Rotten Apple:

An Invasive Threat Actor Targeting Civil Society in Lebanon

SMEX

Executive Summary

The SMEX Digital Forensic Lab presents a report on a spear-phishing campaign that targeted a high profile Lebanese journalist in 2025.

The target, who wishes to remain anonymous, is a highly influential figure within the Lebanese media landscape, with decades of work as a reporter, editor, and with considerable influence shaping political and national discourse. The journalist is well connected to the Lebanese government and is considered to have influence, a network of contacts, and knowledge of political matters, which make them a high-value target.

A first phishing attack took place on May 19, 2025, through the Apple Messages app. A second wave, consisting of two separate phishing messages on WhatsApp, Meta's messaging app, took place on May 21 and 22. All of them used the same infrastructure and had the same goal of compromising the journalist's main Apple Account.

The target reached out after both of these campaigns, on May 25, 2025. Recognizing the high risk and the persistent threat, SMEX's Digital Forensics Lab (DFL) stepped in to analyze the forensic evidence, when available, of these digital attacks. The DFL established a dedicated channel of communication with the victim to provide continuous support and guide them through the necessary security protocols.

The initial attack successfully compromised the target's Apple Account and resulted in the addition of a virtual device. However, forensic evidence was limited, as the case was only shared with SMEX's team several days after the attack had taken place. The second wave of attacks was unsuccessful, but SMEX was able to capture a complete exfiltration of credentials (username, password, and two-factor authentication codes). The analysis shows that the infrastructure was identical in all instances and that the attack window was as short as ca. 30 seconds from the moment of submitting a password to the full account takeover.

SMEX's investigation uncovered a campaign characterized by technical precision and operational persistence. The threat actor demonstrated advanced capabilities including real-time interception of two-factor authentication codes, encrypted victim tracking mechanisms, and anti-forensic techniques designed to frustrate security researchers.

Collaborative information exchange with **Access Now** indicated that this attack shared infrastructure with two cases reviewed by Access Now's helpline. The Helpline collaborated with the mobile security company **Lookout** to review two phishing cases against members of civil society in Egypt investigated by the Helpline. Lookout's assessment was that the campaigns against these two individuals are likely linked to BITTER (known also as APT-C-08 and T-APT-17), a cyber espionage actor known for

targeting government, military, diplomatic, and critical infrastructure sectors mostly across South Asia, with some targets in China, Saudi Arabia, Turkey, and South America. Access Now also believes that the case investigated by SMEX is likely related to the same threat actor identified by Lookout, but more research is needed to confirm this. This threat actor has traditionally been active in South Asia, Saudi Arabia, Turkey, and South America, but our investigation suggests that this threat actor may also be active in South West Asia and North Africa.

This report documents SMEX's technical findings, details the attack infrastructure and methodologies employed, and presents SMEX's assessment of the suggestion by our colleagues at Access Now that the attack is likely related to the two cases they identified that Lookout independently attributed to BITTER. It serves as both a record of this specific campaign and a warning to civil society organizations, journalists, and political figures throughout the region: sophisticated threat actors are actively working to compromise your digital lives, and vigilance remains your most essential defense.

Key findings

- A sophisticated phishing attack successfully compromised an Apple account of a civil society member in Lebanon, successfully harvesting the victim's credentials and potentially multi-factor authentication codes through the phishing page and by attaching a virtual device to the victim's account.

- The phishing campaign included persistent attacks via iMessage/Apple Messenger and WhatsApp app over the course of X days/weeks,etc. impersonating Apple Support.

- While the main focus of this campaign appears to be Apple services, evidence suggests that other messaging platforms, namely Telegram and Signal, were also targeted.

- The methods and indicators of the attack are similar to the attacks conducted against two Egyptian civil society members identified by Access Now in their corresponding investigation. Lookout independently assesses that the hack-for-hire campaign identified by Access Now is likely tied to BITTER.

- Access Now believes that the same threat actor in their investigation is also likely behind the case identified by SMEX, based on the use of similar impersonation tactics, a common fingerprint, and the repeated use of the same attack infrastructure.

