Signal, QR Codes, and Nation-State Threats

Analyzing the Pentagon's Recent OPSEC Bulletin

Published by Off by One, Inc.

https://offx1.com

1. Executive Summary

In March 2025, a leaked OPSEC bulletin from the U.S. Department of Defense, later confirmed by NPR, revealed a concerning vulnerability involving the Signal Messenger app. The bulletin described malicious actors-specifically Russian APT groups-exploiting the "linked devices" feature of Signal, potentially allowing them to intercept encrypted conversations. The memo referenced "malicious QR codes" and "malicious code," hinting at either sophisticated phishing techniques or an undisclosed zero-day vulnerability.

While Signal's core encryption remains intact, the risk stems from compromised linking mechanisms and the possibility of device-level exploitation. The nature of the language used, the timing of internal Pentagon communications, and the attribution to nation-state actors suggest this is not a case of ordinary phishing, but rather the possible disclosure of an advanced cyber operation targeting high-value individuals and sensitive communications.

This report explores what we know so far, analyzes plausible attack vectors, and provides recommendations for safeguarding linked devices against both social engineering and potential software vulnerabilities.

2. Background

Signal is one of the most widely trusted encrypted messaging applications in the world, used by journalists, activists, government officials, and civilians alike. Its reputation for strong end-to-end encryption and its open-source, independently audited codebase has made it a go-to tool for secure communication.

One of Signal's core features is its "linked devices" functionality, which allows users to connect a desktop or tablet client to their mobile device. Linking is done by scanning a QR code generated on the secondary device with the main Signal app. Once linked, the secondary device can send and receive messages as if it were the primary one, with full access to message history going forward.

On March 18, 2025, a classified Pentagon-wide email surfaced warning military personnel about the misuse and abuse of this feature. The memo, later leaked and confirmed by NPR, stated that malicious QR codes were being used by Russian professional hacking groups to gain access to Signal accounts. It also referred to "malicious code" being embedded in those attacks, raising concerns beyond ordinary phishing.

This warning came in the wake of an OPSEC failure in which a journalist was mistakenly added to a Signal group chat discussing sensitive military operations, sparking a reevaluation of Signal's use for unclassified communication.

The bulletin emphasized that while Signal may be used in limited, non-sensitive contexts, it is not approved for storing or transmitting protected or non-public unclassified information. The memo specifically directed personnel to refer to DoD and NSA/CSS policy for proper application usage.

3. What We Know

On March 18, 2025, a Pentagon-wide email circulated to Department of Defense personnel warning of a vulnerability in Signal's linked device feature. The memo, titled F9T53 OPSEC SPECIAL BULLETIN: Signal Vulnerability, was marked UNCLASSIFIED//FOR OFFICIAL USE ONLY, and detailed a new threat allegedly being exploited by Russian professional hacking groups.

The bulletin describes the threat as follows:

> "The enemy is using Signal's linked device feature to spy on encrypted conversations. They achieve this through malicious QR codes or Signal group links, which when clicked or scanned, link a hostile device to a target's Signal account without the victim's knowledge."

> "This allows them to intercept messages in real time, even though the message is encrypted end-to-end."

The warning came just days after a journalist was reportedly added to a Signal group chat where military officers were discussing bombing targets in Yemen-an incident that triggered heightened OPSEC scrutiny.

Shortly after the memo circulated, NPR confirmed its authenticity in a March 25 report, and further noted that:

- The Pentagon reiterated Signal is not authorized for handling sensitive or protected information.
- The memo referred to both "malicious QR codes" and "malicious code," suggesting the attack may go beyond typical phishing or user error.
- Signal spokesperson Jun Harada responded publicly, stating that Signal had not been compromised and that users must still approve all new linked devices, framing the risk as a social engineering attack rather than a technical exploit.

No official vulnerability (CVE) has been disclosed by Signal, Google, Apple, or any major cybersecurity organization at the time of this writing. However, multiple experts have raised questions about the phrasing and tone of the Pentagon memo, noting that it could imply the use of a zero-day exploit or a yet-undisclosed vulnerability in Signal or in the device's QR/image parsing stack.

