Threat Actor Dossier

Greasy Opal: Greasing the Skids for Cybercrime

Overview

In a first, Arkose Labs' threat research unit ACTIR has revealed the details behind a Cyber Attack Enablement business that it has dubbed Greasy Opal based on its threat research taxonomy.

Greasy Opal is an alleged Cyber Attack Enablement business selling products and solutions to a wide spectrum of customers, including bad actors and competing CAPTCHA-solving services. Given Greasy Opal's ability to quickly create reliable machine-learning models for each new type of CAPTCHA challenge, it poses a significant threat in the cybersecurity landscape. Based on public records, Greasy Opal has been operating out of the Czech Republic since 2009.

Greasy Opal is not an attacker per se, but a business that provides attackers the tools with which they can quickly launch massive bot-led attacks with the goal of doing harm. Greasy Opal, thereby, "greases the skids" for cybercrime.

ACTIR has observed that individual attackers using Greasy Opal are launching volumetric, brute force bot attacks, trying to penetrate genuine consumers' digital accounts at sign-in and to set up fake new accounts. Greasy Opal, and other cyberattack enablers, are catalysts for the continuing rise of sophisticated cybercrime globally.

> Greasy Opal is an enabling tool for all kinds of attacks of varying degrees of maliciousness, like credential stuffing, mass fake account creation, social media spam, etc.
>
> **— ACTIR threat researcher**

Greasy Opal Emerges

ACTIR first observed Greasy Opal tools being used to attack Arkose Labs' customers. It's a low-cost, highly efficient solution for bad actors who seek to bypass enterprises' and government agencies' account security measures through bot-led CAPTCHA solving at scale. A comprehensive list of high-risk targets, including government institutions and organizations, is included in the appendix.

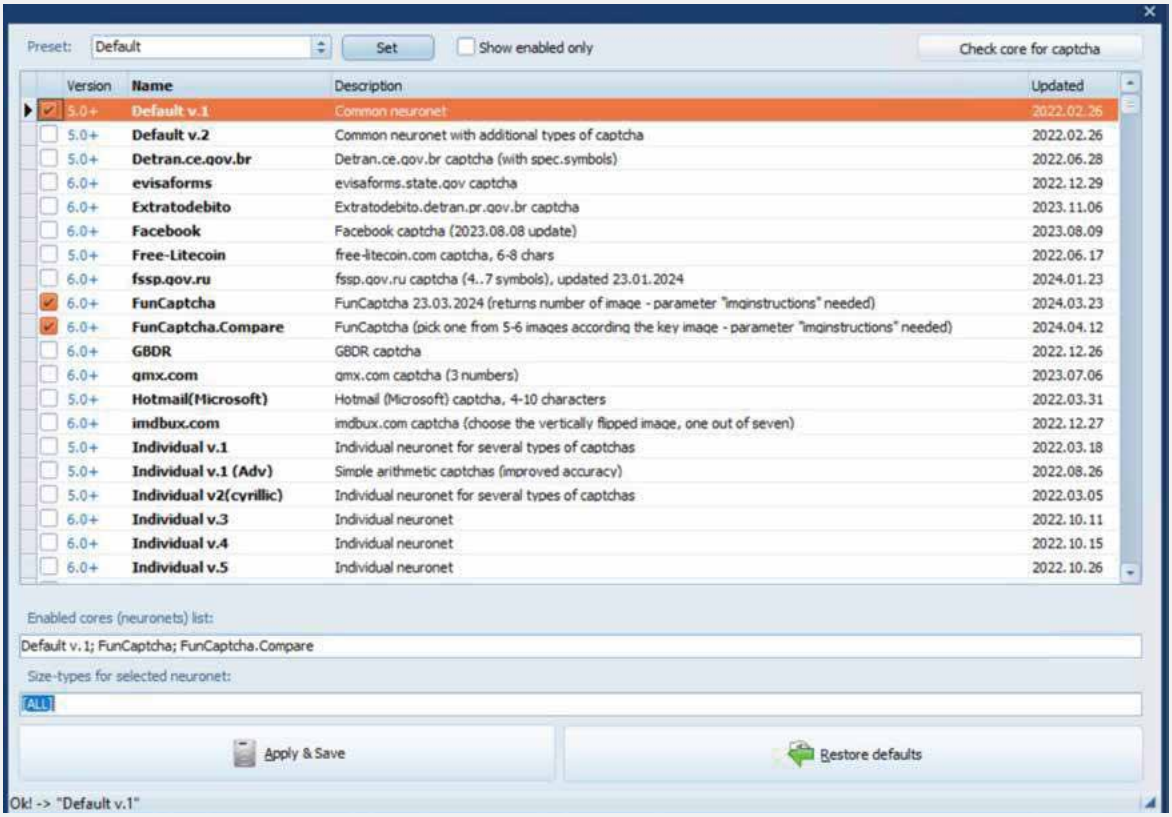

Image 1: This screenshot shows a list of bot protection sources. Greasy Opal developed its software to solve the CAPTCHAs used by these sources to detect and stop volumetric attacks. (See a more exhaustive list in the appendix that includes the government agencies that Greasy Opal targets). *FunCaptcha = Arkose Labs.