Initial attack (May 19, 2025)

The target reached out to the SMEX Digital Security Helpdesk in May 2025, suspecting their Apple Account had been hacked. They received a message from someone purporting to be a login verification service. The message, coming from the account **idapple[.]review@icloud[.]com**, indicated that a new device under the name “iPhone VMWare” had been connected to their account.

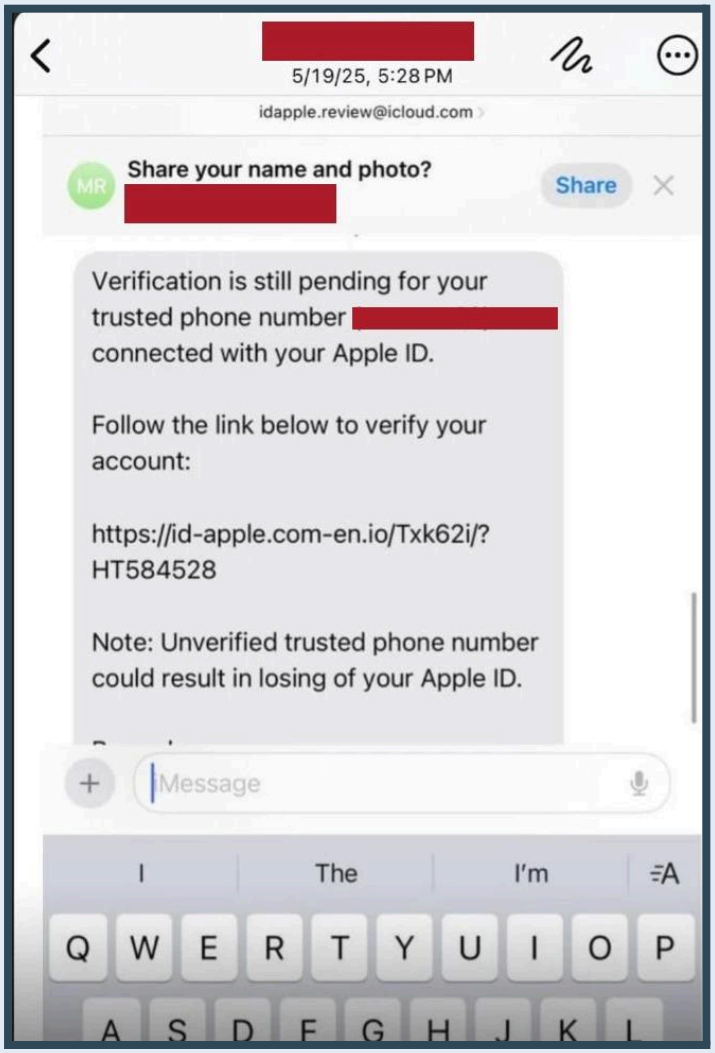

Image 1. *Initial phishing message received on May 19, 2025.*

This method of delivery and sender impersonation suggests a targeted approach, leveraging the victim’s trust in Apple's communication platforms. The core component of the attack was the malicious URL presented to the victim: **hxxps://id-apple[.]com-en[.]io/Txk62i/?HT584528**

This URL exhibits several characteristics common to sophisticated phishing domains:

1. **Brand impersonation:** it includes **id-apple** to mimic an official Apple Account page.
2. **Domain structure:** The use of **com-en[.]io** lends an air of legitimacy (purporting to refer to the English version of a site) while utilizing a non-standard Top-Level Domain (.io), which can sometimes be exploited for easier registration or evasion.
3. **Path and query parameters:** The inclusion of unique path (Txk62i) and query parameters (HT584528) suggests this might have been a tracking link, potentially tied to a specific victim or phishing campaign to monitor success rates.

Attack Outcome and Impact

The attack was successful and resulted in a significant security breach of the victim's device, including:

- **Full compromise of the victim's Apple account:** The victim's primary account was fully compromised, successfully harvesting the victim's credentials (username and password) and potentially multi-factor authentication codes through the phishing page.
- **A virtual device was attached to their Apple account:** Following the credential theft, the attacker attached a virtual device to the victim's Apple account, thereby gaining persistent access to the victim's data, synchronization capabilities, and potentially the ability to receive or intercept sensitive notifications and data in Apple's cloud services, including files, contacts, email, location, and other highly sensitive information.