As of now, no patch has been issued by Signal, and no technical indicators of compromise have been released.

4. Threat Analysis

At the core of this incident is an ambiguity: is this just a social engineering attack using Signal's linked devices feature, or is it a more advanced, possibly nation-state-level exploit involving a zero-day vulnerability?

We evaluate two primary threat models:

Scenario A: Social Engineering / Phishing-Based Attack

In this model, the attack relies on tricking the user into scanning a malicious QR code or clicking a booby-trapped Signal group invite. If the victim accepts, they unknowingly authorize the attacker's device as a linked client.

- Mechanism: Signal requires that new linked devices be authorized by the user through a QR code scan. A phishing attempt could simulate a trusted source (e.g., fake IT support, internal group invite) to convince the target to complete the linking.
- Precedent: Similar attacks have occurred on other platforms, where attackers convince users to share MFA codes or scan QR links they shouldn't.
- Feasibility: This attack is relatively easy to execute against non-technical or complacent users.
- Limitations: It requires active user cooperation and social engineering skill. It does not compromise the app or operating system directly.

Scenario B: Exploit-Based Attack via Malicious QR Code

In this model, the QR code itself is weaponized, embedding a payload that triggers a vulnerability in the Signal app, the device's image processing stack, or its QR decoding libraries. This would allow the attacker to:

- Link a device without the user's approval, or
- Gain remote access or escalate privileges on the host device, allowing stealthy linking and full message access.

Supporting Evidence:

- The memo references both "malicious QR codes" and "malicious code", an unusual distinction if this were purely a phishing campaign.
- There is no known CVE, which is consistent with a zero-day exploit being actively used in the wild.
- The bulletin was distributed internally to military personnel, not released as a public phishing warning - indicating a more serious, possibly covert threat.
- The attribution to Russian APT groups supports the notion of a state-level campaign using advanced, possibly custom, exploits.

Technical Feasibility:

- Vulnerabilities in image parsing and QR libraries have existed before:
- CVE-2023-40889: Buffer overflow in the ZBar QR code library.
- CVE-2024-48214: Command injection via image parsing on certain Android camera stacks.
- Exploiting Signal's QR code linking logic directly would be harder due to strong sandboxing and cryptographic protections, but not impossible - especially if chained with OS-level vulnerabilities.

Conclusion of Threat Analysis

While social engineering attacks cannot be ruled out - and are always a risk - the language used in the memo, the response from the Pentagon, and the lack of CVE disclosure all point to a nation-state level campaign potentially involving an undisclosed zero-day vulnerability.

This is not a broad-based consumer threat. It appears to be a targeted operation against high-value individuals with strategic access - such as military officers, government officials, and possibly journalists.

5. Likelihood Assessment

To assess what type of attack is most likely, we evaluate both the phishing scenario and the zero-day exploit scenario using available signals from the memo, public responses, and known threat actor behaviors. This is a qualitative assessment based on threat modeling and public threat intelligence.

A. Phishing or Social Engineering-Based Attack

Probability Estimate: 30-40%

Supporting Factors:

- Signal's official response framed the attack as a user error issue - a linked device must be approved manually.

- Phishing is a common technique used by APTs because it's reliable and does not rely on undisclosed software vulnerabilities.

- Pentagon security memos may err on the side of caution in labeling even moderate threats if misuse is widespread.

Limiting Factors:

- Does not explain the phrasing "malicious code."

- Does not align with the classified or internal-only nature of the bulletin. Social engineering threats are typically disclosed more widely.

- Would require repeated success against highly trained, security-conscious personnel, which decreases the probability of mass success.

B. Zero-Day Exploit via Malicious QR Code or Image Parsing

Probability Estimate: 60-70%

Supporting Factors:

- The use of "malicious code" implies that something is being executed, not just clicked.

- QR code-based exploits have precedent, and vulnerabilities in image or QR parsing libraries are not uncommon.

- The internal military distribution of the memo - rather than public-facing alert - is a hallmark of threat containment in sensitive environments.

- Attribution to Russian APT groups and targeting of military communication channels is consistent with nation-state-grade cyber operations.

