flare

Crowdsourced DDoS Attacks Amid Geopolitical Events

Table of Contents

Key Findings 3

Introduction 4

Russia-Ukraine Conflict: IT Army of Ukraine & DDoSia 5

Israel-Hamas Conflict: Cyber Army of Palestine 10

Conclusion 17

Crowdsourced DDoS Attacks Amid Geopolitical Events

by Zaid Osta, CTI Analyst

This report explores the rising trend of crowdsourced distributed denial-of-service (DDoS) attacks within the context of recent geopolitical events, examining case studies from the ongoing Russia-Ukraine and Israel-Hamas conflicts.

Key Findings

- **Overall Trend:** The crowdsourcing attack model differs from traditional DDoS attacks carried out by well-funded and sophisticated threat actors, primarily in terms of its accessibility. Threat actors with limited resources and minimal technical expertise can now contribute to significant attacks against private businesses and government agencies, using open-source tools and the support of a network of volunteers driven by shared political beliefs.
- **Increasing Sophistication:** We see crowdsourced attacks becoming increasingly sophisticated as threat groups implement leaderboards, financial rewards, and other incentives in order to motivate individual actors to participate. This fits the broader trend of growing commoditization we see in the cybercrime ecosystem.
- **IT Army of Ukraine:** A volunteer-based collective formed in response to the Russian invasion of Ukraine, targeting Russian digital assets. They utilize open-source DDoS tools, with installation and usage guidance on their website, and employ a leaderboard to gamify and track participants' contributions, adding a competitive element to cyberattacks.
- **DDoSia by NoName057(16)**: Supporting Russia in the conflict, DDoSia has witnessed rapid expansion with its unique model of offering financial incentives. Volunteers are compensated in cryptocurrency, based on their contribution to DDoS attacks against American and European digital assets, attracting both
- **Cyber Army of Palestine**: Established in response to Israel's military operation in Gaza, this group organizes thousands of volunteers, coordinating their efforts in successful anti-Israel DDoS campaigns. They use a Windows-based attack tool named after Hamas' October 7th attack on Israeli cities. Analysis of the tool's source code indicates that it is a recycled version of the IT Army of Ukraine's UAshield tool. The group features a Hamas-themed ranking system, incentivizing participation by linking successful DDoS contributions to ranks of key Hamas figures, including bomb makers and senior military commanders assassinated by Israel.

Introduction

DDoS attacks involve a large network of devices or compromised systems, often known as a botnet, flooding a target with excessive internet traffic to deny availability. These attacks have become increasingly common in recent years as a result of rising tensions and conflicts between nation states. Rather than being tools solely wielded by highly sophisticated actors, these attacks have increasingly become the domain of moderately skilled attackers, or even novices, who exploit geopolitical tensions and conflicts to target victim organizations. This trend signifies a sea change in cyber warfare: the barrier for impactful attacks is lower, while the ability to exploit politically charged events for disruptive purposes is both high and evident.

An example of this escalating threat is seen in Latvia's response to the pro-Russia hacktivist collective Killnet. Following a series of DDoS attacks against Latvian parliamentary web services, Latvia officially designated Killnet as a terrorist organization, underscoring the serious nature of such attacks and their fusion with geopolitics.

Similarly, earlier this year, the Kenyan government experienced a massive politically driven DDoS attack launched by Anonymous Sudan, which disrupted nearly 5,000 government services for almost a week. The attack, in response to the group's perception of Kenyan interference and meddling in Sudanese affairs, affected critical operations, including the processing of passport applications, issuing e-visas for foreigners, and disruptions to train-booking systems. This example highlights the significant disruption of even relatively low sophistication DDoS attacks.

The increasing prevalence of crowdsourced DDoS attacks represents a new trend in the realm of geopolitically driven hacktivism. These attacks leverage the collective power of many individuals and their systems, who are sympathetic to the cause of the threat actor and are aligned with the threat actor's political views.