Containment and Post-Incident Assessment

Upon detecting the compromise, the target took action to mitigate further damage:

- **Access termination and session revocation:** The victim forcefully terminated the attacker's active sessions and revoked any unauthorized access tokens or credentials being used. This effectively locked the attacker out of the compromised account.
- **Escalation to SMEX:** The victim contacted SMEX's Digital Safety Helpdesk approximately a week after the immediate threat was mitigated and the suspicious device labeled "iPhone VMWare" was removed from their account, their passwords changed, and other privacy related settings reviewed by SMEX's Digital Safety Helpdesk team.
- **Forensic limitations:** By the time the case was transferred to SMEX for advanced forensic investigation, the malicious link (hxxps://id-apple[.]com-en[.]io/Txk62i/?HT584528) was no longer functional. This severely limited SMEX's ability to perform immediate

forensic recovery of the attacker's infrastructure, and conduct further exploration to identify related malicious infrastructure or additional victims who might have been targeted by the same campaign.

Persistent Targeting via WhatsApp (May 21–22, 2025)

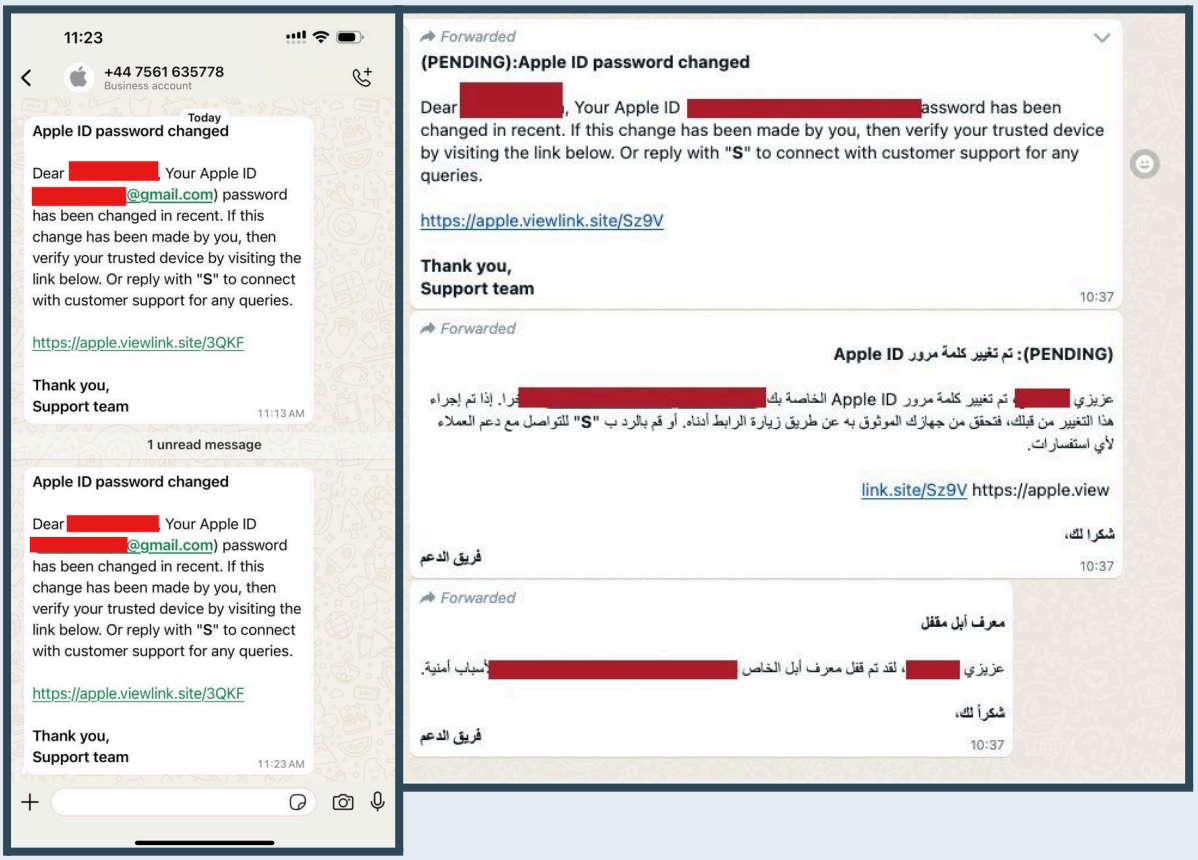

Image 2. *Phishing messages in persistent targeting (May 21 and 22, 2025)*
The victim received two new phishing messages, this time via the WhatsApp messaging app, on May 21 and 22, 2025, after containing the initial attack.

The SMEX Digital Forensics Lab (DFL) team analyzed the technical metadata of these malicious links, as well as to actively monitor their potential activation or subsequent communication attempts.

Analysis of Targeted Phishing Campaign

- **Attack vector:** The primary method of attack involved sending malicious links to targets through WhatsApp messages. This choice of delivery mechanism leverages the high trust associated with private messaging applications and the immediate nature of mobile communication. The accounts used in the attack were also

purporting to be those of the legitimate Apple services, similar to the initial campaign.

- **Targeting window:** The campaign was executed over two consecutive days, suggesting a rapid deployment and the interest of the attackers to regain access, after their previous breach had been contained.
