GLOBAL CYBER RISK SERVICES

Countering Threats to Online Social Network Content Ecosystems

As counter threat efforts mature, OSNs can further tune instrumentation and tools to improve detection of malicious activity and the subsequent defense of the ecosystem.

Online Social Networks (OSN) face a myriad of threats to the integrity and quality of the experience of stakeholders like users, developers, page admins, advertisers, and businesses. These threats seek to leverage the scale and trust built into the OSN to manipulate stakeholders in order to achieve an adversary's specific end state. Often that end state is financial in nature, with illicit profits originating from imposter brands, malicious or fraudulent advertising, pump-and-dump stock manipulation, malware, or identity theft, among others. In other situations, it's the propagation of fake news, negative word-of-mouth campaigns, or other influence operations. As stakeholders become cognizant of that fraud and manipulation, it erodes trust in the ecosystem of digital content cultivated by the OSN.

The breakdown of stakeholders' trust represents a significant business risk to the OSN, while failing to prevent fraudulent or discriminatory promoted content introduces possible regulatory and legal risk. OSNs are further challenged by a globally diverse user base representing unique geopolitical considerations and additional risk to the OSN. As such, OSNs are keen to continually identify solutions that counter nefarious actors within their ecosystem.

Each threat has a sequence of actions that must be executed in order to launch a successful attack against the OSN. Understanding the characteristics of a threat such as the desired end state of the adversary, the anatomy of a successful attack, and threat actors' capabilities and tactics, creates opportunity to define indicators of attack (IOA) and allows the OSN to detail and prioritize each adversary Course of Action (COA). An IOA is a representation of the dynamic execution of those COAs. IOAs, when taken in conjunction with indicators of compromise (IOC), can facilitate machine-based search and automated interdiction of threat actors within the ecosystem.

A machine-based solution that can scale at the speed with which information travels requires more than crowdsourced dispute flagging and pedestrian threat intelligence databases of IOCs. For instance, in order for attacks to succeed at scale, one can assume that a significant percentage of activity associated with the staging and execution of attacks is batched. The nature of batching introduces potential overlap that can be identified at multiple points in the sequence of an attack, both during (IOA) and after (IOC). An effective solution will map these action sequences and identify the various modalities that can be used to determine a legitimate user or account interaction from that of malicious threat actors. Modalities can include: Naming Conventions, Location, Time, IP, ASN, Language, Currency, Patterns, Frequency, Domains, Hashtags, Sentiment, Linked Sources, and Images. Artifacts (i.e. IOCs) can bolster the relative confidence that a particular sequence of events is representative of the staging or execution of an attack. The sheer number of potential relevant modalities that OSNs have access to within their dataset creates a unique hindrance to the defense of their ecosystem; that is, how to articulate the threat in a meaningful way that enables a scalable, automated response to said threat.

Historically, methods to detect and defend against malicious activity on OSNs have relied on the identification of static IOCs and time-consuming investigation to determine that an event is malicious. These piecemeal methods of detection traditionally address threats in isolation and fail to incorporate information available to the OSN in a holistic and meaningful way. Instead, OSNs should create a Counter Threat Fusion Cell to coordinate and focus threat collection, analysis, and subsequent interdiction efforts within their ecosystem.

Fusion cells represent a paradigm shift in that traditional intelligence efforts supporting development of countermeasures are solely focused on the adversary via multiple channels of understanding, whereas a fusion cell eliminates silos and barriers to provide understanding of the entire ecosystem. Fusion cells enable a spectrum of behavior to be developed and enable the holistic integration of data from throughout the OSN that facilitates a more valid understanding of the various stakeholders and threat actors' behavior within the ecosystem. The fusion cell must then sufficiently evaluate the adversary in order to define accurate models that include consideration of the threat actor's patterns of operation, capabilities, and tactics so as to develop accurate adversary COAs. It is this understanding that eliminates uncertainty and facilitates the development of a playbook of countermeasures that can scale across the OSN's ecosystem to address the different threats it encounters.

The remaining challenge for OSNs is to represent these characteristics algorithmically and to apply them holistically across the network without introducing bias. The counter threat fusion cell enables OSNs to focus efforts to process data, analyze, and consume relevant intelligence. The development of technical tools by internal stakeholders to combat fraud and other malicious activity should be guided and focused by counter threat fusion cell products. It's very important that a dialogue exists between operations teams that are implementing solutions and those that are developing and prioritizing adversary COAs; this is a primary benefit of the fusion cell. This feedback loop enables gaps in capabilities and new requirements to be identified and communicated. As counter threat efforts mature, OSNs can further tune instrumentation and tools to improve detection of malicious activity and the subsequent defense of the ecosystem.

OSNs are uniquely positioned to implement new and exciting methodologies and technology to detect and defend stakeholders from fraud and abuse. The sheer scale of data available and the ability to drive bleeding edge enhancements to the user experience enables OSNs to continuously iterate solutions at scale and mature capabilities that facilitate machine-based search and automated interdiction of threat actors within the ecosystem. The creation of a counter threat fusion cell is a cogent opportunity for OSNs to drive focused, holistic engagement internally, minimizing excessive or unproductive development efforts while ensuring a high-quality experience built on trust with stakeholders. In doing so, the OSN reduces the cost of ongoing counter threat efforts, improves efficacy of business development and increases adoption among stakeholders, and reduces risk to the business through a precise understanding of the identities of actors within the ecosystem and enhanced awareness of various regulatory pitfalls.

Contact Us

Global Cyber Risk Services
+1 212 763 1958 (New York)
+1 202 688 4280 (Washington, D.C.)
gcrs@alvarezandmarsal.com

Alvarez & Marsal (A&M) brings a deep operational heritage and hands-on approach to delivering cybersecurity solutions that create sustainable operational, regulatory, and financial results. The A&M GCRS team has extensive experience in designing, developing, and implementing effective and sustainable programs founded on industry and regulatory experience. Our team has decades of government and private sector experience, which includes defending individuals, companies, and nations against the most sophisticated cyber adversaries. We work as advisors, interim leaders, and partners who will not only tell you what you need to know, but will work side by side with you to achieve your objectives.

ABOUT ALVAREZ & MARSAL

Companies, investors and government entities around the world turn to Alvarez & Marsal (A&M) when conventional approaches are not enough to make change and achieve results. Privately held since its founding in 1983, A&M is a leading global professional services firm that provides advisory, business performance improvement and turnaround management services.

With over 3000 people across four continents, we deliver tangible results for corporates, boards, private equity firms, law firms and government agencies facing complex challenges. Our senior leaders, and their teams, help organizations transform operations, catapult growth and accelerate results through decisive action. Comprised of experienced operators, world-class consultants, former regulators and industry authorities, A&M leverages its restructuring heritage to turn change into a strategic business asset, manage risk and unlock value at every stage of growth.

When action matters, find us at: www.alvarezandmarsal.com

Follow A&M on:

ALVAREZ & MARSAL