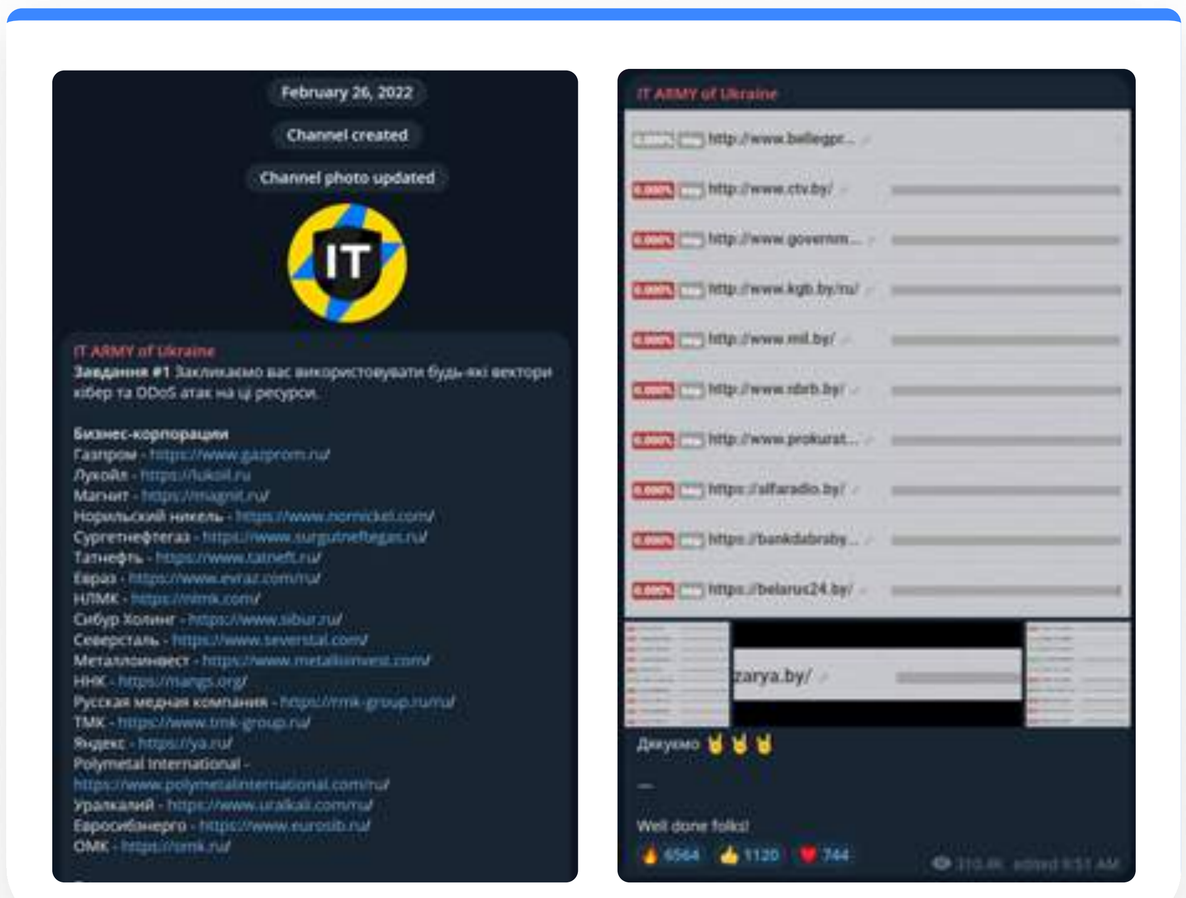
As a result these attacks require no special skills, such as developing malware, compromising devices, and then developing a botnet of these hacked systems, but rather, they only require some coordination and enough participants to temporarily take down a website or service. This report will explore recent case studies of crowdsourced DDoS attacks, from Eastern Europe with the Russia-Ukraine conflict, to the Middle East with the Israel-Hamas conflict. In some cases, we see actors leveraging leaderboards, payments, and other incentives to encourage greater participation in these attacks.

Russia-Ukraine Conflict: IT Army of Ukraine & DDoSia

On February 24, 2022, Russia launched a military invasion of Ukraine, marking the largest attack on a European country since World War II. In response, the "IT ARMY of Ukraine" (hereinafter referred to as the "IT Army") was launched. Just two days after the invasion, on February 26, 2022, the IT Army made its first appearance with a Telegram channel. Their inaugural post reached out to "IT specialists from other countries," soliciting support for "cyber and DDoS attacks" against a range of Russian digital assets.