    - **Phase 1:** May 21, 2025, identified internally as Campaign /QlwcMxhb/ (Tracking ID: **3QKF**).
    - **Phase 2:** May 22, 2025, identified internally as Campaign /x1L5cZ/ (Tracking ID: **Sz9V**).

Technical Infrastructure and Execution

- **Initial Phishing URLs:** The attackers used two distinct URLs, likely to measure effectiveness or to avoid detection by automated filtering services. Both utilized the same base domain, designed to impersonate a legitimate service through typosquatting or brand resemblance:
    - apple[.]viewlink[.]site/Sz9V
    - apple[.]viewlink[.]site/3QKF
- **Redirect Chain Analysis:** Both phishing links consistently redirected victims to a single, identical landing page designed for credential harvesting. This suggests a unified, back-end infrastructure for the two campaign phases:
    - **Redirect Target:** auth-app-le-com-user-auth-manage-service[.]mobilesite[.]co
    - This domain structure is highly indicative of a Man-in-the-Middle (MiTM) or phishing-as-a-service operation, attempting to mimic an authentication or account management portal for a high-profile technology company.

Outcome and Data Exfiltration

- The SMEX DFL team successfully intercepted and analyzed the attack traffic in a controlled environment, using Wireshark For network traffic analysis and capturing the full session data stream in a Packet Capture (PCAP) file.
- **Confirmed exfiltration:** Given our timeline intervention, and running the phishing links in our controlled environment, we were able to confirm that the campaign was effectively designed to capture highly sensitive authentication data, including username, password, and the second-factor authentication codes.

Attack Flow (30-second window):

Timestamp	Action	Data	Response
11:25:59	Password Attempt 1	1234567890	pwFailed
11:26:11	Password Attempt 2	[REDACTED]	pwSuccessCode ✓
11:26:24	2FA Attempt 1	532123	cdFailed
11:26:29	2FA Attempt 2	[REDACTED]	pwCdSuccess ✓

Domains:

Domain	Function
apple[.]viewlink[.]site	WhatsApp redirector
viewlink[.]site	Redirector parent domain
auth-app-le-com-user-auth-manage-service[.]mobilesite[.]co	Phishing kit host
mobilesite[.]co	Kit parent domain

IP Addresses:

IP	ASN/Provider	Location	Association
45.129.199.21	AS62005 BlueVPS OU	Estonia	mobilesite[.]co
85.206.166.23	Informacines sistemos ir technologijos, UAB	Lithuania	com-en[.]io

Additional findings are relevant from this process:

1. The victim's email was hardcoded in JavaScript (*var getEmFromPHP = "[REDACTED]@gmail.com")* suggesting the highly targeted nature of the attacks.
2. Password transmitted Base64-encoded via *btoa()*
3. Auto-submit on 6th 2FA digit
4. 10-year tracking cookie set on compromise: *poH3EvGCwn8YDMRz6vot* (expires 2035)
5. Anti-analysis: Hex padding (~600 lines), DevTools blocking, console hijacking, debugger traps

Elements for attribution

Infrastructure Analysis (Pivoting from Case IOCs)

The indicators of compromise we analyzed followed some observable regularities, including the structure of the query parameters, the inclusion of specific user or session identifiers, and the subdomain naming conventions, which hinted at a broader network or campaign infrastructure.

The URL in question, ***hxxps://id-apple[.]com-en[.]io/Txk62i/?HT584528***, is clearly designed to impersonate an official Apple link, using the pattern "***id-apple***." The subsequent part of the domain, "***com-en***," also presents an interesting pattern, which is feasibly purporting to mimic the language formats of a broader page, in this case English (en).

A passive DNS search for id-apple\[.\]com-en\[.\]io resolved to the IP address **85.206.166.23**. This IP address hosts several other subdomains which share the identical pattern as shown in the table below. This finding strengthens our hypothesis regarding a concerted phishing effort.

Domains	IP	Subdomains	ASN/Provider	Location
com-en[.]io	85[.]206[.]166[.]23	join-telegram[.]com-en[.]io telegram[.]com-en[.]io id-apple[.]com-en[.]io facetime[.]com-en[.]io numbers[.]com-en[.]io secure-signal[.]com-en[.]io join-fts[.]com-en[.]io	Informacines sistemos ir technologijos, UAB	Lithuania

We subsequently attempted a pivot using the parameter ***HT584528*** via URLScan, to identify any related patterns that might resemble the list of subdomains we had acquired. URLScan is a well-known platform with a substantial collection of submitted URLs. This process resulted in two additional noteworthy URLs that were publicly accessible on URLScan.

*httpx://www[.]**join-facetime**[.]**ar-id**[.]cc/Txk62i/?**HT151059***
and
*httpx://**appleid-apple**[.]**me-info**[.]io/Txk62i/?**HT151059***

We used PassiveDNS records to identify the associated IPs and subdomains as shown in the following table:

Domains	IP	Subdomains	ASN/Provider	Location
ar-id[.]cc	84[.]238[.]133[.]18	join-facetime[.]ar-id[.]cc call-join-facetime[.]ar-id[.]cc appleids-manage[.]ar-id[.]cc appleids-trusted-number[.]ar-id[.]cc encryption-sgnl[.]ar-id[.]cc j34idf[.]ar-id[.]cc mng-num-blk[.]ar-id[.]cc	Redcluster LTD	Ireland
me-info[.]cc	91[.]206[.]228[.]22	join-facetime[.]me-info[.]io num-wid[.]me-info[.]io appleid-apple[.]me-info[.]io	FlokiNET ehf	Romania

The domains found highlight a pattern suggestive of a coordinated and localized operation, which include the use of consistent naming conventions. Concretely, the initial domain under scrutiny featured the structure com-en[.]io, clearly denoting an English localization (-en). This pattern evolved in the pivoted domains, which displayed structures like ar-id[.]cc or me-info[.]cc, indicating Arabic (ar) and Middle East (me) or potentially Indonesian (id) localizations. The switch from com-**en**[.]io to **ar**-id[.]cc was a critical finding that strongly suggested a deliberate targeting and localization strategy.

In collaboration with Access Now's Digital Security Helpline, we found that similar infrastructure and campaigns had been used in other attacks. We also cross-referenced our data with publicly available threat research, including a previous ESET report which specifically documents the use of the domain com-ae[.]net within the campaign's IOCs.

This convergence of data, the domain naming patterns, the confirmed sightings by partners at Access Now, and the explicit infrastructure overlap with the ESET findings, provides substantial evidence linking the observed activity to a known, sophisticated campaign targeting users in the region.