It emerges as a notably easy, fast and flexible tool for the automatic recognition of a wide array of CAPTCHAs.

Greasy Opal positions its service as enhancing recognition velocity significantly (up to 10 times faster) and is therefore a replacement for competitive CAPTCHA-solving solutions like:

1. AntiGate (Anti-Captcha)
2. RuCaptcha
3. DeCaptcher

Greasy Opal has built a thriving conglomerate of multi-faceted businesses, offering not only CAPTCHA-solving services but also SEO-boosting software and social media automation services that are often used for spam, which could be a precursor for malware delivery. This threat actor group reflects a growing trend of businesses operating in a gray zone, while its products and services have been used for illegal activities downstream.

Additionally, Greasy Opal has built a business around offering tools that can facilitate malicious activities, as many of its services are based on attacking other platforms and can be thought of as an “attacker’s toolkit,” enabling adversaries to deploy harmful sophisticated bots efficiently and effectively.

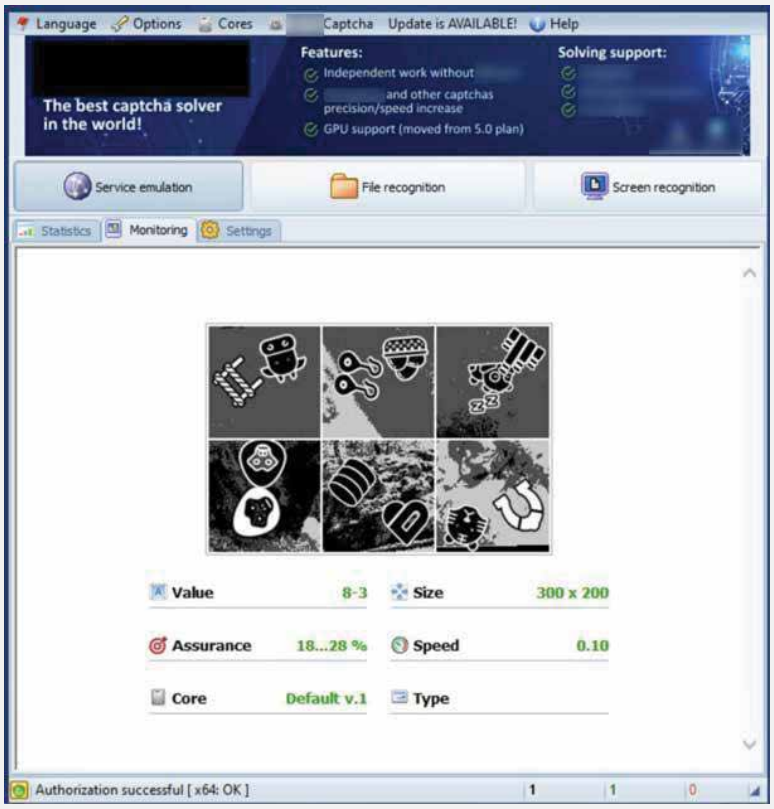

Image 2: This is a screenshot of Greasy Opal’s primary tool that uses image recognition and ML to attempt to solve CAPTCHAs that have been deployed to protect consumers’ online accounts.

Hundreds of individual attackers are using Greasy Opal software to build bots and stage volumetric attacks. For example, ACTIR researchers observed that Vietnam-based Storm-1152 used Greasy Opal in conjunction with attacks that created 750 million fake Microsoft accounts.

The Microsoft Digital Crimes Unit, using threat intelligence from the ACTIR unit, seized control of the Storm-1152 domains first in December 2023. ACTIR discovered that Storm-1152 reconstituted in January 2024 and the unit worked with Microsoft to disrupt the threat actors again in early August 2024.

> If every user of Greasy Opal's malicious software sends 10 attacks a day, when multiplied by the threat actor's entire customer base, that's a very large attack surface. Now, consider this: If each attack makes tens of thousands of attempts at account login or account creation, that's a massive potential impact on an enterprise. This scenario is what enterprises around the world are dealing with daily.
>
> **— ACTIR threat researcher**

Pricing

These types of businesses are gateways to cybercrime and are very lucrative. They operate in a gray area where they have a volume of customers, thus can price at a lower amount. As of this writing, attackers can purchase Greasy Opal's toolkit for US$70. For an additional US$100 customers can upgrade to get the beta version.

Regardless of the version, Greasy Opal requires customers to pay an additional US$10 per month as a subscriber fee. It also offers a package that bundles all of its tools, costing US$190 plus the US$10 for the subscription.