This initial call to action included a list of prominent Russian business, bank, and state service websites, such as Gazprom, Yandex, and the Kremlin. Later that day, the IT Army posted two IP addresses linked to Gosuslugi, Russia's official internet portal for government services. Just 13 minutes after this post, the IT Army announced a successful DDoS attack on the Gosuslugi service, claiming their volunteers took it down in "just 1 minute."

The momentum continued the following day with the IT Army shifting its focus to Belarusian websites, identified by their ".by" country code top-level domain, likely in response to Belarus' support for Russia in the war. This strategy quickly yielded results again, as several targeted Belarusian websites were taken down, and a congratulatory post was shared on the IT Army's channel with proof of HTTP connection failures to the websites.



Screenshots depicting the first post on the IT Army's official Telegram channel (left), and a congratulatory message posted by the IT Army (right) with images indicating the temporary unavailability of prominent Belarusian websites. [Source: Telegram]

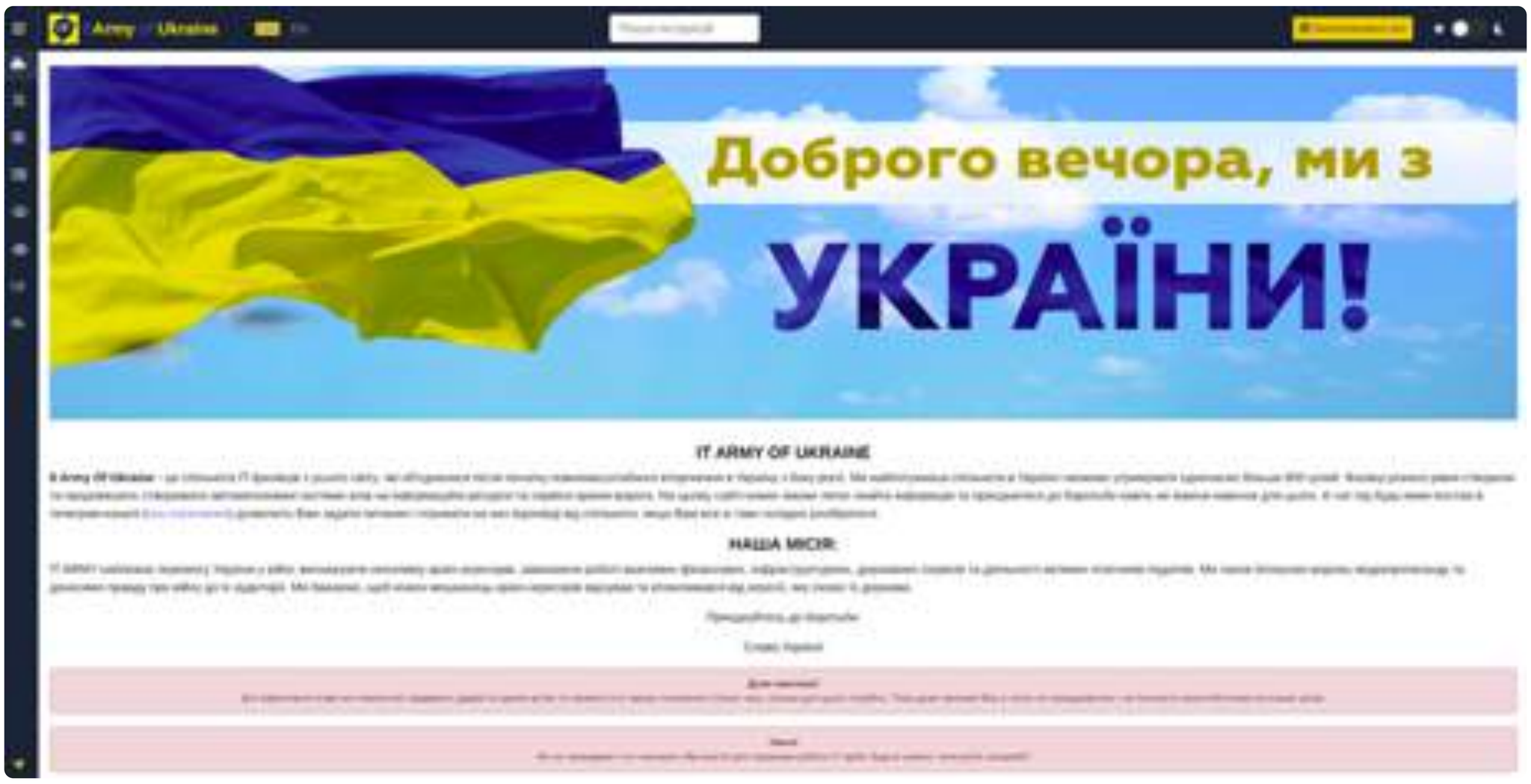
This model of operation, which involved publicly sharing target domains and IP addresses along with their respective port numbers, and then displaying screenshots as proof of successful takedowns, continued for several months with successful back-to-back DDoS attacks. During this period, however, the IT Army was developing custom tools and a website to streamline future attacks. According to a WHOIS lookup, the IT Army's official website was registered on April 5, 2022, two weeks before the IT Army first publicly announced it.