Domains	IP	Subdomains	ASN/Provider	Location
com-ae[.]net	94[.]156[.]128[.]159	verify-apple[.]com-ae[.]net join-facetime[.]com-ae[.]net android[.]com-ae[.]net encryption-plug-in-signal[.]com-ae[.]net	Belcloud LTD	Bulgaria

We observe high consistency in the attackers' use of matching Top-Level Domain (TLD) patterns across the four distinct domains identified, suggesting a unified and centrally managed operation.

The primary and most concentrated focus of this campaign appears to be th**FaceTime** and **Apple ID**. Howe sophisticated targeting of users of Apple Services. This is evidenced by the prominent impersonation of critical Apple functionalities like ever, the scope of the operation is not limited solely to Apple users, as other related URLs seem to impersonate additional messaging and communication platforms frequently used by civil society, namely **Telegram** and **Signal**. This expansion indicates an attempt to compromise a wider range of targets and communication channels, potentially seeking sensitive information from civil society users at risk.

Pivoting Findings:

1. Domain Pattern Analysis:

- **Apple impersonation**: id-apple, apple-id, app-le-com patterns
- **Geographic TLD targeting**: *.com-en.io (Lebanon), *.com-ae.net (UAE)
- **Signal/Telegram impersonation**: signai[.]site, secure-signal[.]com-en[.]io

2. Shared Infrastructure Indicators:

- Exfiltration endpoint yPQwuCNFqDKs.php identical on both *viewlink[.]site* URLs
- Both viewlink[.]site and com-ae[.]net resolve to BlueVPS OU (AS62005)

3. Connection to Known Threat Actor:

- Domain com-ae[.]net documented in **ESET report**: "New spyware campaigns target privacy-conscious Android users in the UAE"
- IP 94.156.128.159 associated with com-ae[.]net infrastructure

Infrastructure Comparison:

Attribute	Observed Campaign (Lebanon)	ESET UAE Campaign
Domain Patterns	*.com-en.io	*.com-ae.net
Target Apps	Apple ID, Signal, Telegram	Signal, ToTok
Target Profile	Lebanese journalist figures	UAE residents, privacy-conscious users
Attack Method	iCloud credential theft + 2FA interception	Spyware distribution, account compromise
Region	SWANA (Lebanon focus)	SWANA (UAE focus)
Hosting	BlueVPS OU (Estonia)	BlueVPS OU (Estonia)

Who's the Threat Actor?

Access Now's Digital Security Helpline and SMEX believe that the Lebanese journalist case presented here corresponds to Access Now's investigations of two other spear-phishing cases against civil society in the Middle East and North Africa. Those cases have revealed a pattern of similar tactics, techniques, and procedures (TTPs) as those used here.

Based on their collaboration with Access Now, the threat intelligence team at mobile security company Lookout attributes the two attacks identified by Access Now to an Asian threat actor which uses a combination of social engineering, with highly-targeted phishing, and the delivery of malicious Android files.

Lookout's attribution of the attacks documented by Access Now to an Asian threat actor and established technical links between the threat infrastructure employed in the attacks that Access Now documented and a toolkit, which Meta documented in 2022. Access Now and Lookout also interpret the ESET ProSpy findings mentioned above as an evolution or continuation of a previous operation.

As mentioned above, Access Now reviewed our results, and both our organizations collaborated in the analysis.

Conclusion

This investigation has uncovered a sophisticated and highly targeted phishing campaign aimed at compromising the digital accounts of a high profile Lebanese journalist. While the attack was contained shortly after its initial success, this investigation provides a greater insight to the techniques and capacities of espionage actors operating in the region.

The cross analysis and collaboration between **SMEX's Digital Forensics Lab** and **Access Now's Digital Security Helpline** team suggests that this campaign is likely related to the similar campaign identified by Access Now and attributed by Lookout to **an Asian Threat Actor.**

The threat actor demonstrated advanced capabilities including real-time 2FA interception within a 30-second window, encrypted URL parameters for victim tracking, and multi-layered anti-forensic measures. The same victim was targeted on consecutive days using identical infrastructure, reflecting a determined and well-resourced operation.

