Inside LameDuck: analyzing Anonymous Sudan's threat operations

Threat brief - October 31, 2024

The United States Department of Justice (DOJ) recently unsealed an indictment outlining efforts to dismantle Anonymous Sudan, a prominent group tracked by Cloudflare as LameDuck, notorious for its apparent politically motivated hacktivism and significant involvement in distributed denial-of-service (DDoS) attacks. This broad initiative to bring to justice the group's key members is an impressive step in improving internet security, and was made possible through coordinated efforts among international law enforcement agencies and private sector entities, including Cloudflare. It underscores the importance of partnership across all stakeholders in combating today's most advanced cyber threats, while also demonstrating the value transparency brings to improving threat intelligence. As such, Cloudflare is eager to share insights from our experience in tracking and disrupting LameDuck operations to help bolster your defenses against similar threats.

Executive summary

- DOJ recently unsealed an indictment revealing charges against two Sudanese brothers for orchestrating LameDuck's large-scale DDoS operations from January 2023 through March 2024. The indictment was made possible through coordinated efforts across law enforcement and private industry, including Cloudflare

- LameDuck developed and managed “Skynet Botnet”, a Distributed Cloud Attack Tool, allowing them to conduct more than 35,000 confirmed DDoS attacks in the span of a year, while profiting financially from selling their DDoS services to possibly more than 100 customers
- The threat actor’s operations revealed an unusual combination of motives along with a wide spectrum of targeted industries and governments across the globe
- Cloudflare observed a timely correlation between geopolitical events and LameDuck strikes against high-profile targets, aligning with an anti-Western ideology

Who is LameDuck?

LameDuck is a threat group that emerged in January 2023, presenting itself as an anti-Western, pro-Islamic politically motivated collective. The group is known for launching thousands of DDoS attacks against a wide array of global targets across critical infrastructure (airports, hospitals, telecommunications providers, banks), cloud providers, healthcare, academia, media, and government agencies.

LameDuck gained notoriety by amplifying their successful attacks against widely recognized organizations via social media, while also offering DDoS-for-hire services. Their operations have included not only successful large-scale DDoS attacks, but also DDoS extortion or ransom DDoS. The group’s focus on monetary gain has called into question their emphasis on a political or religious narrative, with many of its operations more closely resembling financially driven cybercrime.

Mixed motives

To further add complexity to this actor’s motives, activity conducted by LameDuck revealed a disparate blend of operations, where high-profile strikes were launched against a vastly diverse set of targets in self-proclaimed support of an odd mix of anti-Israeli, pro-Russian and Sudanese nationalist sentiments. It is possible, however, these attacks were simply driven by a need to bolster their reputation and gain notoriety. In fact, LameDuck heavily leveraged their own social media presence to issue public warnings and spread their narrative in order to attract widespread attention.

Attribution

LameDuck’s unusual combination of motives, along with their religious rhetoric and apparent alliances with other hacktivist groups (e.g., collaboration with Killnet, Türk Hack Team, SiegedSec, and participation in #OpIsreal and #OPAustralia hacktivist campaigns), intensified speculation regarding their true origins and objectives. Previous theories on attribution suggested LameDuck was a Russian state-sponsored group masquerading as Sudanese nationalists. However, the unsealing of DOJ’s indictment revealed that the individuals orchestrating LameDuck’s prolific and highly disruptive DDoS operations were, in fact, not Russian and instead two Sudanese brothers.

Criminal charges against the Sudan-based leaders of LameDuck do not necessarily discount possible Russian involvement in the group’s operations. It’s hard to ignore their shared ideologies, use of the Russian language and inclusion of pro-Russian rhetoric in LameDuck messaging, targeting that aligns with Russian interests, and the group’s coordination with pro-Russian "hacktivist" collectives such as Killnet.

LameDuck targeting and victimology

LameDuck often conducted operations against prominent, high-profile targets to attract greater attention and amplify the impact of their attacks. Their targeting covered a wide geographic range, including the United States, Australia, and countries across Europe, the Middle East, South Asia, and Africa. LameDuck targets also spanned numerous sectors and industry verticals, with some of the more notable targets belonging to the following:

- Government and foreign policy
- Critical infrastructure
- Law enforcement
- News and media
- Tech industry

This list represents only a portion of the industries targeted, emphasizing the wide scope of sectors affected by LameDuck's operations.