According to their stated mission, the IT Army "aims to help Ukraine win by crippling aggressor economies, blocking vital financial, infrastructural and government services, and tiring major taxpayers. We also stop hostile media propaganda and spread truth about the war. We want every resident of aggressor countries to feel and tire from their state's aggression."

The website explains that the IT Army is "a worldwide IT community united to resist the Russian invasion to Ukraine. We are supreme power in Ukraine capable to block over 800 targets simultaneously... keep using automated systems to harass websites and internet services of the country-aggressor.

This website is made to provide guidelines for joining our resistance **even if you are very rookie in technologies**" - which is exactly why crowdsourcing DDoS attacks is concerning: even a "rookie in technologies" can effectively contribute to attacks.

The IT Army's website offers detailed guidance on conducting DDoS attacks against designated targets. It presents a range of tools, encouraging users to try them out to find the most suitable one for them. The website emphasizes using these tools on a virtual private server (VPS), to prevent local network overload and increase attack efficiency with better resource availability. It provides specific guidelines for various operating systems, including Windows, Linux, and Mac. It also advises users to disable their antivirus softwares prior to installing the tools: "Our Russian foes leveraged antivirus software to consider DDoS potentially unsecured hence blocked."



Screenshot depicting the homepage of the IT Army's official website. [Source: IT Army]

The IT Army assures volunteers that the recommended tools — MHDDoS, DB1000N, Distress, UKITA, and UAshield — are safe, claiming: "Our tools do not contain any harmful components for your cybersecurity." Detailed instructions cover each tool's installation, optimal tool settings, and tips on using VPNs for improved attack performance and enhanced anonymity. Here is an overview of the tools facilitating the IT Army's crowdsourced DDoS attacks:

- **MHDDoS**

  MHDDoS is a DDoS tool with a "user-friendly" interface that does not require a VPN, as it "automatically downloads and selects working proxies."

- **DB1000N (Death by 1000 Needles)**

  DB1000N is a Go-based DDoS tool, described by its Ukrainian author as "a simple distributed load generation tool." The author adds: "Feel free to use it in your load tests (wink-wink)." On the tool's documentation page, the author explains the motive behind writing the tool: "On 24th of February Russia has launched a full-blown invasion on Ukrainian territory. We're doing our best to stop it and prevent innocent lives being taken."

- **Distress**

  Distress is a Rust-based DDoS tool written by a "Senior Java Software Engineer" currently residing in Kyiv, Ukraine, as per his LinkedIn profile. Another contributor to the tool is a "15-year-old Web Developer from Ukraine," as per his GitHub profile.

