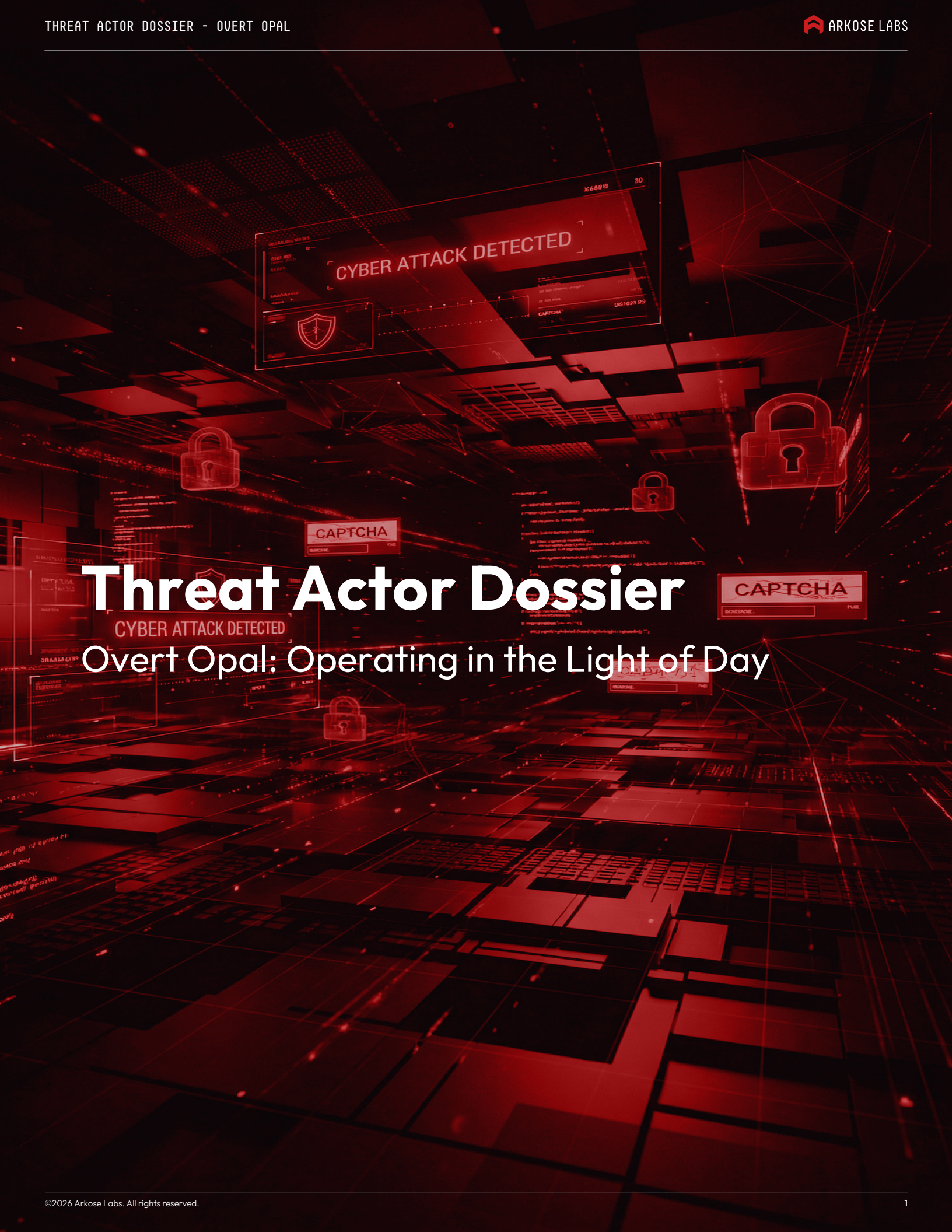

Threat Actor Dossier

Overt Opal: Operating in the Light of Day

This threat actor group provides a human-led CAPTCHA-solving service that is used by scammers and fraudsters. The Russia-based company is hiding in plain sight and can be accessed on the regular internet versus the dark web. It operates across all industries. Overt Opal pays its workers $0.50 per hour. Based on their IP addresses, we estimate that most of the workers are located in Russia, Pakistan, India and South America. Its service can be used to attack any company in any industry.

CAPTCHA solvers are used by cybercriminals to set up fake accounts to sell on the dark web or to spread disinformation. Human fraud farm activity like that of this group can be harder to spot than bot attacks, due to a lower volume of attacks that operate at a slower pace. While automated solvers use algorithms to complete the CAPTCHAs, groups like Overt Opal simply have real people using common devices. These “low and slow” attacks can blend in more seamlessly with good user traffic, compared to volumetric bots.