Potential reasons for LameDuck targeting include:

- The targeted organization or entity was in opposition to LameDuck's ideological beliefs
- LameDuck may have selected specific infrastructure for targeting due to its potential to impact a larger user base, amplifying the disruption caused and enhancing the group's notoriety
- The ease of successfully executing DDoS attacks on specific infrastructure, due to vulnerabilities and/or poor security practices

Politically motivated targeting

Cloudflare observed that a substantial volume of LameDuck targeting aligns with its self-proclaimed identity as a pro-Muslim Sudanese "hacktivist" group. In particular, the conflict in Sudan and its political repercussions seem to inform a subset of its targets. For example, attacks against Kenyan organizations could be explained by the increasingly tense relations between the Sudanese government and Kenya, culminating in Sudan recalling its ambassador to Kenya in January. Politically motivated attacks were aimed at private sector companies like Microsoft and OpenAI, as LameDuck announced plans to indiscriminately target U.S. companies as long as the U.S. government continued "intervening in Sudanese internal affairs." Apart from the conflict, LameDuck conducted operations revealing support of Sudanese nationalist sentiments, such as their targeting of Egyptian ISPs, which they claimed were meant "to send a message to the Egyptian government that they should hold accountable anyone who insults Sudanese people on social media, just as we do in Sudan to those who insult Egyptians."

LameDuck's pro-Muslim stance also led to targeting organizations perceived as Islamophobic. For example, the high level of targeting against Swedish organizations was claimed to be punishment for the burning of Qurans. Also, after perceived insults against Muslims in Canada and Germany, LameDuck announced the addition of these countries to their target list.

LameDuck also placed additional focus on pro-Israeli targets following the attack by Hamas on October 7, 2023 and the subsequent Israeli military action. Cloudflare observed widespread operations against Israeli organizations across various sectors, with attacks in October 2023 focusing, for example, on major U.S. and international news outlets accusing them of "false propaganda." Cloudflare not only observed and mitigated attacks against various organizations but also became a target itself. Last November, LameDuck "officially declared war" on Cloudflare, stating the attack was due to our status as an American company and the use of our services to protect Israeli websites.

In other instances, Cloudflare observed LameDuck heavily targeting Ukraine, in particular state organizations, or critical transportation infrastructure in the Baltics. These activities have fueled speculations about Russian involvement in LameDuck's operations, as Sudanese actors are not active in Ukraine. However, the geopolitical developments in Sudan are not detached from the Russian war of aggression in Ukraine, as both Russian and Ukrainian forces have been active in Sudan. Not to mention, this past summer, Russia shifted its support to favor the Sudanese Armed Forces and has been sanctioned for providing weapons to Sudan in exchange for access to a port. While previous misconceptions about the group's origin have been dispelled and an understanding of their mixed motivations has somewhat emerged, their disparate targeting and operations that seem to align with pro-Russian sentiments still raise questions about possible affiliations.

Cybercriminal targeting

In addition to LameDuck's politically motivated targeting, the group engaged in financially driven cybercrime, including DDoS-for-hire services. While it is easier to associate ideologically driven targeting with LameDuck actors, attributing operations motivated by financial gain has often proven less straightforward. The group's DDoS-for-hire services makes it difficult to differentiate their attacks from those conducted by their customers. Through the unsealing of DOJ's indictment, we learned that LameDuck had more than 100 users of their DDoS capabilities, which were leveraged in attacks targeting numerous victims worldwide.

LameDuck was also known for engaging in DDoS extortion, demanding payment from their victims in exchange for stopping the attacks. Like other LameDuck operations, these extortion attempts were directed at a wide range of targets. In July 2023, the group attacked the fanfiction site Archive of our own and demanded $30,000 in Bitcoin to withdraw the attack. Setting their sights on a much larger target, LameDuck claimed credit in May of this year for an attack on the Bahrain ISP Zain, publicly stating, "if you want us to stop contact us at InfraShutdown_bot and we can make a deal." This, of course, wasn't their only prominent target. The group initiated a wave of DDoS attacks against Microsoft, and shortly after demanded $1 million to halt their operation and prevent further attacks. Another high profile target included Scandinavian Airlines, which suffered a series of attacks, causing disruption to various online services. LameDuck's attempts to extort the airline began with demands of $3,500 and later escalated to a staggering $3 million. Whether successful or not, these extortion demands are unusual for a self-proclaimed hacktivist group and further highlight LameDuck's use of mixed tactics and apparent need for attention.

