It's Probably Nothing
by Sierra Echo Charlie

EDITION 19 / 3 NOVEMBER 2026

Fake nuclear alerts, on both sides of the war

Emergency apps hijacked in Ukraine and Russia, Amadeus notifies airlines, and BITTER's PapRAT goes LOLBin.

3 stories / Listen online - 6:33

THE TAKEAWAY

The overnight lead is grim and oddly symmetrical: Ukraine's Air Alert and Russia's EMERCOM app were each compromised within hours, pushing fake radiation, chemical, missile and nuclear warnings to phones while both governments insisted the real warning systems stayed up. Attribution is still foggy, and that fog is part of the story.

01 / THE BRIEF

Both sides had their emergency alert apps hijacked on the same night

Late on 1 November, Ukraine's Air Alert app sent false warnings about radiation hazards, chemical threats, street fighting in Kyiv and an Oreshnik missile strike; around 21:00 UTC the Ukrainian Air Force said on Telegram the app had likely been compromised and stressed there was no radiation threat. One Russian-language fake message referencing Oreshnik linked to a Telegram channel tied to a previously unknown group calling itself Hitcore Corp, which claimed responsibility, though that is only a reported claim. Ajax Systems said unauthorised people interfered with the app, push notifications were disabled and restoration began by early Monday, with the threat map still temporarily off; Air Alert had 6.6 million active users as of January 2026. Hours later, Russia's EMERCOM app pushed fake warnings of nuclear strikes across all regions of Russia, referencing the P1-Sun Ukrainian drone and urging food stockpiling. The emergencies ministry confirmed a massive cyberattack around 00:30 UTC on 2 November and said normal operation returned about 90 minutes later. A Kyiv-based group calling itself DC8044 claimed it got in through the app's API and posted alleged technical details, again unverified. Both governments said the primary warning infrastructure was unaffected: sirens, SMS, TV and radio carried on, Ukraine's national warning system operated normally, and Kyiv Digital stayed functional.

Even if the serious channels stayed up, this is a direct shot at public trust in the apps people actually stare at during raids. The timing is sharp too: the Ukrainian compromise surfaced around

the same reported time a six-day Kherson ceasefire officially ended after Russia declined an extension. The Russian-language Oreshnik reference is the sort of sloppy tell that makes you raise an eyebrow, not a provenance certificate.

WORTH ASKING

If you work anywhere near public-warning or crisis-comms tooling, this is worth a quiet tabletop: supporting apps are now clearly in play, even when sirens and SMS are fine.

QUALIFICATIONS

Perpetrators are not established. A Ukrainian MP told the BBC it was almost certainly part of Russia's cyber war, Russia has not explicitly blamed Ukraine, and the Hitcore Corp and DC8044 claims remain unverified.

SOURCES

Nuclear threats and street brawls: Russia, Ukraine report attacks on their emergency alert apps - Reporting / context

Russian and Ukrainian hackers hijack emergency apps to spread fake nuclear attack warnings - Reporting / context

Emergency Alert Apps in Ukraine and Russia Reportedly Hacked to Send False Warnings - Reporting / context

02 / THE BRIEF

Amadeus breach reaches daylight and airlines start counting

On 2 November, airlines in our region began confirming they had been told by Amadeus IT Group about unauthorised access to one of its systems. Qantas said Amadeus advised the issue was contained in September, that there was no impact to Qantas's own systems or databases, and that it had notified the Australian Cyber Security Centre. Cathay Pacific, Korean Air, Asiana, Japan Airlines and ANA were also named as affected, with hotels and car-hire companies globally reportedly caught up and hundreds of travel companies impacted. In a statement quoted by 7NEWS, Amadeus said it became aware of a vulnerability affecting a travel booking display environment, that certain booking-display data was accessible through it, that there is no evidence payment or financial data was accessed, and that there are no indications it was exploited for ransomware. Cathay said Amadeus told it containment included a password reset plus enhanced monitoring and detection.

The intrusion may be old news internally, but the disclosure is new and the blast radius is very travel-industry: a shared supplier, big airlines, and customer-impact questions still unresolved. No payment data is a useful qualification, not an all-clear; booking displays sit close enough to itineraries and identities that airlines are right to start counting carefully.

WORTH ASKING

If your organisation books a lot of travel through the big carriers, keep an eye out for airline-specific notices rather than waiting for a single neat Amadeus FAQ.

QUALIFICATIONS

Whether customer information was actually breached is still under investigation and the scope of affected bookings and passengers is not established.

SOURCES

Airlines including Qantas, Cathay Pacific impacted in Amadeus cyber attack - Reporting / context

Qantas among several airlines probing data breach and customer booking impacts after Amadeus cyber attack - Reporting / context

03 / THE BRIEF

BITTER's new PapRAT does its shopping with Windows' own tools

FortiGuard Labs has attributed a South Asian espionage campaign to BITTER, also tracked as TA397, with high confidence based on lure filenames, C2 patterns, metadata and malware analysis. The report details PapRAT in C++ and Rust forms, aimed at government, energy and engineering targets in South Asia. The neatest chain is also the rudest: a malicious LNK abuses the native ftp.exe exclamation-mark command execution, then uses curl, scripts and scheduled tasks without dropping a traditional malware executable. Two other chains deliver PapRAT through MSI installers triggered from an LNK inside a VHDX image or fetched via a WebDAV URL shortcut; in the third, PapRAT also pulls down WmRAT. The Rust variant grows the command set from eight to eleven, adding PowerShell execution, sleep and clean-exit commands, moves C2 from plaintext HTTP to HTTPS, and hides the C2 address with reversed, ROT-3-shifted strings. Fortinet published IOCs including rivingtonclarks[.]com and netmansrvdns[.]com and says customers have filtering and antivirus coverage.

This is a useful reminder that living-off-the-land is not a boutique technique anymore. An infection chain built from ftp.exe, curl and scheduled tasks is designed to stroll past controls that are still waiting for a suspicious executable to clear its throat.

WORTH ASKING

If you are hunting this, look for ftp.exe exclamation-mark execution, curl or MSI activity kicked off by LNK files, VHDX or WebDAV lure handling, and odd scheduled tasks around those events.

QUALIFICATIONS

Attribution is Fortinet's high-confidence assessment rather than independent confirmation. The research is dated 2 November; Fortinet's feed metadata relays 14:00 UTC, inside the window.

SOURCES

BITTER Expands Its Arsenal with PapRAT - Primary source

BITTER Targets South Asian Organizations With PapRAT and Native Windows Tools - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.