But signals and red flags help our team to pinpoint bad actor activity that is orchestrated using Overt Opal’s service. Attacks utilizing Overt Opal can sometimes be identified based on whether they are coming from a specific domain that isn’t associated with the company the user is transacting with. In addition, we might commonly see a long delay of around two minutes between a CAPTCHA solve and a verified token, compared with the much shorter timestamps we’d expect from genuine users.

Identity / Location

Overt Opal is a subsidiary of a well-established, Russia-based company that is a leading commercial CAPTCHA-solving service provider offering automated solutions for various types of CAPTCHA challenges. The company maintains a presence in the global market through its international platform.

- [redacted].com (Russian service)
- [redacted].com (International service)

The company deliberately obscures its physical location and jurisdiction:

- Website registered in Denver, Colo., U.S. (Domain ID: [redacted]_DOMAIN_COM-VRSN, related to VeriSign) based on the Whois records.
- TrustSploit account claimed by 'alex[redacted].com' with business registered in Russia.
- Sitejabber account claimed by ‘Mark M’ with business registration in Dubai.

Services Offered

Overt Opal provides solutions for multiple CAPTCHA types:

1. reCAPTCHA v2/v3/Enterprise
2. hCaptcha
3. Arkose Labs CAPTCHA
4. GeeTest
5. Image/text CAPTCHAs
6. Math CAPTCHAs
7. Cloudflare Turnstile
8. + 26 other types

The service provides API libraries and code examples for each supported language to help users with CAPTCHA-solving functionality.

Captcha type		Price per 1000	Solving speed	Free capacity, per minute
Image Captcha	How to Solve · Demo	$0.5 - $1	5 Sec	12,129
reCAPTCHA V2	How to Solve · Demo	$1 - $2.99	12 Sec	11,460
Arkose Labs CAPTCHA (FunCaptcha)	How to Solve	$2.99 - $50	26 Sec	1467
Geetest CAPTCHA	How to Solve · Demo	$2.99	14 Sec	4815
Cloudflare Turnstile	How to Solve · Demo	$1.45	14 Sec	3137
Amazon Captcha	How to Solve	$1.45	25 Sec	9012

Arkose Labs is the most expensive, and fewer fraud farm workers are willing to work on the Arkose Labs challenges because they are difficult to solve and, therefore, workers cannot make much money when trying to solve them.

Integrations

[redacted].com supports multiple software integrations, with hundreds of active users weekly.

- 4,500+ software applications integrated
- 300+ programs in verified catalog from 230 developers
- 1,861 weekly users for top Python package alone

Top 10 Most Used Software (Weekly Users)

- [redacted]-python PyPI - 1,861 users (Python API library)
- [redacted]-solver - 1,286 users (Chrome extension)
- Puppeteer reCAPTCHA Plugin - 518 users (Web scraping)
- [redacted]-javascript npm - 482 users (JS wrapper)
- ZennoPoster - 241 users (Bot platform, $87)
- CaptchaSolver.NET - 203 users (.NET library)
- BrowserAutomationStudio - 182 users (Free automation tool)
- Galxe-AIO - 147 users (Crypto/gaming bot)
- GSA Search Engine Ranker - 62 users (SEO tool, $99)
- Firefox reCAPTCHA Solver - 40 users (Browser addon)

Monetization

The scammer pays the third party for CAPTCHA solutions in bundles of 1,000. Many scammers use CAPTCHA-solving services as a component of a larger credential stuffing attack, which justifies the expense. For example, a scammer could test one million credentials from Pastebin — a text hosting service that stores millions of credentials attackers use for brute-force attacks — against a target site. Assuming a 1.5% successful credential reuse rate, the scammer can take over 15,000 accounts, which can all be monetized.

Overt Opal receives payment from the attacker on a per 1000 CAPTCHA basis. Services like Overt Opal then take a cut of the bid price and dole out the rest to their human workforce. Since CAPTCHA solving services are used as a solution at scale, the profits add up nicely. Even if Overt Opal only receives $1 per 1,000 CAPTCHAs solved, they net a minimum of 60 cents per bundle. The owners of these sites are often in developing countries themselves, so the seemingly low revenue is substantial.

