Bastille

RESEARCH REPORT

Emerging Wireless-Enabled Threats in 2025

A Threat Intelligence Briefing

Introduction

Wireless communication is the backbone of modern national security, business operations, and critical infrastructure. However, as reliance on wireless technologies grows, so does the attack surface available to sophisticated adversaries. Nation-state actors, cybercriminal groups, and malicious insiders exploit Wi-Fi, Bluetooth, and Radio Frequency communication vulnerabilities to conduct espionage, sabotage systems, and steal sensitive information.

The threats outlined in this report represent the most pressing wireless-enabled risks that all enterprises, especially the new US Executive administration, must address. These include state-backed cyberattacks, the misuse of consumer surveillance devices, and vulnerabilities in widely deployed wireless standards. As adversaries refine their techniques, the U.S. government must implement proactive security measures to protect national interests, as the potential impact of these threats is significant.

1-“Nearest Neighbor Attack” from APT-28

APT-28, also known as *Fancy Bear*, is a Russian state-sponsored cyber espionage group linked to the GRU. The group is known for its advanced network exploitation techniques, including the *Nearest Neighbor Attack*, which hijacks nearby wireless network connections to attack proximity targets.

Attack Methodology

1. **Signal Manipulation**: APT-28 used high-gain directional antennas to amplify a rogue Wi-Fi signal, tricking target devices into believing it was the strongest available connection.
2. **Deauthentication & Reassociation**: Using *de-authentication packets*, APT-28 forces devices to disconnect from their legitimate network and automatically reconnect to the rogue AP.
3. **MITM Attack & Data Interception**: APT-28 acts as an intermediary, intercepting network traffic to steal credentials, decrypt encrypted data, and inject malware into devices.
4. **Post-Compromise Persistence**: Stolen credentials and compromised session cookies allow AP-28 to maintain access even after the victim disconnects from the rogue network.

Recent Exploits

APT-28 targets diplomatic missions, military bases, and government offices. Their ability to infiltrate organizations is a risk to national security. APT-28 recently targeted an organization using a multistage attack using wireless networks of neighboring organizations to infiltrate the target without

needing to be geographically nearby - the “Nearest Neighbor Attack” report recently published by Volexity.[1]

APT-28 used a password spray attack to validate credentials but could not log into the network due to MFA controls. Next, they compromised a nearby network and leveraged a system connected to both wired and wireless networks to attack the target. They used these validated credentials to log into the target’s Wi-Fi network, which did not have MFA protections. APT-28 stayed in the target for two years, using multiple neighboring Wi-Fi networks to stay connected to the target network.

Mitigation Strategies

- **Use certificate-based authentication for Wi-Fi** to prevent unauthorized access points from imitating trusted networks.
- **Deploy endpoint security tools** that detect and block unauthorized Wi-Fi connections.
- **Implement wireless intrusion detection systems (WIDS)** to monitor for rogue APs and de-authentication attacks.
- **Enforce mandatory VPN usage** to encrypt all network traffic, even if connected to a compromised network.

2-Typhoon APT Threat Groups

China’s state-sponsored hacking groups, known collectively as *Typhoon APTs* (e.g., APT-40, APT-41, Mustang Panda), are among the most aggressive cyber adversaries targeting the U.S. and its allies. These groups have advanced capabilities in wireless network infiltration and target government agencies, critical infrastructure, and defense contractors.

Attack Techniques

1. **Industrial Wi-Fi Exploitation**: Typhoon APTs focus on proprietary wireless communication protocols used in **SCADA (Supervisory Control and Data Acquisition)** systems, which control industrial operations.
2. **RF Beacons for Persistent Access**: Attackers implant RF beacons within compromised environments, enabling long-term data exfiltration even after removing the malware.

---

1 https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

3. **Strategic Rogue AP Deployment**: These groups place rogue Wi-Fi access points near embassies, defense contractor facilities, and corporate headquarters to intercept sensitive data.
4. **Wi-Fi Mesh Network Exploitation**: Attackers create hidden mesh networks using compromised IoT devices that evade traditional security monitoring.

