activity time to near-zero [99], significantly impeding detection. The consequences include the necessity for detection methods to evolve towards behavioural anomaly analysis.

6.3. Hypothesis 2 – AI Exploitation

H2: The Evil Twin attack will leverage artificial intelligence for the automated creation of rogue access points and precise attack targeting. AI may enable intelligent victim detection, dynamic real-time SSID generation, and the utilisation of data from previous attacks for adaptation.

 doi:10.20944/preprints202606.0325.v1

6.4. Hypothesis 3 – IoT Integration

H3: With the growing number of IoT devices, the Evil Twin attack will integrate with mobile devices, routers, and smart IoT devices, enabling a broader attack reach and improved concealment from detection systems. IoT devices do not always possess adequate protection mechanisms, rendering them new attack vectors.

6.5. Hypothesis 4 – Complex Attacks Leveraging 5G

H4: With the widespread adoption of 5G technology, the Evil Twin attack will become more complex, leveraging higher transfer speeds and lower latency to conduct attacks on a global scale. The consequences include an increased threat to major cities and public areas, as well as a reduction in the time from initiation to data exfiltration.

7. Summary and Conclusions

This paper constitutes a comprehensive study of the evolution of the Evil Twin attack, one of the most persistent and adaptive threats in the domain of wireless network security. Since its first public demonstration in 2005 at the Black Hat conference, this attack has undergone a profound transformation – from passive network traffic interception to advanced, hybrid variants integrating elements of social engineering, automation, and artificial intelligence.

The chronological analysis, based on a data triangulation methodology drawing from scientific literature, industry reports (e.g., Verizon DBIR, IBM X-Force, WatchGuard Threat Lab), and institutional reports (NIST, ENISA, CISA), revealed a systematic reduction in exposure time, hybridisation of techniques, and a growing underestimation of incidents in global statistics, where these attacks are subsumed under broader categories such as phishing (16–19% of entry vectors in DBIR 2025) and credential abuse (22%).

The key authorial contribution is the redefinition of the Evil Twin attack not as an isolated technique but as an offensive campaign initialisation vector, implementing a non-standard kill chain with emphasis on the phases preceding Initial Access (TA0001). The proposed mutation taxonomy divides the evolution into four categories: classical (2005–2013), hybrid (2014–2019), flash (2020–2026), and opportunistic-hybrid (projected 2026+).

An exposure time metric was introduced:

$$T_e = T_a + T_i + T_d$$

with empirical time ranges. The T_e scale categorises attacks from very short (<10 [s], very high profitability) to long (>120 [s], very low profitability). The profitability model $O(T_e) = (1 - P_x(T_e))/T_e$ and the effectiveness model $E_{\text{eff}} = P_{\text{succ}} \times \int_0^{T_e} D(t)\,\mathrm{d}t \times (1 - P_x(T_e))$ quantify the trade-off between minimising T_e and maximising gains. These tools address a gap in MITRE ATT&CK – the missing temporal dimension – and propose extending incident reporting with a dedicated "Wi-Fi Spoofing / Rogue AP Impersonation" category.

Evil Twin does not disappear but rather mutates in response to security measures, becoming a resilient threat within the 5G/IoT ecosystem. Its underestimation in industry reports leads to a chronic underestimation of scale, which delays the development of defences. From a practical perspective, this paper recommends reducing WIDS detection cycles below 10–20 [s] [100,101], integrating AI/ML for beacon analysis [93], and updating standards (ENISA/NIST/CISA) to account for opportunistic flash mutations.

Limitations include model simplifications (e.g., additivity of T_e, linear P_x) and the lack of complete data on confidential incidents. Directions for future research include validation through penetration testing, estimation of $D(t)$ for tools such as Wi-Fi Pineapple Mk VII, and extension to BLE/5G attacks. Ultimately, this paper underscores the attack-defence asymmetry, where minimisation of T_e overshadows the significance of technical improvements, opening the path to the adaptation of frameworks and reporting policies for improved visibility of radio-layer threats.

 doi:10.20944/preprints202606.0325.v1

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.