For CAPTCHA solvers, the work is far from lucrative. Based on the metrics provided on Overt Opal's website, it's possible to calculate the following payout: Assuming it takes 6 seconds per CAPTCHA, a worker can submit 10 CAPTCHAs per minute, or 600 CAPTCHAs per hour. In an 8-hour day, that's 4,800 CAPTCHAs. Based on what was earned during our trial as an employee for Overt Opal (roughly $0.0004 per solution), this equates to US$1.92 per day. This is not a worthwhile endeavor for individuals in developed countries, but for those who live in locales where a few dollars per day can go relatively far, CAPTCHA solving services are an easy way to make money.

Pricing

Overt Opal's pricing model is based on the provider of the CAPTCHAs to be solved. At €2.80 - €50.00 (roughly US$3.19 - $56.89) per 1,000 successfully solved CAPTCHAs, solving Arkose Labs CAPTCHA tokens carries the highest price tag and largest price band. This finding indicates that our CAPTCHAs are tougher and more time-consuming to solve, thus highly effective at eating into the ROI of fraud groups. For financially motivated scammers, it's faster and easier to target companies using the cheaper CAPTCHA methods. This dramatic pricing disparity between Arkose Labs and other CAPTCHA tools shows that our CAPTCHAs are more bothersome for bots and human fraud farm workers alike, highlighting the effectiveness of Arkose MatchKey—the CAPTCHA tool of the Arkose Account Security platform—for global enterprises.

Tech Details

- Users upload CAPTCHAs via API, providing the required details (Public Key, siteURL, pageURL)
- The user receives a unique ID for tracking
- The user waits for 10-20 secs to send a response GET HTTP request to get the tokenID for a solved CAPTCHA

API Rate Limits

- 5-second minimum between requests
- 10-20 second timeout for reCAPTCHA retrieval
- No explicit concurrent request limit but throttling implemented
- ERROR_NO_SLOT_AVAILABLE indicates capacity limits

Monitoring and Analysis

In October of 2024, our team's analysis showed that very few solved CAPTCHAs from Overt Opal resulted in Arkose Labs verified sessions. As of this year, there's evidence that a small volume of CAPTCHA solves from this company could be verified in some cases, specifically in the gaming industry.

This finding follows the same pattern we've seen with other threat actor groups and underscores the persistence of cybercriminals today. After we disrupt them to near zero, groups retool and come back stronger, testing a new approach in particular sectors. As with Storm-1152, we're working to halt the criminal activities of Overt Opal once again in 2026. An analysis shows that we are in fact disrupting this second wave at significant levels.

Similar Services

During our investigation of Overt Opal, several services were identified operating on the public internet:
• SolveCaptcha.com (https://solvecaptcha.com/captcha-solver/[redacted]-bypass)

Captcha	Avg recognition time. sec.	Received %	Correctly solved %	Avg bid / 1000
Image (Picture)	12	100	73	1.00
Image (Picture) Chinese	32	98	68	1.00
Image (Picture) Russian	43	70	57	1.00
reCAPTCHA V2 Hard	52	98	98	2.99
reCAPTCHA Google	50	98	86	2.99
reCAPTCHA V2 Moderate	55	98	92	2.99
reCAPTCHA V2	2.47	100	98	2.99
reCAPTCHA V3	13	100	77	2.99
Cloudflare Turnstile	15	100	92	1.45
Cloudflare Challenge	11	100	98	1.45

SolveCaptcha accuracy for other services

- [redacted] Captcha.com (https://[redacted] captcha.com/apidoc/task-types/FunCaptchaTaskProxyless)
- [redacted].net (https://docs.[redacted].net/su-dung-api/api-giai-captcha/funcaptcha)
- [redacted] Cap (https://www.[redacted]cap.wtf/)
- Captcha[redacted] (https://captcha[redacted].ru/)

Solving Service	Avg recognition time. sec.	Received %	Correctly solved %	Avg bid / 1000
[redacted]	102	91	63	1.45
solvecaptcha solvecaptcha.com	89	95	72	3.00
DEATH BY CAPTCHA deathbycaptcha.com	0.33	100	0	0

Comparison table for different CAPTCHA solvers

These CAPTCHA-solving services employed a standardized workflow: users provided the public key, the target page URL and the siteURL (sURL). Upon successful submission of this information, the system required a 10-20 second delay before a subsequent request could be made to retrieve the generated CAPTCHA token.

Overt Opal's AI-Enabled Fraud Infrastructure

Overt Opal has evolved beyond CAPTCHA-solving services to become a sophisticated AI enablement platform for cybercriminal operations. The group now offers comprehensive dataset annotation and labeling services specifically designed to train AI/machine learning models, marketing itself as a turnkey solution for organizations requiring large-scale data preparation. While ostensibly legitimate, this AI training infrastructure directly supports the development of more sophisticated automated attack tools. By providing labeled datasets for image recognition, natural language processing and other AI applications, Overt Opal enables threat actors to create highly accurate AI/ML models capable of bypassing advanced security measures, automating social engineering attacks and scaling fraudulent operations at unprecedented levels.