ACTIR researchers estimate that Greasy Opal's revenues for 2023 were at least US$1.7 million.

Additional Information

ACTIR has observed that Greasy Opal serves as an important toolkit in the broader ecosystem of browser automation. Notably it is used by Bablesoft's Browser Automation Suite (BAS), which is a tool that provides fingerprint (FP) databases and a drag and drop interface to create and launch attacks, reducing the skill level needed by attackers.

> When Greasy Opal and BAS are used together, malicious actors' skill level can be pretty low to deploy a successful attack.
>
> **— ACTIR threat researcher**

ACTIR engagement includes tracking these software and codebases, gathering 70,000 fingerprints for evaluation, testing against Greasy Opal to reduce information or pattern leaks, and enhancing CAPTCHA defenses.

ACTIR has observed Greasy Opal tools being used to facilitate varying degrees of attacks, from benign to serious. Greasy Opal's tools are being used to attack many industries with the latest focus specifically targeting:

1. Social media companies
2. Forums (message boards)
3. Gaming companies
4. Banks
5. Gig economy companies

Technology and Features

Greasy Opal utilizes advanced optical character recognition (OCR) technology coupled with sophisticated machine-learning algorithms to solve with high accuracy text CAPTCHAs in general, and more focused tools for other specific popular text CAPTCHAs. It provides software that attackers use to circumvent common antibot measures when developing their bots.

Key Features

- **Advanced OCR Technology:** Greasy Opal employs cutting-edge OCR technology to effectively analyze and interpret text-based CAPTCHAs, even those distorted or obscured by noise, rotation, or occlusion.
- **Machine-Learning Models:** The service develops machine-learning algorithms trained on extensive datasets of images. This training allows for continuous learning and adaptation, enhancing Greasy Opal's capability to solve new CAPTCHA variations.
- **Crowd-Sourced Labeling:** A notable aspect of Greasy Opal's operation is its use of crowd-sourced labeling for training its machine-learning models. This involves the collection and human annotation of a vast number of images, which are then used to improve the accuracy of the models.

Greasy Opal is known for its regular updates, which enhance its machine-learning models and allow for the quick adaptation to new types of CAPTCHAs.

Impact and Abatement

ACTIR is currently abating Greasy Opal tools in many ways, like new AI-resistant CAPTCHAs.

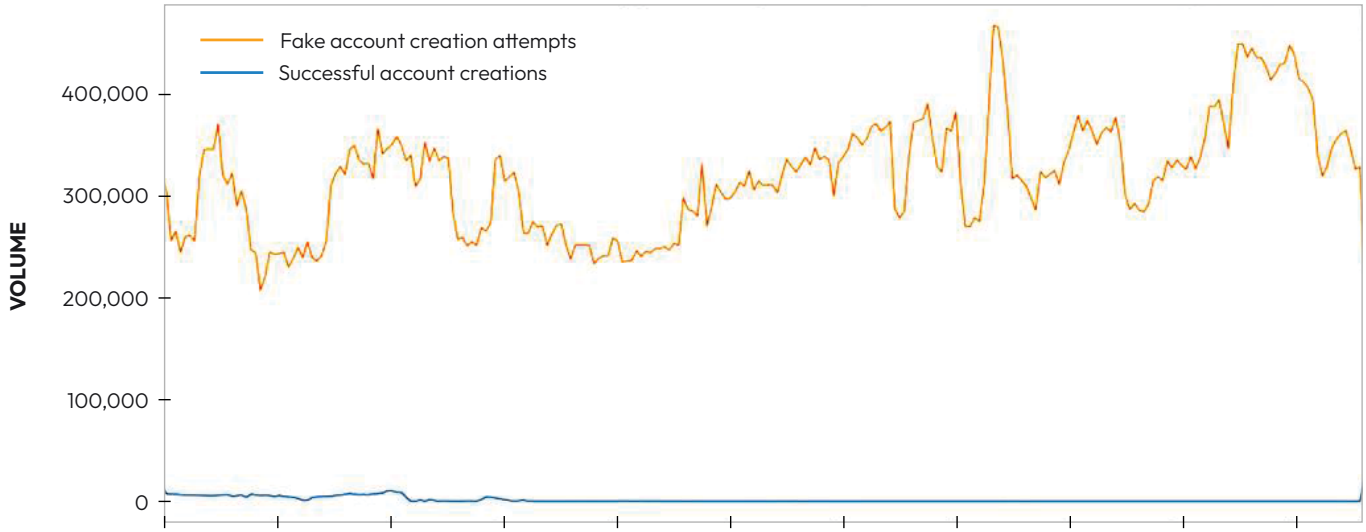

Chart 1

Chart 1 visualizes an ongoing, but unsuccessful, attack on an Arkose Labs customer. It illustrates the effectiveness of AI-based mitigation strategies, like presenting targeted challenges that escalate in difficulty, against a high volume of malicious traffic perpetrated by Greasy Opal's customers. Unlike sudden spikes, this attack presents a constant flow, underscoring the persistent threat landscape enterprises face today.