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. Alotaibi, B.; Elleithy, K. Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions. *Wireless Personal Communications* **2016**, *90*, 1261–1290. https://doi.org/10.1007/s11277-016-3390-x.
2. Kohlios, C.P.; Hayajneh, T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. *Electronics* **2018**, *7*, 284. https://doi.org/10.3390/electronics7110284.
3. Nazir, R.; Laghari, A.A.; Kumar, K.; David, S.; Ali, M. Survey on Wireless Network Security. *Archives of Computational Methods in Engineering* **2022**, *29*, 1591–1610. https://doi.org/10.1007/s11831-021-09631-5.
4. Vanhoef, M.; Piessens, F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In Proceedings of the Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, 2017, pp. 1313–1328. https://doi.org/10.1145/3133956.3134027.
5. Verizon. Data Breach Investigations Report (DBIR), 2025. Accessed: 2026-01-15.
6. Verizon. 2025 Data Breach Investigations Report. Technical report, Verizon Business, 2025. Accessed: 2026-01-15.
7. Verizon. Credential Stuffing and Credential Abuse – DBIR Insights, 2025. Accessed: 2026-01-15.
8. Beyond Identity. Key Takeaways from the Verizon DBIR 2025, 2025. Accessed: 2026-01-15.
9. Keepnet Labs. Verizon DBIR 2025 Analysis: Key Findings, 2025. Accessed: 2026-01-15.
10. Mimecast. Verizon DBIR: Human Error Remains Top Factor, 2025. Accessed: 2026-01-15.
11. SpyCloud. Insights from the Verizon DBIR 2025, 2025. Accessed: 2026-01-15.
12. Descope. Verizon DBIR 2025: Identity and Access Trends, 2025. Accessed: 2026-01-15.
13. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials* **2016**, *18*, 2027–2051. https://doi.org/10.1109/COMST.2016.2548426.
14. National Institute of Standards and Technology. NIST Special Publication 800-97: Establishing Wireless Robust Security Networks. Technical report, NIST, 2007. Accessed: 2026-01-15.
15. Frankel, S.; Eydt, B.; Owens, L.; Scarfone, K. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Technical Report SP 800-97, NIST, 2007. Accessed: 2026-01-15.
16. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025. Technical report, ENISA, 2025. Accessed: 2026-01-15.
17. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025 – Booklet. Technical report, ENISA, 2025. Accessed: 2026-01-15.
18. 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. https://doi.org/10.3390/data9100119.
19. 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). Springer, 2024, Vol. 1060, *LNNS*. https://doi.org/10.1007/978-3-031-78928-1_26.
20. Chatzisofroniou, G.; Kotzanikolaou, P. Exploiting WiFi Usability Features for Association Attacks in IEEE 802.11: Attack Analysis and Mitigation Controls. *Journal of Computer Security* **2022**, *30*, 357–380. https://doi.org/10.3233/JCS-210036.