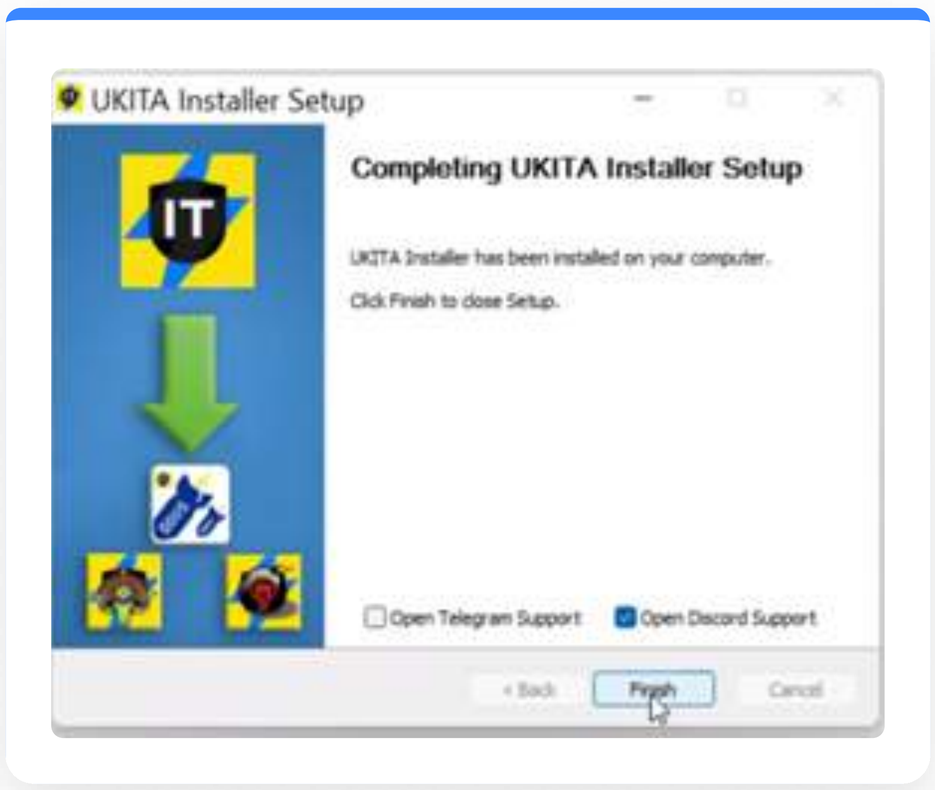
- **UAshield**

  UAshield is yet another DDoS tool, self-described on its GitHub repository page as: "Voluntary Ukraine security platform to protect us from Russian forces in the Internet."

Screenshot depicting the UAshield interface for Windows. [Source: IT Army]

- **UKITA (Ukraine IT Army Installer)**

  UKITA is an all-in-one suite of the above DDoS tools, available for Windows only.

