



| Flash |

Yandex Strikes in Russia Unlikely to Impact Threat Actors

F-2026-10-19a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Threat Actor, Dark Web, Geopolitics

October 19, 2026

Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 10:00 AM (EDT) on October 19, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | Yandex Strikes in Russia Unlikely to Impact Threat Actors

| Key Findings

- Overnight on October 7–8, 2026, drone strikes almost certainly launched by Ukrainian forces struck a Yandex data center in the Ryazan Oblast of Russia. On October 9, 2026, Yandex confirmed that several data center modules were completely disabled at its Kaluga facility, and on October 11, 2026, a strike on the company's data center near Vladimir caused what Yandex described as a complete shutdown. These three sites constitute half of Yandex's six data centers.
- The data center losses caused a near-total collapse of Yandex services on October 11, 2026, with most systems still operating roughly 90 percent below baseline on October 13, 2026.
- The Yandex disruptions have likely had limited impact on ransomware and digital extortion (R&DE) threat actors. Threat actor traffic was disrupted but did not disappear; instead threat actors likely pivoted to other services to maintain their infrastructure.
- Although the strikes almost certainly caused significant disruptions to Yandex, its cloud services, and its large client base in Russia, the Ukrainian drone strikes are

very unlikely to have major impacts on Russian threat actor infrastructure or activity.

Details

Overnight on October 7–8, 2026, drone strikes almost certainly launched by Ukrainian forces struck a Yandex data center in the Ryazan Oblast of Russia, resulting in a fire at the data center in the city of Sasovo and affecting part of the Yandex.Cloud infrastructure.¹ The Sasovo site housed two of Yandex's three supercomputers; there have been no public disclosures regarding the extent of damage.² Immediately following the strikes, the status page for the Yandex.Cloud service stated that its ru-central-b region was unavailable.³

- Yandex is a Russian technology company that is often referred to as "Russia's Google." The company dominates the Russian market for email, search, and mapping services.
- It is very likely that Russian-speaking threat actors extensively use Yandex's legitimate services to establish infrastructure needed for criminal operations.

On October 9, 2026, Yandex said that "several data center modules are completely disabled"⁴ at its Kaluga facility, which was likely the result of subsequent Ukrainian drone strikes. In the early morning hours of October 11, 2026, a strike on the company's data center near Vladimir caused what Yandex deemed a "complete shutdown."⁵ The three sites—Sasovo, Kaluga, and Vladimir—constitute half of Yandex's six data centers.⁶

¹ [hXXps://www.theregister\[.\]com/off-prem/2026/10/09/ukrainian-drone-attack-takes-out-russian-datacenter/5302137](https://www.theregister.com/off-prem/2026/10/09/ukrainian-drone-attack-takes-out-russian-datacenter/5302137)

² [hXXps://meduza\[.\]io/en/feature/2026/10/08/ukraine-strikes-yandex-data-center-housing-two-of-the-company-s-supercomputers](https://meduza[.]io/en/feature/2026/10/08/ukraine-strikes-yandex-data-center-housing-two-of-the-company-s-supercomputers)

³ [hXXps://www.theregister\[.\]com/off-prem/2026/10/09/ukrainian-drone-attack-takes-out-russian-datacenter/5302137](https://www.theregister.com/off-prem/2026/10/09/ukrainian-drone-attack-takes-out-russian-datacenter/5302137)

⁴ [hXXps://www.themoscowtimes\[.\]com/2026/10/09/ukraine-drones-hit-second-yandex-data-center-in-two-days-a93927](https://www.themoscowtimes.com/2026/10/09/ukraine-drones-hit-second-yandex-data-center-in-two-days-a93927)

⁵ [hXXps://www.themoscowtimes\[.\]com/2026/10/11/russias-yandex-says-data-center-in-vladimir-shut-down-after-drone-attack-a93942](https://www.themoscowtimes.com/2026/10/11/russias-yandex-says-data-center-in-vladimir-shut-down-after-drone-attack-a93942)

⁶ [hXXps://meduza\[.\]io/en/cards/ukrainian-drone-strikes-have-plunged-russia-s-internet-into-crisis-meduza-explains-why-the-damage-has-been-so-extensive-and-why-a-full-recovery-will-likely-take-months](https://meduza[.]io/en/cards/ukrainian-drone-strikes-have-plunged-russia-s-internet-into-crisis-meduza-explains-why-the-damage-has-been-so-extensive-and-why-a-full-recovery-will-likely-take-months)

The data center losses caused a near-total collapse of Yandex services on October 11, 2026, with most systems still operating roughly 90 percent below baseline on October 13, 2026.⁷ According to Russian media, the disruption reached Yandex Pay, Mail, Disk, Go, Eats, and Yandex's voice assistant service, along with major Russian retailers and users in Kazakhstan, Kyrgyzstan, Uzbekistan, and Armenia.⁸ As of October 14, 2026, Yandex traffic was back to roughly 85 percent of normal.⁹

Lost capacity will almost certainly take longer to recover than lost service. Yandex had rehearsed the loss of one data center; after three were hit, Yandex.Cloud ran out of spare capacity. While recovery continues, Yandex has arranged for customers to temporarily move to competitor services inside Russia, because Russian data localization laws limit how much of that load can be moved abroad.¹⁰