 doi:10.20944/preprints202606.0325.v1

21. Beetle.; Potter, B. Rogue Squadron: Evil Twins, 802.11intel, Radical RADIUS, and Wireless Weaponry for Windows. Black Hat USA 2005, 2005. Accessed: 2026-05-06.
22. Gopinath, K.N. Multipot: A More Potent Variant of Evil Twin. DEF CON 15, 2007. Accessed: 2026-05-06.
23. Gopinath, K.N. Multipot: A More Potent Variant of Evil Twin – Whitepaper, 2007. Accessed: 2026-05-06.
24. Gopinath, K.N. Multipot: A More Potent Variant of Evil Twin – Presentation, 2007. Accessed: 2026-05-06.
25. Ramachandran, V. Official Instagram Profile, 2026. Accessed: 2026-05-06.
26. Ramachandran, V. Official Facebook Profile, 2026. Accessed: 2026-05-06.
27. d'Otreppe de Bouvette, T. Aircrack-ng, 2006. Official project website. Accessed: 2026-05-06.
28. Black Hat USA 2011 Archives, 2011. Accessed: 2026-05-06.
29. Advanced Wi-Fi Pentesting. Black Hat USA 2015 Training, 2015. Accessed: 2026-05-06.
30. Advanced Wi-Fi Attack and Defense for Hackers and Pentesters. Black Hat USA 2016 Training, 2016. Accessed: 2026-05-06.
31. 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. *International Journal of Wireless and Ad Hoc Communication* **2013**. Accessed: 2026-05-06, https://doi.org/10.1109/WCCIT.2013.6618697.
32. TrustedSec. Social Engineer Toolkit, 2026. GitHub repository. Accessed: 2026-05-06.
33. TrustedSec. Social Engineer Toolkit User Manual, 2026. Accessed: 2026-05-06.
34. Shinal, J. Fake Wi-Fi Hotspots Lure RNC Attendees. USA Today, 2016. Accessed: 2026-05-06.
35. Greenwald, G. Journalists and Trump delegates among those tricked by fake Wi-Fi networks at RNC, 2016. The Intercept. Accessed: 2026-05-06.
36. Intercept, T. Glenn Greenwald Profile, 2026. Accessed: 2026-05-06.
37. The Intercept, 2014. Digital media outlet founded in 2014. Accessed: 2026-05-06.
38. Intercept, T. The Intercept, 2026. Accessed: 2026-05-06.
39. Organisation for the Prohibition of Chemical Weapons. OPCW – About Us, 2026. Official OPCW website. Accessed: 2026-05-06.
40. OPCW. Organisation for the Prohibition of Chemical Weapons, 2026. Accessed: 2026-05-06.
41. Government of the United Kingdom. Salisbury attack: UK government response, 2018. Official UK government collection. Accessed: 2026-05-06.
42. 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. Accessed: 2026-05-06.
43. 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, 2019. Final report. Accessed: 2026-05-06.
44. Federal Bureau of Investigation. Aleksei Sergeyevich Morenets, 2026. Accessed: 2026-05-06.
45. UK Sanctions List – Aleksei Morenets, 2026. Accessed: 2026-05-06.
46. Federal Bureau of Investigation. Evgenii Mikhaylovich Serebriakov, 2026. Accessed: 2026-05-06.
47. OpenSanctions Entry – Evgenii Serebriakov, 2026. Accessed: 2026-05-06.
48. Federal Bureau of Investigation. Oleg Mikhaylovich Sotnikov, 2026. Accessed: 2026-05-06.
49. OpenSanctions. Oleg Mikhaylovich Sotnikov, 2026. Accessed: 2026-05-06.
50. Federal Bureau of Investigation. Alexey Valerevich Minin, 2026. Accessed: 2026-05-06.
51. OpenSanctions. Alexey Valerevich Minin, 2026. Accessed: 2026-05-06.
52. Lowenthal, M.M. *Intelligence: From Secrets to Policy*, 8th ed.; CQ Press: Washington, DC, 2020.
53. Government of the United Kingdom. Minister for Europe statement: Attempted hacking of the OPCW by Russian military intelligence, 2018. Accessed: 2026-05-06.
54. OPCW. EC-89 United States National Statement, 2018. Accessed: 2026-05-06.
55. BBC News. Russia cyber-plots: US, UK and Netherlands allege attacks, 2018. Accessed: 2026-05-06.
56. CrowdStrike Intelligence. FANCY BEAR (APT28): A Window into Russia's Cyber Espionage Operations. Technical report, CrowdStrike, 2016. Threat intelligence report. Accessed: 2026-05-06.
57. 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. Accessed: 2026-05-06.
58. GovInfo. Evil Twins, Eavesdropping, and Password Cracking, 2020. Accessed: 2026-05-06.
59. Jain, V.; Laxmi, V.; Gaur, M.S.; Mosbah, M. ETGuard: Detecting D2D Attacks Using Wireless Evil Twins, 2019, [1903.05843]. Accessed: 2026-05-06.