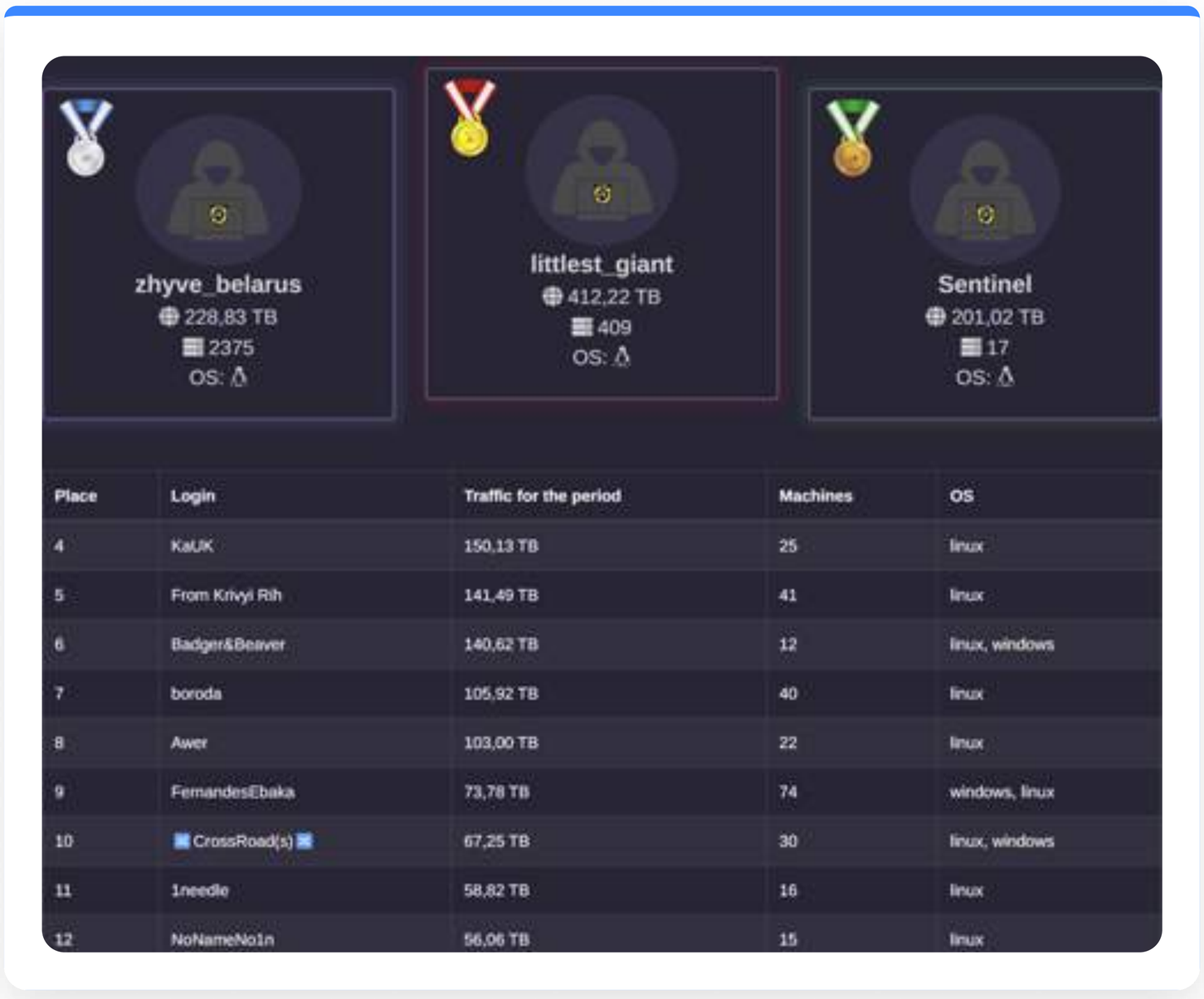


Screenshot depicting the UKITA Windows installer. [Source: IT Army]

- **ADSS (Automatic DDoS Server Starter)**

  ADSS, is a shell script designed for Linux. It automates tasks such as self-updating, determining the OS version, and installing DDoS tools. It also installs a firewall and sets MHDDoS to start automatically during Linux boot.

For effective attack coordination, the IT Army automates target selection, allowing volunteers to simply focus on tool deployment. An interesting feature of IT Army is the tracking of per-user attack traffic. This system uses a Telegram bot to assign an anonymous ID to each volunteer, enabling them to monitor their individual impact on the DDoS attacks. Instructions explain how to obtain and integrate this ID with the DDoS tools, and the "Leaderboard" section on the website, updated every 7 minutes and posted weekly to Telegram, showcases these statistics. This approach introduces a gamified and competitive element to volunteering in DDoS attacks.



Place	Login	Traffic for the period	Machines	OS
4	KaUK	150,13 TB	25	linux
5	From Krivyi Rih	141,49 TB	41	linux
6	Badger&Beaver	140,62 TB	12	linux, windows
7	boroda	105,92 TB	40	linux
8	Awer	103,00 TB	22	linux
9	FernandesEbaka	73,78 TB	74	windows, linux
10	CrossRoad(s)	67,25 TB	30	linux, windows
11	1needle	58,82 TB	16	linux
12	NoNameNo1n	56,06 TB	15	linux

Screenshot depicting the IT Army Leaderboard, where "littlest_giant" secures the number 1 spot, having unleashed a staggering 412 TB of DDoS traffic on IT Army targets, using 409 Linux-based machines. [Source: IT Army]