LameDuck tactics and techniques

In its first year of operation, LameDuck conducted more than 35,000 confirmed DDoS attacks by developing and employing a powerful DDoS tool known by several names, including “Godzilla Botnet,” the “Skynet Botnet,” and “InfraShutdown”. Despite its many names suggesting it is a botnet, the DDoS tool leveraged by LameDuck is actually a Distributed Cloud Attack Tool (DCAT), which is comprised of three main components:

1. A command and control (C2) server
2. Cloud-based servers that receive commands from the C2 server and forward them to open proxy resolvers
3. Open proxy resolvers run by unaffiliated third parties, which then transmit the DDoS attack traffic to LameDuck targets

LameDuck used this attack infrastructure to overwhelm a victim organization’s website and/or web infrastructure with a flood of malicious traffic. Without proper protections in place, this traffic can severely impact, if not completely impede, a website’s ability to respond to legitimate requests, leaving actual users unable to access it. Since its emergence in early 2023, LameDuck employed a variety of tactics and techniques using its DCAT capabilities. Several identified patterns include:

- Launching layer 7 attacks via HTTP flooding. The type of flood attack we detected and mitigated was an HTTP GET attack, which involves the attacker sending thousands of HTTP GET requests to the targeted server from thousands of unique IP addresses. The victim server is inundated with incoming requests and responses, resulting in denial of service for legitimate traffic. LameDuck was also known to leverage multi-vector attacks (e.g., a combination of TCP-based direct-path and various UDP reflection or amplification vectors).
- Using paid infrastructure. Unlike many other attack groups, research indicates that LameDuck did not use a botnet of compromised personal and IoT devices to conduct attacks. Rather, the group used a cluster of rented servers — which can output more traffic than personal devices — to launch attacks. The fact that LameDuck had the financial resources to rent these servers was another reason some researchers believed the group were not the grassroots hacktivists they claimed to be.
- Traffic generation and anonymity. LameDuck used public cloud server infrastructure to generate traffic, and also leveraged free and open proxy infrastructure to randomize and conceal the attack source. Evidence indicates the group in some cases also used paid proxies to obscure their identity.
- High cost endpoints. In some instances LameDuck operations were aimed at high-cost endpoints of the targeted infrastructure (i.e. endpoints responsible for resource intensive processing). Attacking these endpoints are far more disruptive than taking out several dozen less computationally intensive, low-cost endpoints.
- High demand periods. For some targets, LameDuck was careful to choose attack times that corresponded to high-demand periods for the target. For example, attacks during peak consumer periods to aim for maximum disruption.

- Blitz approach. LameDuck was known to initiate a series of concentrated attacks on multiple interfaces of their target infrastructure simultaneously.
- Subdomain overwhelming. A similar concept to the attack technique above, where LameDuck would simultaneously target numerous subdomains of the victim domain.
- Low RPS. The attack's requests per second (RPS) was relatively low in an attempt to blend in with legitimate traffic and avoid detection.
- Threats via public announcements and propaganda. LameDuck often threatened targets in advance of actual attacks, and sometimes made threats that were never borne out. Likely reasons for doing so included gaining attention for their ideological motives and sowing uncertainty amongst potential targets.

Recommendations

Cloudflare has successfully defended numerous customers against attacks facilitated by LameDuck, whether it be those conducted directly by the group or those initiated by individuals utilizing their DDoS-for-hire services. It's important to note that LameDuck's advanced DDoS capabilities enabled them to severely impact networks and services that did not have proper protections in place. With that said, this group is unfortunately only one of many to employ successful large-scale DDoS attacks, which are only growing in size and sophistication. Organizations can protect themselves from attacks like those launched by LameDuck and similar advanced adversaries by following a standard set of DDoS mitigation best practices.

- Use dedicated, always-on DDoS mitigation. A DDoS mitigation service uses a large bandwidth capacity, continuous analysis of network traffic, and customizable policy changes to absorb DDoS traffic and prevent it from reaching a targeted infrastructure. Organizations should ensure they have DDoS protection for Layer 7 traffic, Layer 3 traffic, and DNS
- Use a web application firewall (WAF). A WAF uses customizable policies to filter, inspect, and block malicious HTTP traffic between web applications and the Internet
- Configure rate limiting. Rate limiting restricts volumes of network traffic over a specific time period, essentially preventing web servers from getting overwhelmed by requests from specific IP addresses
- Cache content on a CDN. A cache stores copies of requested content and serves them in place of an origin server. Caching resources on a content delivery network (CDN) can reduce the strain on an organization's servers during a DDoS attack
- Establish internal processes for responding to attacks. This includes understanding existing security protection and capabilities, identifying unnecessary attack surfaces, analyzing logs to look for attack patterns, and having processes in place for where to look and what to do when an attack begins