- No CVE or advisory has been issued, which is consistent with an actively exploited zero-day being investigated quietly behind the scenes.

Limiting Factors:

- No independent confirmation or technical teardown has surfaced yet.

- Signal has not issued an emergency patch or public admission of vulnerability - though this is not uncommon in zero-day incidents with national security implications.

Scenario	**Estimated Likelihood**	**Notes**
Basic Phishing / Social Engineering	30-40%	Relatively simple but unlikely to cause this level of
Zero-Day Exploit / Nation-State Attack	60-70%	Stronger match to memo language, secrecy, and A

Key Takeaway

While it's possible that some affected individuals were phished, the broader response from the Pentagon and the structure of the warning suggest a technical vulnerability is being exploited in the wild - likely through QR parsing or image handling. This points to a nation-state operation, consistent with known Russian APT tactics.

6. Implications

The incident involving Signal's linked devices feature has broad implications for a range of stakeholders - from military and intelligence professionals to journalists, activists, developers, and everyday users who rely on Signal for secure communication.

For Military and Government Personnel

- Operational Security Risk: If this is an exploit-based attack, it means encryption alone is no longer sufficient. Even using approved apps on unsecured devices could expose sensitive data if the underlying system is compromised.
- Device Trust Is Critical: The attack highlights the importance of hardware and OS integrity. If a malicious actor can gain access at the device level - especially via a zero-day - no app can guarantee security.
- Policy Shift Likely: We may see stricter controls around approved messaging platforms and a broader move toward controlled communications environments using hardened hardware and software stacks.
- Loss of Trust: Even perceived vulnerabilities - especially when confirmed by OPSEC memos - can erode confidence in tools widely used for "secure" communication.

For Journalists, Activists, and At-Risk Users

- Targeting is Now More Surgical: APTs no longer need to break encryption - they just need to insert themselves into the session using compromised devices. This is especially dangerous for reporters or dissidents who operate in hostile environments.
- QR Codes Are Now a Threat Surface: Practices like scanning shared QR codes (e.g. in group chats, protest organizing spaces) should now be treated with suspicion.
- Privacy Culture Needs Updating: Many users rely on Signal as a set-it-and-forget-it privacy tool. This incident reminds us that secure habits and operational hygiene are as important as the tool itself.

For Developers and Security Engineers

- Authentication via QR Codes Needs Rethinking: QR-based auth is elegant and user-friendly - but it's now clearly a potential attack vector. Image parsing libraries and QR decoding systems should be considered part of the security-critical surface.
- Zero Trust Principles Apply at the UX Layer: Just as we apply zero trust to networks, we may need to extend that mindset to device pairing and session creation - especially for encrypted communications platforms.

- Need for Secure Input Sanitization: This is a wake-up call for reviewing how user-scanned content is processed, not just in Signal, but across all mobile applications that allow QR-based linking or onboarding.

For Signal and Similar Apps

- Time to Re-Evaluate Device Linking UX: If it's possible to silently link a device via a zero-day, the model needs additional layers of user validation (e.g., notification of newly linked devices, physical confirmation).

- Crisis Communication Matters: Signal's initial framing of this as a phishing issue may be accurate - but if a zero-day is in play, failing to communicate it openly risks damaging trust long-term.

- Further Audits Likely: If not already underway, independent audits will likely be conducted on Signal's QR code parsing system and device linking mechanisms in the coming months.

Summary

This incident demonstrates a critical evolution in attack methodology: one where targeting the authentication layer - rather than the cryptographic layer - becomes the focal point. Whether through sophisticated social engineering or technical exploits, secure messaging platforms must now defend not only their encryption algorithms, but their session management and device onboarding processes.

Legal Disclaimer

This report is provided for informational purposes only by Off by One, Inc. The content reflects research, analysis, and opinion as of the date of publication and is subject to change. While efforts have been made to ensure accuracy, Off by One, Inc. makes no warranties, express or implied, regarding the completeness, reliability, or suitability of this report for any purpose. Use of any information contained in this document is at your own risk. Off by One, Inc. assumes no liability for any damages or losses arising from the use of this material.