 doi:10.20944/preprints202606.0325.v1

60. Shrivastava, P.; Jamal, M.S.; Kataoka, K. EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi. *IEEE Transactions on Network and Service Management* **2020**, *17*, 89–102. https://doi.org/10.1109/TNSM.2020.2972774.
61. Kitisriworapan, S.; Jansang, A.; Phonphoem, A. Client-Side Rogue Access-Point Detection Using a Simple Walking Strategy and Round-Trip Time Analysis. *EURASIP Journal on Wireless Communications and Networking* **2020**, *2020*, 252. https://doi.org/10.1186/s13638-020-01864-5.
62. da Silva, L.M.; Andreghetti, 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 Proceedings of the 6th International Conference on Machine Learning and Machine Intelligence (MLMI 2023). ACM, 2023, pp. 168–175. https://doi.org/10.1145/3635638.3635665.
63. WatchGuard Technologies. WatchGuard Technologies, 2026. Accessed: 2026-05-06.
64. WatchGuard Technologies. Six Wi-Fi Attacks Impacting Hotel Guests, 2026. Accessed: 2026-05-06.
65. WatchGuard Technologies. Exposed: Networks Vulnerable to Evil Twin Attacks, 2026. Accessed: 2026-05-06.
66. WatchGuard Technologies. Trusted Wireless Environment, 2026. Accessed: 2026-05-06.
67. Messer, P. Rogue Access Points, 2026. Accessed: 2026-05-06.
68. Miercom. Miercom, 2026. Accessed: 2026-05-06.
69. Australian Federal Police. Man charged over creation of Evil Twin free Wi-Fi networks to access personal data, 2024. Accessed: 2026-05-06.
70. Security Affairs. Evil Twin WiFi attack on plane, 2024. Accessed: 2026-05-06.
71. TechTudo. Depois que conheci esse golpe, nunca mais usei redes de Wi-Fi públicas, 2025. Accessed: 2026-05-06.
72. Olhar Digital. Cuidado com o Evil Twin! Conheça o golpe do Wi-Fi falso e veja como se prevenir, 2025. Accessed: 2026-05-06.
73. Canaltech. Agências dos EUA e Europa recomendam desligar Wi-Fi ao sair de casa; entenda, 2025. Accessed: 2026-05-06.
74. Jana, S.; Kasera, S.K. On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews. In Proceedings of the Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom). ACM, 2008, pp. 104–115. https://doi.org/10.1145/1409944.1409958.
75. Han, H.; Sheng, B.; Tan, C.C.; Li, Q.; Lu, S. A Timing-Based Scheme for Rogue AP Detection. *IEEE Transactions on Parallel and Distributed Systems* **2011**, *22*, 1912–1925. https://doi.org/10.1109/TPDS.2011.125.
76. 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 Proceedings of the 10th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet). ACM, 2014, pp. 87–98. https://doi.org/10.1145/2642687.2642691.
77. Schepers, D.; Ranganathan, A.; Vanhoef, M. On the Robustness of Wi-Fi Deauthentication Countermeasures. In Proceedings of the Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22). ACM, 2022, pp. 245–256. https://doi.org/10.1145/3507657.3528548.
78. 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). Springer, 2022, Vol. 13291, *LNCS*, pp. 235–251. https://doi.org/10.1007/978-3-031-08147-7_16.
79. Cisco Systems. Cisco Adaptive Wireless Intrusion Prevention System, 2026. Accessed: 2026-05-07.
80. Cisco Systems. Cisco CleanAir Technology, 2026. Accessed: 2026-05-07.
81. 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 Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2010, pp. 323–332. https://doi.org/10.1109/DSN.2010.5544302.
82. Monica, D.; Ribeiro, C. WiFiHop — Mitigating the Evil Twin Attack through Multi-hop Detection. In Proceedings of the Proceedings of the 16th European Symposium on Research in Computer Security (ESORICS 2011). Springer, 2011, Vol. 6879, *LNCS*, pp. 21–39. https://doi.org/10.1007/978-3-642-23822-2_2.
83. Yang, C.; Song, Y.; Gu, G. Active User-Side Evil Twin Access Point Detection Using Statistical Techniques. *IEEE Transactions on Information Forensics and Security* **2012**, *7*, 1638–1651. https://doi.org/10.1109/TIFS.2012.2207383.
84. Nakhila, O.; Zou, C. User-Side Wi-Fi Evil Twin Attack Detection Using Random Wireless Channel Monitoring. In Proceedings of the Proceedings of the 2016 IEEE Military Communications Conference (MILCOM). IEEE, 2016, pp. 1243–1248. https://doi.org/10.1109/MILCOM.2016.7795501.

