30 January 2026

An Analytic Intelligence Wire Prepared by The Students of Embry-Riddle Aeronautical University

# Issue 487
## Of Eagle Eye Intelligence


***Authors***

Garrett Williams
Christina Muchow
Riley Callan


30 January 2026

# Issue 487
## Of Eagle Eye Intelligence

***In This Issue***

## RUSSIA: Cloud-Based Phishing Campaign Likely to Increase Malware's Resilience

**Summary**: A newly identified phishing campaign targeting Russian users will likely increase cybercriminal resilience by abusing legitimate cloud services to distribute Amnesia RAT and ransomware.

**Development**: On 24 January, cybersecurity researchers identified a multi-stage phishing campaign targeting users in Russia that delivers a remote access Trojan known as Amnesia RAT and a ransomware payload. The campaign uses phishing emails containing compressed attachments with decoy documents and malicious Windows shortcut files disguised as text files. When executed, the shortcut files initiate PowerShell commands that retrieve additional scripts and malware hosted on GitHub and Dropbox. Researchers reported that the malware enables remote access, credential theft, and data exfiltration before attempting to disable endpoint security defenses and deploy ransomware.

**Analysis**: The campaign's reliance on legitimate cloud services will likely increase the durability and scalability of similar cyber operations. Hosting malicious payloads on trusted platforms almost certainly complicates detection and response efforts, as defenders must balance security actions against the risk of disrupting legitimate services. The attack also underscores the continued effectiveness of social engineering over software exploitation, almost certainly suggesting that user behavior remains a primary vulnerability. This method will likely be adopted by additional threat actors seeking low-cost, low-visibility malware distribution mechanisms.

[Garrett Williams]

## AFGHANISTAN: Border Clashes Likely Tolerated to Prevent Domestic Insurgency

**Summary:** Kabul probably has permitted recent Islamist militant activity along the Afghanistan-Pakistan and Afghanistan-Tajikistan borders to appease the most virulent militants within its society, diverting potential domestic insurgency while maintaining plausible deniability.

**Development:** On 24 January, a suicide bomber targeted members of a peace committee in Khyber Pakhtunkhwa, a province in Northwestern Pakistan near the Afghanistan-Pakistan border, according to *Al Jazeera*. This follows repeated attacks within Pakistan and high tensions along the border, with Islamabad accusing Kabul of offering Islamist militants, most notably the Tehrik-e-Taliban Pakistan (TTP), safe harbor. On 18 January, Tajik border guards clashed with a group of Jamaat Ansarullah fighters attempting to enter the country from Afghanistan. This also follows months of border tensions, including multiple terrorist attacks within Tajikistan.

**Analysis:** Kabul is likely diverting jihadist elements within its society towards Pakistan and Tajikistan to prevent large-scale domestic insurgency. Kabul likely does not have significant direct control over the executors of these attacks and likely does not intend to use these attacks to meaningfully expand its influence; if it intended to meaningfully expand its control or cause serious damage to Islamabad and Dushanbe, it almost certainly would have used a larger contingent of its own (Afghan Taliban) fighters rather than small groups of TTP and Jamaat Ansarullah fighters. Rather, Kabul is likely harboring these terrorist groups, permitting them to use Afghanistan as a base of operations without lending significant material aid or direction, to divert active and intended militants away from counter-Taliban insurgency. By not opposing these groups, Kabul can maintain its image among radical Islamists as an ally committed to jihad, rather than an enemy to oppose. On the other hand, by not offering these groups overt public support, Kabul can maintain plausible deniability of knowledge of their activities within the country, thus preventing large-scale conflict with its neighbors and allowing it to continue to receive humanitarian aid and economic engagement from other countries.

[Christina Muchow]

## IRAN: Islamic Revolutionary Guards Corps Units Disapprove of Internet Shutdown

**Summary:** The Iranian government's decision to block internet access nationwide likely represents the first step toward disillusionment among the Islamic Revolutionary Guards Corps.

**Development:** On 8 January, the Tehran shut off Iranian internet access amid significant protests over economic decline and dissatisfaction with the regime. In June 2025, Tehran had utilized the same strategy in the 12-day war with Israel. The current shutdown is the longest and most comprehensive the country has experienced. An Islamic Revolutionary Guards Corps (IRGC) "news" telegram channel posted on 21 January amid a slight, inconsistent thaw, "Continuing the internet shutdown creates more discontent, not security." This Telegram account has criticized the regime before, including condemning the government for unclear information on lifting the restrictions. While this account is purportedly run by "fans," members of military organizations often post under "fan" or "unaffiliated" accounts maintain anonymity. The internet shut down costs the country over thirty-seven million dollars per day, according to AP. Additionally, "A confidential plan is under way to turn international internet access into a 'governmental privilege, according to Filterwatch.

**Analysis:** This dissent, likely coming from within the IRGC, could indicate early fractures in institutional loyalty among some within the Iranian system, especially as the internet takedown significantly furthers the economic crisis and IRGC members continue to directly suffer from the consequences. While "fans" of the IRGC run this account, it likely speaks directly from at least some IRGC members. Several converging pressures, such as the internet shutdown and continuing economic struggles for IRGC members, suggest conditions under which internal realignment of at least some IRGC members against the regime could become more likely. If the government permanently revokes internet access for Iranians, this would also increase the likelihood of IRGC members becoming disaffected with the regime. While current evidence does not indicate a large-scale fracture, such signs could mark the first steps of a shift in the internal balance of loyalty, especially as economic pressures deepen and the regime's coercive strategy becomes more costly to maintain. If IRGC members become more vocal in criticizing the regime, it would increase the likelihood of it defecting from the regime.

[Riley Callan]

## About GSIS

Embry-Riddle Aeronautical University's (ERAU) Bachelor of Science in Global Security & Intelligence Studies (GSIS) degree program at our Prescott Campus blends both academic and professional studies to equip students with the knowledge and skills necessary to become future leaders in intelligence, security, and law enforcement. The program provides students with a sound foundation in the liberal arts, including international relations, foreign languages and cultures, international law, foreign policy, political and military history, and other essential topics.

## About EE

Eagle Eye Intelligence (EE) is an intelligence and research organization led by the students of the GSIS program at ERAU in Prescott, Arizona.

Dr. Philip E. Jones founded EE and Embry-Riddle's GSIS program in 2002, following a career with the Central Intelligence Agency and consulting work in international development and global security. Currently, Professor Dale R. Avery, a former career intelligence analyst, serves as EE's faculty advisor.

EE strives to provide actionable intelligence and analysis to its customers during the academic year. We are driven by a number of goals – continuous development, nonpartisanship, interdisciplinary studies, global awareness, and professionalism.

EE does not cite sources in the final publication; however, we log every source we use in our research and are happy to share them upon request. The official EE Source Database is available on our website's resources page for a general overview of our sourcing methods.

The views expressed in this publication are those of the authors, and do not represent the position Embry-Riddle Aeronautical University or the College of Business, Security, and Intelligence.

Christina Muchow, a Senior in the GSIS program, currently serves as EE's Editor in Chief. For questions or comments, contact the team at editorsee@gmail.com or Professor Avery at 928.777.4708. If you use material from this publication, you should attribute: Eagle Eye Intelligence Edition 487, a publication created by students at Embry-Riddle Aeronautical University in Prescott, Arizona.



Eagle Eye Intelligence
3700 Willow Creek Rd.
Prescott, AZ 86301eagleeyeintel.com