The Yandex disruptions have likely had limited impact on R&DE threat actors. Prior to the strikes, traffic from the Yandex.Cloud network was roughly 95 percent automated, and none of it came from verified bots. After the strikes, bot traffic from that network fell about 40 percent, WordPress plugin probing fell 90 percent, and scanner traffic fell 93 percent.¹¹

However, the traffic did not disappear; it almost certainly moved to other providers. Automation aimed at one gambling site dropped to zero from Yandex.Cloud and reappeared from two other provider networks with the same JA4 TLS fingerprint, request paths, and headers. Following the strikes, Russian bot traffic aimed at gambling sites rose from 167.7 million to 170.1 million requests, an increase of 1.4 percent. (Before the strikes, Yandex.Cloud accounted for about 2 percent of Russia-origin bot requests and about 0.01 percent globally.¹²)

⁷ [hXXps://blog.cloudflare\[.\]com/yandex-outage/](https://blog.cloudflare.com/yandex-outage/)

⁸ [hXXps://www.themoscowtimes\[.\]com/2026/10/12/ukraines-strikes-on-yandex-data-centers-explained-a93953](https://www.themoscowtimes.com/2026/10/12/ukraines-strikes-on-yandex-data-centers-explained-a93953)

⁹ [hXXps://blog.cloudflare\[.\]com/yandex-outage/](https://blog.cloudflare.com/yandex-outage/)

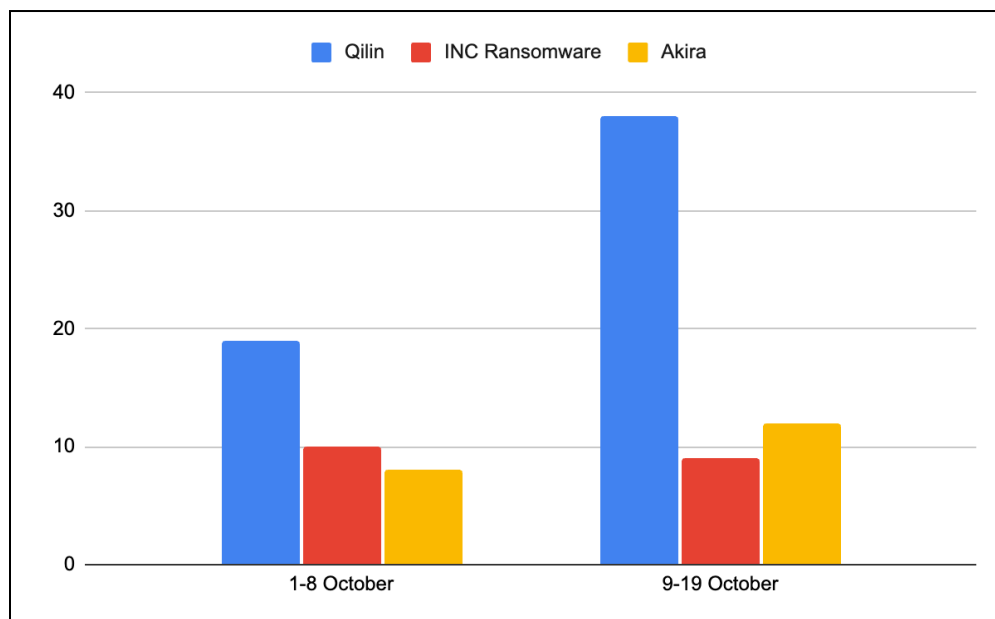
¹⁰ [hXXps://meduza\[.\]io/en/cards/ukrainian-drone-strikes-have-plunged-russia-s-internet-into-crisis-meduza-explains-why-the-damage-has-been-so-extensive-and-why-a-full-recovery-will-likely-take-months](https://meduza[.]io/en/cards/ukrainian-drone-strikes-have-plunged-russia-s-internet-into-crisis-meduza-explains-why-the-damage-has-been-so-extensive-and-why-a-full-recovery-will-likely-take-months)

¹¹ [hXXps://blog.cloudflare\[.\]com/yandex-outage/](https://blog.cloudflare.com/yandex-outage/)

¹² *Ibid.*

- A JA4 TLS fingerprint is a modern, human-readable network fingerprinting standard used to identify client software, libraries, and operating systems during a digital handshake.¹³

Ransomware leak-site analysis also shows an increase. Prior to the drone strikes, ZeroFox observed 608 victim postings across 73 groups between September 16 and October 6 (about 29 per day). Following the strikes, we saw 361 postings across 56 groups between October 8 and October 15 (about 45 per day). Likely Russian threat actors Qilin, INC Ransom, Akira, LockBit, Play, and DragonForce each posted victims between October 12 and October 15, and SafePay posted on October 12.¹⁴



Major likely Russian threat actor incidents pre- and post-strikes

Source: ZeroFox Intelligence

Although the strikes almost certainly caused significant disruptions to Yandex, its cloud services, and its extensive Russian client base, they are very unlikely to have any major impact on Russian threat actor infrastructure or activity. After the drone strikes, ZeroFox observed that nearly all major Russian threat actor activity remained at or above normal operational pace. It is almost certain that Russian threat actors will continue to operate mostly unabated throughout the reconstitution and recovery time for Yandex services.

¹³ <https://www.browserless.io/blog/tls-fingerprinting-explanation-detection-and-bypassing-it-in-playwright-and-puppeteer>

¹⁴ <https://api.ransomware.live/v2/victims/2026/10>

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%