 doi:10.20944/preprints202606.0325.v1

85. 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 Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT). IEEE, 2018, pp. 1–6. https://doi.org/10.23919/ICACT.2018.8323699.
86. Hewlett Packard Enterprise. Aruba RFProtect Wireless Intrusion Protection, 2026. Accessed: 2026-05-07.
87. Cisco Systems. Cisco Meraki Air Marshal, 2026. Accessed: 2026-05-07.
88. 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), 2020, pp. 517–533. https://doi.org/10.1109/SP40000.2020.00031.
89. Halbouni, A.; Ong, L.Y.; Leow, M.C. Wireless Security Protocols WPA3: A Systematic Literature Review. *IEEE Access* **2023**, *11*, 112438–112450. https://doi.org/10.1109/ACCESS.2023.3322931.
90. Chatzoglou, E.; Kampourakis, G.; Kolias, C. How is Your Wi-Fi Connection Today? DoS Attacks on WPA3-SAE. *Journal of Information Security and Applications* **2022**, *64*, 103058. https://doi.org/10.1016/j.jisa.2021.103058.
91. Kamble, A.; Kshirsagar, D. Feature Selection in Wireless Intrusion Detection System for Evil Twin Attack Detection. In Proceedings of the Proceedings of the 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT). IEEE, 2023, pp. 1–6. https://doi.org/10.1109/CISCT57197.2023.10351382.
92. Liu, X.; Yang, J.; Chen, Y.; Guo, X.; Xie, Y. Real-Time Identification of Rogue WiFi Connections in the Wild. *IEEE Access* **2022**, *10*, 126896–126910. https://doi.org/10.1109/ACCESS.2022.3226421.
93. 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. https://doi.org/10.1109/ACCESS.2024.3363748.
94. 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. *International Journal of Information Security* **2024**, *23*, 3457–3479. https://doi.org/10.1007/s10207-024-00899-9.
95. 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), 2023, pp. 694–709. https://doi.org/10.1109/SP46215.2023.10179441.
96. Muthalagu, R.; Sanjay, S. Evil Twin Attack Mitigation Techniques in 802.11 Networks. *International Journal of Advanced Computer Science and Applications (IJACSA)* **2021**, *12*. https://doi.org/10.14569/IJACSA.2021.0120605.
97. Louca, C.; Peratikou, A.; Stavrou, S. A Novel Evil Twin MiTM Attack through 802.11v Protocol Exploitation. *Computers & Security* **2023**, *130*, 103261. https://doi.org/10.1016/j.cose.2023.103261.
98. Vanhoef, M. Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 161–178.
99. Braga, D.D.A.; Kulatova, N.; Sabt, M.; Fouque, P.A.; Bhargavan, K. From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake. In Proceedings of the 2023 IEEE 8th European Symposium on Security and Privacy (EuroSP), 2023, pp. 707–723. https://doi.org/10.1109/EuroSP57164.2023.00048.
100. Kumar, Y.; Kumar, V. A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications. *Wireless Personal Communications* **2023**, *133*, 395–452. https://doi.org/10.1007/s11277-023-10773-x.
101. Nivaashini, M.; Thangaraj, P. Computational Intelligence Techniques for Automatic Detection of Wi-Fi Attacks in Wireless IoT Networks. *Wireless Networks* **2021**, *27*, 2761–2784. https://doi.org/10.1007/s11276-021-02594-2.