27 September 2024

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

Issue 456
Of Eagle Eye Intelligence

Authors

Matthew Quackenbush
Brandon Greenaway
Tucker Jones

27 September 2024

Issue 456
Of Eagle Eye Intelligence

In This Issue

CHINA: Cyberespionage Discovery Likely to Intensify International Cyber Activity 1

UKRAINE: Ban of Social Media Telegram Likely to Limit Russian Surveillance Efforts 2

ISRAEL: Air Strike Campaign and Telecom Hack Likely Indicates Invasion Preparation 3

CHINA: Cyberespionage Discovery Likely to Intensify International Cyber Activity

Summary: Following similar methods as the Volt Typhoon, the new China-based "Raptor Train" attack begins a growing pattern of Beijing's covert preparation and cyberattack readiness.

Development: On 18 September, the United States Department of Justice announced the discovery and takedown of the Chinese state-sponsored hacker group Flax Typhoon's botnet campaign "Raptor Train." The Raptor Train attack remained undetected since its creation in 2021 and gave Flax Typhoon the potential to route data, commit distributed denial-of-service attacks, and transport malware. The cyberespionage endeavor mirrors the Volt Typhoon attack from earlier this year. Both attacks followed a similar formula: target and infect internet routers and other consumer devices that no longer receive protection from the manufacturer, connect the infected devices to the massive botnet, and use infected devices to disguise and deploy malware as routine traffics. The Raptor Train attack targeted mainly the United States and Taiwan; with efforts focused on military, government, private corporations, higher education, telecommunication, media outlets, and others.

Analysis: China-based hacker groups will likely continue this method of infiltration given its effectiveness at remaining undetected, ease of engaging in cyberespionage, and potential to deploy a cyberattack at a larger scale if Beijing deems necessary. China-based hacker groups will likely begin protectionary measures in effort to remain undetected by foreign authorities. Nations that fall victim to Raptor Train attack will likely focus cyber defense efforts toward uncovering and dismantling the possibility of more China-based botnet infiltrations and developing solutions that would prevent future attacks of this nature.

[Matthew Quackenbush]

UKRAINE: Ban of Social Media Telegram Likely to Limit Russian Surveillance Efforts

Summary: Kyiv's recent ban on the social media platform Telegram will likely limit Moscow's ability to conduct surveillance on Ukrainian government and military officials.

Development: On 20 September, Kyiv's National Security and Defense Council (NSDC) announced the ban on downloading or using the social media application Telegram on official devices used by government officials, military leaders, and workers in defense. The ban comes after evidence emerged of Moscow's ability to access user messaging history, including deleted messages and other personal data, according to AP News. The NSDC also stated that Moscow actively used Telegram to launch cyber-attacks, spread phishing messages and malicious software, track users' locations, and gather intelligence on Ukrainian facilities, according to The Hacker News. In response, Telegram issued a statement that it never provided any message data to any country, adding that any instance of leaked messages resulted from a compromised device, whether by confiscation or malware, according to Reuters. Ukrainian media estimates that around 75% of Ukrainians frequently use Telegram for communication and that around 72% see it as a key source of information, according to *Al Jazeera*.

Analysis: Telegram's ban will likely severely limit Moscow's ability to conduct surveillance and obtain critical information on Kyiv officials in critical sectors. Moscow will likely change its surveillance strategy by seeking alternative communication platforms, among other methods. However, Moscow will likely still utilize the app for information warfare and other misinformation campaigns due to its widespread use. The ban's exclusivity on official devices makes it highly unlikely to impact country-wide communication.

[Brandon Greenaway]

ISRAEL: Air Strike Campaign and Telecom Hack Likely Indicates Invasion Preparation

Summary: Tel Aviv struck 1,300 Hezbollah-related targets in Lebanon days after it moved troops to its border with Lebanon, along with a telecommunications company hack to instruct people to evacuate through text messages. The air strike campaign, coupled with the evacuation warnings, likely indicates a ground invasion into Lebanon.

Development: On 24 September, Tel Aviv struck 1,300 locations concerning Hezbollah's combat infrastructure. The air strike campaign led to nearly 500 deaths, marking the deadliest day in Lebanon since the 1975-90 civil war. Tel Aviv also hacked Lebanese telecom companies to send messages ordering people to evacuate southern Lebanon and the suburbs of Beirut. Israeli Prime Minister Benjamin Netanyahu gave a speech after the air strikes urging Lebanese civilians to leave southern Lebanon. The Israeli Defense Forces chief said Israel is preparing for "next phases in Lebanon." Tel Aviv and Hezbollah have been exchanging cross-border fire daily since the beginning of the Israel-Gaza. Tel Aviv moved its army's 98th Division, a unit fighting on the front lines in the Gaza Strip, to its northern border with Lebanon.

Analysis: Despite Tel Aviv exchanging daily cross-border fire with Hezbollah for nearly a year now, the magnitude of the recent strike campaign, along with the mass evacuation warning, indicates Israel is shifting its focus on its northern front with Hezbollah. Israeli air strikes on Hezbollah's infrastructure and leadership almost certainly would need completion before a successful ground campaign in Lebanon. Tel Aviv choosing to move troops from the front lines of the Gaza Strip to its northern border with Lebanon likely indicates a priority shift from Gaza to Lebanon. The concentration and casualties of civilians in the Israeli campaign in Gaza remain the primary obstacle in the campaign; if Tel Aviv decides to launch a ground invasion into Lebanon, it would likely seek to remove similar obstacles found in the invasion of Gaza.

[Tucker Jones]

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.

Sebastien Bragg, 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 456, a publication created by students at Embry-Riddle Aeronautical University in Prescott, Arizona.

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