Monitoring and Analysis

ACTIR is actively monitoring Greasy Opal. These efforts include conducting experiments to understand how Greasy Opal's ML models work and how it is training them. ACTIR is looking for weaknesses in Greasy Opal's ML models that can be used to identify or mitigate when these models are being used.

Conclusion

Greasy Opal is a group bringing technology usable for cyberattacks to the masses. Its sophisticated use of OCR and AI, combined with its approach to model training through crowd-sourced labeling, positions it as a formidable cyber attack enabler tool in the hands of malicious actors.

If your company finds its name on the list in Image 1 or on the comprehensive list in the Appendix, there is a likelihood that Greasy Opal's tools are enabling attacks on your company. Companies should ensure that their bot management security stack is robust, including proof-of-work solutions and modern CAPTCHA challenges as well as AI-resistant challenges that feature anti-ML techniques.

Greasy Opal's AI-built bots solve traditional CAPTCHAs inexpensively, which is important to financially motivated attackers. Greasy Opal bots are very efficient, but they do have an Achilles Heel: Its bot technology doesn't scale well because it is CPU-based not GPU-based. This limitation in scalability arises from the inherently lower parallel processing power of CPUs compared to GPUs, leading to slower data processing and reduced efficiency in handling large-scale bot attacks. Consequently, the system's vulnerability is exacerbated by its reliance on outdated hardware architecture, making it more susceptible to being stopped by advanced countermeasures designed to exploit this weakness.

Greasy Opal's tools are cheap and accessible because they are sold as a product (go to a website and buy). Attackers don't need high-end server hardware to run these tools. The fact that it has a large number of buyers reflects that Greasy Opal's tools are a threat, and security teams need to stay vigilant to detect and stop attacks using these tools.

About ACTIR

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 Greasy Opal. Recently it partnered with Microsoft DCU and law enforcement to disrupt Vietnamese threat actor group Storm-1152. Through collaboration with Arkose Lab's 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 here.

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

Media Contact

Cassie Stevenson
Arkose Labs
Director of Brand and Communications
c.stevenson@arkoselabs.com

APPENDIX

This is a comprehensive list of websites that Greasy Opal supports to assist attackers. For example, if an attacker wanted to attack the Russian electronic passport service, Greasy Opal software would assist them in bypassing protections.

High Risk List (Government Institutions and Organizations)

detran.ce.gov.br
Secretary of Infrastructure (Brazil)

evisaforms.state.gov
USA Bureau of Consular Affairs
(Embassy appointment portal)

extradebito.detran.pr.gov.br
Brazil Vehicle search

fssp.gov.ru
Russia Federal Bailiff Service

portal.elpts.ru
Russia Electronic Passport
Service

kad.arbitr.ru
Russia Federal Arbitration
Courts Service

service.nalog.ru
Russian Tax Service

es.pfrf.ru
Social fund of Russia

eaisto.gibdd.ru
Russia State TrafÏc Service

ve.cbr.ir
Russian Marriage Loan Service

ipva.sefin.ro.gov.br
Russia State Secretary of Finance

rnis.mos.ru / transport.mos.ru
Moscow Unified Navigation and
Information System

All Supported List

Detran.ce.gov.br
evisaforms.state.gov
extradebito.detran.pr.gov.br
Facebook Captcha
free-Litecoin.com
fssp.gov.ru
funcaptcha
GDBR Captcha
gmx.com and portal.elpts.ru
Hotmail Captcha
imdbux.com
Joomla Captcha
kad.arbitr.ru
1gabba.net
liteking.io
service.nalog.ru
nanogames.io
nfprompt.io
esale.ikd.ir
OK.ru
pennyearner.com
playserver.in.th
Rambnler
RosReestr
B2C.passport.rt.ru
seo-fast.ru
SolveMedia
Steam
es.pfrf.ru
traf-hub.ru
Vkontakte
WhatsApp
WorldOfTanks
Xtremetop100.com
nyyaanimail.com
Yandex.ru
basetools.sk
bidencash.asia
capthap.online
crbot
eaisto.gibdd.ru
ve.cbr.ir
ipva.sefin.ro.gov.br
joblab.ru
kdmid
meteex.com
mv
Pars2024
rnis.mos.ru
sicmt.ru
transport.mos.ru
2krn.cc
Amazon
Apple.com
Avito
bagi.co.in
Blacksprut
Bradesco.com.br
cinematic.net
cryptowin.io
csgo2.run
farpost.ru
qarena.sq
m3qa.at
NNSM
9olx
SocPublic.com