For defenders, this represents a concerning evolution in the cybercrime-as-a-service ecosystem, where traditional manual bypass techniques are being supplemented and/or replaced by AI-powered automation that can adapt and learn from defensive countermeasures in real-time.

How we're working to stop fraud farm attacks

The Arkose Account Security platform presents suspicious traffic with increasingly difficult and cumbersome challenges that erode fraud-farm worker morale faster. These more onerous CAPTCHAs are served only when fraud farm activity is suspected and are designed to waste time and cost attackers money until they quit. It's effective, as seen in the statement below:

[redacted]
5d

Dear customers,
We used to keep our rates unchanged even when the load is extremely high. We always try to make sure we have enough capacity to handle the load in advance. Unfortunately, we surrender with this new Arkose Labs captcha, as sometimes it takes up to 4 minutes to bypass one single challenge. We pay our workers with the rate of 1.5 USD per 1000 solutions and they refuse to work with funcaptcha and even quit working. So we decided to change our approach starting on Monday.

In this image, workers complain because it is too hard to solve and they couldn't make any money.

bypass microsoft sign up captcha "funcaptcha" using [redacted]

Asked 8 months ago Modified 6 months ago Viewed 298 times

so i go a result when i send the request and then i tried to inject it and post and some other methods but no one worked right

Conclusion

Overt Opal is a formidable threat that enables low-skill attackers to launch sophisticated "low and slow" human fraud farm attacks at scale. By providing real people to solve CAPTCHAs for as little as $0.50 per hour, Overt Opal makes it easy and cost-effective for scammers to set up fake accounts or spread disinformation, blending in with legitimate traffic.

Although Overt Opal attacks can be harder to detect than high-volume bot attacks, there are still signals that point to their malicious activity. Telltale signs include attacks originating from unexpected domains unaffiliated with the target company, and long delays between CAPTCHA solves and verified tokens.

After being disrupted to near zero activity, Overt Opal has retooled and launched a second wave of attacks, demonstrating the persistence of today's cybercriminals. However, through careful monitoring and advanced detection techniques, Arkose Labs is once again significantly impeding Overt Opal's malicious campaigns.

As Overt Opal targets a lengthy list of companies across all industries, its human-driven fraud attacks put virtually all digital consumers at risk. Businesses must remain vigilant and adopt modern defense strategies to safeguard their websites and protect their users from becoming this threat actor's next victims.

Recommendations

1. Adopt an adaptive approach to detect and disrupt human fraud farm activity. Apply incrementally harder CAPTCHAs when signs of fraud farm traffic are detected, to waste attackers' time and deplete their resources.

2. Closely monitor user interactions for anomalies like long delays between CAPTCHA solves and token verification. Investigate sessions originating from unexpected domains unaffiliated with your business to identify potential Overt Opal attacks.

3. Leverage industry-wide intelligence sharing to proactively identify emerging Overt Opal tactics and targets. Collaborate with peer organizations and threat research teams to gain early warning of novel attack techniques and adapt defenses accordingly.

4. Counter AI with AI: Leverage advanced AI and machine learning models to detect and block Overt Opal's evolving tactics. Implement AI-powered threat detection systems that analyze behavioral patterns and contextual anomalies to spot the subtle indicators of compromise that traditional security measures might miss.

About ACTIR

The Arkose Cyber Threat Intelligence Research (ACTIR) unit is a dedicated and specialized counterintelligence team embedded in Arkose Labs. Composed of full-time experts in cyber threat analysis, digital forensics and cybersecurity operations, ACTIR's primary mission is to identify, assess and neutralize sophisticated cyber threats. By leveraging cutting-edge technologies and methodologies, ACTIR provides actionable intelligence and orchestrates coordinated responses to mitigate threats posed by entities like Veiled Marble and Greasy Opal. Recently it partnered with Microsoft DCU and law enforcement to disrupt Vietnamese threat actor group Storm-1152, twice. Through collaboration with Arkose Labs' award-winning SOC, ACTIR plays a pivotal role in enhancing the cybersecurity posture and ensuring the integrity of the digital infrastructure of Fortune 500, category leading enterprises and trailblazing businesses. Access ACTIR's threat research taxonomy.

Contact ACTIR to discuss these insights: actir@arkoselabs.com