Key Targets & National Security Risks

- **Energy Grids & Critical Infrastructure**: Wireless-based attacks on SCADA systems could lead to blackouts, water supply disruptions, or tampering with industrial processes.
- **Defense Contractors**: Stolen military technology and classified data could give adversaries an edge in geopolitical conflicts.
- **Financial Sector**: Cybercriminals backed by state actors could infiltrate banking networks to steal funds or disrupt economic stability.

Recent Exploits

Beginning around 2022, the Salt Typhoon group infiltrated at least nine major firms, including Verizon, AT&T, T-Mobile, Spectrum, Lumen, Consolidated Communications, and Windstream. The attackers exploited vulnerabilities in network devices, particularly routers manufactured by Cisco, to gain unauthorized access.

Once inside, Salt Typhoon employed "living-off-the-land" tactics, utilizing existing network tools to avoid detection. This approach allowed them to access sensitive data, including call and text message metadata, such as timestamps, IP addresses, and phone numbers, for over a million users, primarily in Washington, D.C.

The breach extended to systems used by U.S. law enforcement and intelligence agencies for court-authorized wiretapping, potentially exposing information about ongoing surveillance operations.

Mitigation Strategies

- **Isolate SCADA systems from corporate Wi-Fi networks** to reduce wireless attack vectors.
- **Use RF monitoring to detect unauthorized emissions** from hidden beacons or rogue access points.
- **Enforce strict access controls** and require multi-factor authentication (MFA) for all wireless network connections.

3-Pegasus & Predator / APT-29 Spyware

Adversaries use spyware tools like *Pegasus* and *Predator* in targeted surveillance campaigns against journalists, government officials, and corporate executives. APT-29 (*Cozy Bear*), a Russian intelligence-backed cyber group, has adopted similar techniques to access high-value targets.

Spyware Deployment Methods Over Wireless Networks

1. **Zero-Click Exploits**: Malicious payloads delivered over Wi-Fi or Bluetooth to infect devices without user interaction.
2. **Wi-Fi Injection Attacks**: Attackers inject spyware into devices connected to compromised public Wi-Fi networks.
3. **Bluetooth-Based Infection**: Exploits in Bluetooth pairing allow attackers to install spyware by simply being near a target.

Capabilities & Implications for National Security

Once installed, spyware provides adversaries with:

- **Complete access to messages, emails, and calls** of high-value targets.
- **Real-time GPS tracking** to monitor officials' movements.
- **Covert microphone and camera activation** for espionage operations.

Mitigation Strategies

- **Mandate government-approved mobile security software** for all classified personnel.
- **Disable Bluetooth and Wi-Fi in sensitive environments** when not in active use.
- **Use Faraday cages or RF-blocking enclosures** for high-security meetings.

4-Low-Cost Consumer Spy Devices

Widely available consumer surveillance devices introduce a significant new espionage threat. Malicious actors can repurpose these wireless-enabled gadgets – often designed for personal security (like nanny cams) or convenience (pens with audio recorders) – for covert surveillance in government offices, corporate boardrooms, and high-security installations. Many of these devices are challenging to detect due to their small size, camouflaged appearance, and ability to transmit

data wirelessly over Wi-Fi, Bluetooth, or cellular networks. However, anyone can purchase them through familiar online retailers.

Examples of Wireless Spy Devices

- **Wi-Fi-Enabled Hidden Cameras:** These devices stream video over Wi-Fi and look like everyday objects such as smoke detectors, USB chargers, light bulbs, and alarm clocks. They make remote surveillance easy for adversaries.
- **Bluetooth Microphones:** Miniature microphones hidden inside office supplies, furniture, or electronic devices can record and transmit audio to nearby listening posts. Some advanced models automatically activate only when voices are detected, reducing the risk of detection.
- **RFID-Based Tracking Devices:** Small RFID or GPS-based trackers can be discreetly placed in luggage, clothing, or electronic devices to monitor the movement of high-value targets. Some of these trackers operate in passive mode, requiring no power source, making them extremely difficult to locate.
- **Smart Home Devices:** Internet-connected smart plugs, voice assistants, and even smart thermostats can be compromised or pre-configured to capture audio and send it to foreign intelligence agencies.
- **Spy Pens & USB Drive Recorders:** Miniaturized recording devices disguised as office supplies or external storage devices can capture sensitive discussions without raising suspicion.

