|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **DDoS on Israeli Websites (October 7, 2023)** | | | |
| Preparing for DDoS attacks | Search Open Websites/Domains: Search Engines | To perform the DDoS attacks, the group would have identified the websites and searched them. They also gathered domain properties needed to perform the DDoS attacks. |  |
| Search Open Websites/Domains: Social Media |
| Gather Victim Network Information: Domain Properties |
| Anonymous Sudan launched several DDoS attacks on > 40 websites, including the Jerusalem Post, the Israeli Security Agency (Mossad) and Prime Minister’s sites. | Network Denial of Service | They launched several DDoS attacks. |  |
| Block Content | In using DDoS attacks, the group prevented access to websites, preventing access to information about the Hamas attacks. |  |
| Control Information Environment through Offensive Cyberspace  Operations |
| Service Stop | The websites were temporarily unavailable. |  |
| Continue to Amplify | Alongside the DDoS attacks, the group uses chat apps to share their attacks. In attacking several websites, the attacks are amplified. |  |
| Anonymous Sudan has a pre-existing botnet / distributed cloud attack tool used for DDoS attacks. | Acquire Infrastructure: Server | To establish the Botnet, necessary infrastructure was acquired. The botnet used is described as a “distributed cloud attack tool”. |  |
| Acquire Infrastructure: Botnet |
| Acquire Botnets |
| Obtain Capabilities: Tool |
| **Telegram channel** | | | |
| Telegram channel used to communicate | T0043.001: Use Encrypted Chat Apps | Telegram, an encrypted chat application, was used to broadcast the DDoS attacks to followers of Anonymous Sudan. The group uses the pseudonym “Anonymous Sudan” in the channel, to remain anonymous. However, recently the identities of the two brothers involved in the group have been revealed. |  |
| T0043: Chat apps |
| Use Pseudonyms |
| T0090.001: Create Anonymous Accounts |
| Create Community or Sub-group |
| Posting claims of cyberattacks on the channel | Develop Text-Based Content | The content in the channel is largely text-based, describing the motivations of the attacks and who the group is attacking. |  |
| Post Content |
| Messages depicting motivations for cyberattacks posted “Infrastructure of the Israeli has been down because of what they did to Palestine,”  “Bomb our hospitals in Gaza, we shut down yours too, eye for eye,” – in reference to their DDoS attack on a Jewish hospital in LA | T0066: Degrade Adversary | From these quotes, the group aimed to degrade their adversary (Israel and organisations associated with supporting Israel). These motivations are relevant to the Israel-Hamas conflict. |  |
| Dismay |
| Dismiss |
| T0068: Respond to Breaking News Event or Active Crisis |
| Threatening to attack other services | Harass | The group threatened to attack other services. |  |
| Marketing DDoS service to potential customers + communicating with customers |  | Not present  According to the US Justice investigation, the group also sells their DDoS service. A technique to reflect this could not be found. |  |
| Cryptocurrency used for transactions when services purchased | Use Cryptocurrency | Transactions completed by the group use Bitcoin, aiming to conceal their identity and prevent tracking. |  |
| Conceal Network Identity |  |
| Calling for others to join the attacks |  | Not present  The closest technique found was “Call to attend event”, however this does not exactly fit the scenario. |  |
| **Disrupting Israeli warning systems (October 7, 2023)** | | | |
| Briefly disabled online early warning systems used in Israel. | Network Denial of Service | This aspect of the operation is not modelled separately, as it shares the same techniques as the DDoS attacks on the other websites. This event is considered within the broader use of DDoS attacks on October 7 modelled in the diagram. |  |
| Preventing warnings from reaching Israelis. Disrupted an hour after Hama’s assault (1,200 people were killed and 200 abducted). | Control Information Environment through Offensive Cyberspace  Operations |
| Targeted two companies that provide online applications to alert danger | Search Victim-Owned Websites |
| Red Alert representative (one of these companies) confirms it suffered a DDoS attack on its website (however did not affect its alert system) |  |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | Before launching their attacks, the group identified their targets, target audiences, and aim. |  |
| Determine Strategic Ends |
| After | Measure effectiveness: Message reach | As the group uses Telegram, they can check the responses to their posts and messages. |  |