ACTIR Unit Threat Research Taxonomy

Creating a threat research taxonomy achieves five goals:

1. Creates a coherent vocabulary to enable understanding of various cyber menaces.
2. Stimulates and simplifies knowledge sharing within the threat intelligence community.
3. Advances the effectiveness of threat intelligence analysis.
4. Informs proper countermeasures and aids in the meaningful comparison of corrective strategies.
5. Facilitates clear communication with the broader world.

The ACTIR (Arkose Cyber Threat Intelligence Research) Unit has created this taxonomy for specific types of cybersecurity threats: those that are volumetric and automated and those that are low-and-slow.

Volumetric attacks typically involve a malicious bot, which is a software application that operates autonomously and is created by a cybercriminal to do harm. Low-and-slow attacks, however, tend to be deployed by human fraud farms and are more manual in nature.

We consider bots in two categories and define them as:

1. Bots: Limited bots that perform simple, repetitive tasks.

2. Advanced Bots: Bots capable of complex, context-aware interactions.

Low-and-slow attacks are still viable despite today's automated digital work.

Human fraud farms tend to conduct manual attacks and are defined as: Organized networks, powered by coerced labor or work-from-home employees in low-wage areas. They often operate in conjunction with automation, with humans taking on the automation-resistant tasks like solving challenges.

ACTIR has observed a new attack delivery method emerging: mobile device farms. They are defined as: Different from human fraud farms, attackers are setting up and using mobile devices to generate fingerprints and solve sessions. ACTIR has observed the use of mobile device farms primarily emanating out of China.

Attacks delivered with the combined use of bots and human fraud farms and/or mobile device farms are considered hybrid.

ACTIR categorizes the threat actors it observes into three categories based on their technical expertise. Given the nature of cybercrime, all threat actors have some level of technical skill. The attacker profiles are defined as follows:

1. **Amateur:** An adversary who primarily depends on pre-existing tools to perform attacks. They have enough technical skillsto fiddle with coding, and may be willing to make a moderate time investment as long as it's profitable. Typically, if amateurs encounter resistance, they tend to move on to other endeavors.

2. **Professional:** An adversary who views attacking as their career and main source of personal wealth creation. Professionals have strong developer skills and thrive on innovating new attack methods. Typically, professionals operate within the CaaS business model (defined below).

3. **Maverick:** An adversary who tends to be quite technically skilled, but is motivated by ego or is operating on a whim. They thrive on experimentation and testing the bounds of what they can get away with. Mavericks tend to be creative and persistent.

Over the years, a robust cybercrime economy has emerged, shadowing the legitimate global economy. Many adversaries consider their cybercrime efforts as their primary careers and their path toward personal wealth creation. This taxonomy, therefore, focuses on classifying financially motivated adversaries instead of nation-state attackers, while acknowledging nation state attacks as a separate "business model" (see more below).

ACTIR has identified and defined four cybercrime "business models." The consistent characteristics that link these models together is that they attack consumers' digital accounts and use automated bots.

1. **Cybercrime-as-a-Service:** A fully outsourced entity* that generates revenue from bad actors who purchase a subscription for use of the service. Similar to a peer-to-peer (P2P) model, CaaS is an attacker-to-attacker (A2A) model. The founders of CaaS entities tend to be entrepreneurial in nature.

   A CaaS entity provides a hosted software platform that either (1) can be used to actively engage in criminal attacks on their subscribers' behalf, or (2) provides an enabling service (e.g. circumventing security measures like SMS verification or bot detection) assisting subscribers with their own attacks. Notable examples include: credential stuffing platforms, scraping platforms, Phishing-as-a-Service, CAPTCHA solving services and the deployment of fraud farm services.

   This business model also includes bulk sellers accommodating non-technical offenders with readymade tools, like credential stuffing bots, scraper bots, sniper/scalper bots, scripts and tokens.

   CaaS businesses are just as likely to be found on the legitimate internet as they are to be found on the dark web.

2. **Direct Attack Model:** Cybercriminals who purchase CaaS subscriptions and then use the service platforms to design and deploy their own automated attacks to earn money. This business model enables bad actors to attack enterprises directly without having to spend time developing the underlying technology to attack. This is a popular model because it speeds up attackers' time-to-attack metric.

*Of note, some of these platforms were built and are used for legitimate purposes, but bad actors are using them for illicit purposes without the platform owner realizing it.