Recent Incidents & Threat Landscape

Reports indicate that foreign intelligence agencies have deployed these consumer-grade surveillance devices in:

- **Embassy Buildings:** Intelligence agencies have discovered hidden cameras and microphones in guest quarters and conference rooms used by foreign dignitaries.
- **Government Facilities:** Devices found in secure areas suggest that adversaries have successfully placed surveillance equipment within classified environments.
- **Corporate Offices:** Major multinational corporations have reported espionage attempts where adversaries used hidden microphones and smart office equipment to steal intellectual property.

The affordability and ease of access to these devices make them an increasing concern for security professionals, especially as adversaries continue to exploit the proliferation of smart homes and IoT-enabled technologies.

Mitigation Strategies

- **Deploy RF Scanners and Spectrum Analyzers:** These tools detect unauthorized radio transmissions from hidden cameras, microphones, and other wireless surveillance devices.
- **Conduct Routine Physical Security Sweeps:** Trained personnel should regularly inspect sensitive areas for concealed devices, particularly before high-level meetings.
- **Ban Unapproved Electronic Devices from Secure Locations:** Personal electronic devices, including smartphones, smartwatches, and wireless-enabled gadgets, should be prohibited in classified environments.
- **Use Signal Jamming and Shielding Technologies:** Secure rooms should incorporate RF-blocking materials to prevent unauthorized transmissions.

5-Chinese-Built Wi-Fi Routers

The widespread use of Chinese-manufactured networking hardware introduces significant cybersecurity risks to government and enterprise environments. Multiple reports from intelligence agencies and cybersecurity researchers have identified backdoors, hidden remote access capabilities, and covert data exfiltration mechanisms in routers produced by Chinese vendors. These vulnerabilities present a critical national security risk, as compromised routers could allow adversaries to conduct **mass surveillance, traffic interception, and cyberattacks** against U.S. and allied networks.

Threats Posed by Chinese-Built Wi-Fi Routers

- **Backdoors for Remote Access:** Many routers include undocumented administrative accounts, which allow adversaries to control the device remotely.
- **Data Interception & Exfiltration:** Malware embedded in router firmware can silently forward traffic to foreign intelligence agencies, compromising sensitive communications.
- **Kill-Switch Capabilities**: Researchers have discovered Chinese-manufactured router models with firmware that allows attackers to turn off entire networks remotely, posing a critical risk to national security infrastructure.
- **Firmware Updates Controlled by Foreign Entities:** Because manufacturers often control firmware updates, adversaries can deploy malicious updates to compromise networks long after the organization installs the device.
- **Botnet Recruitment:** Attackers can integrate compromised routers into large-scale botnets for distributed denial-of-service (DDoS) attacks and espionage operations.

Mitigation Strategies

- **Procure Network Hardware from Vetted, Trusted Suppliers:** Government agencies and critical infrastructure organizations should only purchase networking equipment from manufacturers with transparent security practices.
- **Conduct Firmware Integrity Checks and Audits Before Deployment:** Security teams should inspect router firmware for unauthorized modifications before integrating it into networks.
- **Implement Deep Packet Inspection (DPI) Tools:** DPI can detect anomalous outbound traffic patterns associated with covert data exfiltration.
- **Disable Unused Router Features:** Organizations should turn off remote administration, universal plug-and-play (UPnP), and other high-risk functionalities that attackers exploit.

6-WPA-2 Weaknesses

Despite the availability of WPA-3, **WPA-2 remains the most commonly used Wi-Fi security protoco**l. This widespread use makes many networks vulnerable to well-documented exploits. Attackers continue to exploit weaknesses in WPA-2 encryption, enabling them to intercept wireless traffic, steal credentials, and gain unauthorized access to enterprise and government networks.