Given the use of social engineering and credential harvesting in this attack, we suspect that the threat actor's incursion to Lebanon in efforts to target independent journalists and possibly civil society more broadly.

The flexible toolkit observed, which also includes Android malware, indicates an actor capable of adapting techniques to operational requirements. This investigation underscores that phishing remains a highly effective vector for compromising journalists, activists, and political figures, so we caution the community and recommend preventative measures to individuals and organizations with a high-risk profile. As threat actors like BITTER continue expanding their geographic reach and technical sophistication, vigilance, information sharing, and collective defense remain essential to protecting civil society from these evolving campaigns.

Indicators of Compromise (IOCs)

Domains

Domain	Function
id-apple[.]com-en[.]io	Apple ID phishing
apple[.]viewlink[.]site	WhatsApp redirector
viewlink[.]site	Redirector parent domain
auth-app-le-com-user-auth-manage-service[.]mobilesite[.]co	Phishing kit host
mobilesite[.]co	Kit parent domain
com-en[.]io	Parent domain (Lebanon)
join-telegram[.]com-en[.]io	Telegram phishing
telegram[.]com-en[.]io	Telegram phishing
facetime[.]com-en[.]io	FaceTime phishing
numbers[.]com-en[.]io	Apple phishing
secure-signal[.]com-en[.]io	Signal phishing
join-fts[.]com-en[.]io	FaceTime phishing
ar-id[.]cc	Parent domain (Arabic)
join-facetime[.]ar-id[.]cc	FaceTime phishing
call-join-facetime[.]ar-id[.]cc	FaceTime phishing
appleids-manage[.]ar-id[.]cc	Apple ID phishing
appleids-trusted-number[.]ar-id[.]cc	Apple ID phishing
encryption-sgnl[.]ar-id[.]cc	Signal phishing
j34idf[.]ar-id[.]cc	Unknown
mng-num-blk[.]ar-id[.]cc	Unknown
me-info[.]io	Parent domain (Middle East)
join-facetime[.]me-info[.]io	FaceTime phishing
num-wid[.]me-info[.]io	Unknown
appleid-apple[.]me-info[.]io	Apple ID phishing
com-ae[.]net	Parent domain (UAE)
verify-apple[.]com-ae[.]net	Apple ID phishing
join-facetime[.]com-ae[.]net	FaceTime phishing
android[.]com-ae[.]net	Android targeting
encryption-plug-in-signal[.]com-ae[.]net	Spyware distribution

IP Addresses

IP	ASN/Provider	Location	Associated Domain
45.129.199.21	AS62005 BlueVPS OU	Estonia	mobilesite[.]co
85.206.166.23	Informacines sistemos ir technologijos, UAB	Lithuania	com-en[.]io
84.238.133.18	Redcluster LTD	Ireland	ar-id[.]cc
91.206.228.22	FlokiNET ehf	Romania	me-info[.]io
94.156.128.159	Belcloud LTD	Bulgaria	com-ae[.]net

URLs

- hxxps://id-apple[.]com-en[.]io/Txk62i/?HT584528
- hxxps://apple[.]viewlink[.]site/Sz9V
- hxxps://apple[.]viewlink[.]site/3QKF
- hxxps://www[.]join-facetime[.]ar-id[.]cc/Txk62i/?HT151059
- hxxps://appleid-apple[.]me-info[.]io/Txk62i/?HT151059
- hxxps://encryption-plug-in-signal[.]com-ae[.]net/signal_encyption_plugin[.]apk

Hashes

Filename	SHA256
signal_encyption_plugin.apk	ef33e17f1fb4c9d3c05c5e885926aa85db3806090363805c7d26301509430240

Email Addresses

Email	Usage
idapple[.]review@icloud[.]com	iMessage phishing sender

MITRE ATT&CK Mapping

Technique ID	Technique Name	Usage
T1566.002	Spearphishing Link	WhatsApp/iMessage delivery
T1539	Steal Web Session Cookie	10-year tracking cookie
T1111	Multi-Factor Authentication Interception	Real-time 2FA relay
T1078	Valid Accounts	iCloud account takeover
T1204.001	User Execution: Malicious Link	Phishing link click