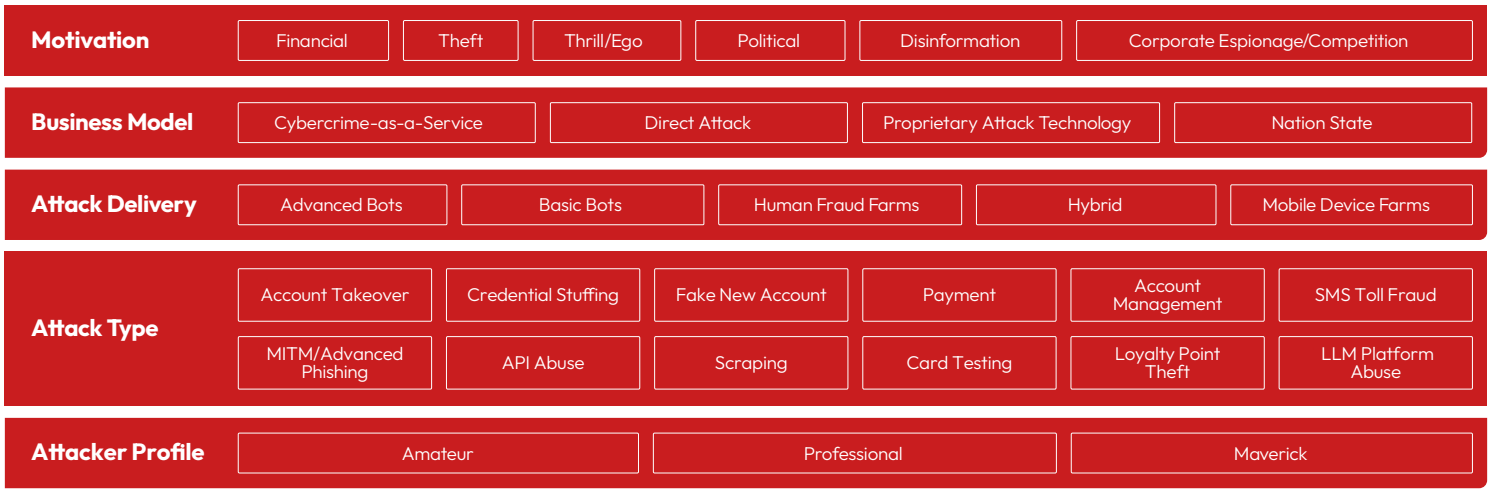
3. **Proprietary Attack Technology Model:** Cybercriminals who are attempting to build a dynasty by operating a vertically integrated enterprise. They develop the necessary technology and deploy their own automated attacks and/or run their own fraud farms. This business model also includes entities with two revenue streams: cybercriminals who develop their own tools and use those tools to deploy their own attacks to make money; they then sell a CaaS subscription so that other attackers can also use their proprietary tools to attack.

   This model enables the cybercriminal to make money by attacking enterprises themselves and by selling their attack tools/services to other cybercriminals.

4. **Nation State Model:** This model is not meant to generate revenue, but instead to influence elections, take down a country's critical infrastructure, to disrupt non-governmental organizations and cause chaos, and gain national secrets through espionage.

We recognize that cybercriminals operate fluidly and that they may switch between these four models at any given time, as that occurs ACTIR will report on that movement.

The below taxonomy is a framework, which enables enterprises to articulate their risk concerns and security priorities.



Our threat actor naming construct is aligned to the rock formations indigenous to Australia, where Arkose Labs was founded. The threat actors are then given an adjective that reflects a characteristic, behavioral pattern, or TTPs distinct to that threat actor. The complexity and ubiquity of automated, human fraud farms, mobile device farms and hybrid attacks is escalating, driving the need to articulate how ACTIR communicates insights about these threats so that we can empower our customers quickly, clearly, and without a shadow of doubt. As a result of this construct, cybersecurity professionals will know immediately the type of adversary they are up against simply by reading the two-word name assigned to an attacker or cybercrime gang.

Business Model (Type of Entity)	Family Name
Cybercrime-as-a-Service	 Marble
Direct Attack	 Shale
Proprietary Attack Technology	 Ironstone
Nation State	 Basalt

An example of this naming convention is: ACTIR first observed the threat actor group Boomerang Marble two years ago and shut it down. A determined group, it has returned with a whole new set of tactics.

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 naferious entities. Recently it partnered with Microsoft DCU and law enforcement to disrupt alleged 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.

BOOK A DEMO

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.