Common WPA-2 Exploits

- **KRACK (Key Reinstallation Attack):** This attack exploits a flaw in WPA-2's four-way handshake process. Attackers can decrypt Wi-Fi traffic and intercept sensitive data, including login credentials, emails, and banking transactions.
- **PMKID Hash Retrieval Attacks:** This offline attack allows adversaries to capture WPA-2 handshake data and crack network passwords using brute force or pre-computed dictionary attacks.
- **Evil Twin Attacks:** Attackers create fake access points with the identical SSID as a legitimate network, tricking users into connecting and unknowingly transmitting their credentials.

Mitigation Strategies

- **Accelerate WPA-3 Adoption Across Government Networks:** WPA-3 provides enhanced encryption and resistance against brute-force attacks.
- **Use Enterprise-Grade Authentication Methods:** Organizations should implement 802.1X authentication with RADIUS servers to prevent unauthorized access.

- **Employ Real-Time Anomaly Detection:** AI-driven security solutions should monitor network activity for signs of WPA-2 exploitation attempts.
- **Mandate Multifactor Authentication (MFA) for Wireless Access:** This strategy reduces the risk of compromised credentials leading to network breaches.

7-Wireless Earbuds (Bluetooth) as an Espionage Vector

Wireless earbuds have unexpectedly become a powerful espionage tool. Exploiting **Bluetooth Low Energy (BLE)** vulnerabilities, attackers can remotely hijack Bluetooth connections, eavesdrop on conversations, and even manipulate devices for surveillance purposes.

How Attackers Exploit Wireless Earbuds

- **Bluetooth Hijacking:** Attackers use BLE vulnerabilities to intercept or modify audio streams.
- **Covert Audio Recording:** Attackers can use compromised earbuds to record and transmit conversations without the user's knowledge.
- **Man-in-the-Middle (MITM) Attacks:** By exploiting insecure Bluetooth connections, adversaries can inject malicious commands into paired devices, potentially activating microphones, altering settings, or accessing other connected hardware.
- **Location Tracking:** Attackers can exploit Bluetooth tracking features to monitor the physical movements of targets, exposing the location of government personnel and high-profile executives.

Real-World Threats

- **Corporate Espionage:** Wireless earbuds used in executive meetings can be compromised, allowing adversaries to eavesdrop on confidential business discussions.
- **Diplomatic Surveillance:** Governments have observed foreign intelligence agencies using Bluetooth exploits to track and monitor diplomatic personnel.
- **Military & Government Security Risks:** Adversaries can use compromised Bluetooth audio devices to exfiltrate classified discussions.

Mitigation Strategies

- **Enforce Bluetooth Restrictions in Classified Environments:** Disable Bluetooth functionality in government buildings and secure locations.

- **Ensure Firmware Updates for All Bluetooth Devices:** Many exploits target outdated firmware – regular updates help mitigate risks.
- **Deploy Wireless Intrusion Detection Systems (WIDS):** These systems can detect unauthorized Bluetooth connections and BLE attacks.
- **Use Wired Headsets in High-Security Environments:** Wired audio devices eliminate the risk of wireless interception.

Conclusion

Wireless threats continue to evolve as adversaries refine their tactics. The new administration must prioritize securing wireless infrastructure by:

- **Enhancing wireless threat intelligence and monitoring.**
- **Deploying RF spectrum analysis tools.**
- **Implementing stringent security policies for wireless use.**

The US can proactively address these threats to strengthen national security against an increasingly sophisticated cyber adversary landscape.

About Bastille

Bastille is the leader in wireless airspace defense through software-defined radio. Bastille enables enterprise security teams to assess and mitigate the risk associated with the growing number of Cellular, RF, and Wireless threats. Bastille's patented software and security sensors bring visibility to devices emitting radio signals (Wi-Fi, Cellular, Bluetooth, BLE, and other IoT communications) in your organization's airspace. Through its software-defined radio, AI, and machine learning technology, Bastille senses, identifies, and localizes threats, providing security teams the ability to accurately quantify risk and mitigate airborne threats that could pose a danger to sensitive information and network infrastructure. Learn more at www.bastille.net or follow us on LinkedIn.