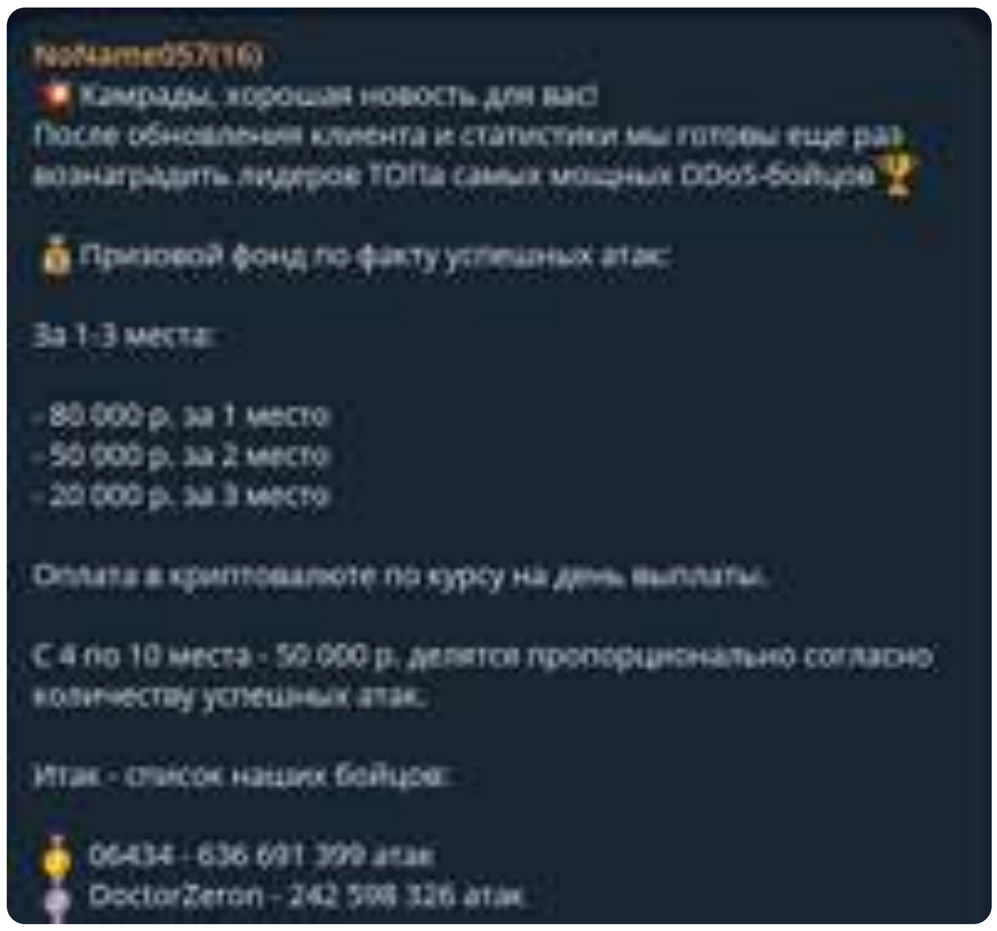
On the other side of the Russia-Ukraine conflict in the realm of crowdsourced DDoS attacks is DDoSia. This cybercrime project is operated by the pro-Russian hacktivist group "NoName057(16)" (hereinafter referred to as "NoName"), which began its DDoS attacks in early 2022. NoName has attracted considerable attention due to its frequent disabling of prominent websites belonging to American and European private businesses, media outlets, and government agencies. As of December 2023, NoName's primary Russian-language Telegram channel has reached nearly 60,000 subscribers.

Since its inception, the DDoSia project has seen remarkable growth, expanding by a massive 2,400% in less than a year. Originally developed in Python and initially exclusive to Windows, DDoSia has since broadened its compatibility to include versions for Windows, Linux, and Mac, as of the November 30, 2023, distribution of the tool.

Similar to the Ukrainian IT Army's statistics bot, NoName automates participation through Telegram bots and a leaderboard, too. However, DDoSia stands out by offering financial incentives, attracting not only those ideologically aligned with NoName's anti-Western and pro-Russian stance, but also opportunists interested in monetizing cybercrime.

NoName has used a distributed payout model to reward the "most active fighters of the DDoSia Project," as stated in a Telegram post by the group. This model's rewards are based on the number of "successful attacks" (likely successful HTTP requests to target websites), and paid in cryptocurrency at the exchange rate on the day of payment. The rewards according to NoName are 80,000 rubles ($882) for 1st place, 50,000 rubles ($551) for 2nd place, 20,000 rubles ($220) for 3rd place, and a proportional division of 50,000 rubles ($551) among 4th to 10th place users.

Under a per-user reward system, new DDoSia members provide a TON (Telegram Open Network) wallet address to receive cryptocurrency, and an automated bot generates a unique client ID. Attack participants link this ID to their cryptocurrency wallet, earning money for participating in DDoS attacks, with the payment being proportional to their attack contribution.



Screenshot depicting an October 11, 2022, NoName Telegram post addressing "comrades" and announcing monetary rewards for their "most powerful DDoS fighters." Volunteer "06434" has launched over half-a-billion "attacks." [Source: Telegram]

Israel-Hamas Conflict: Cyber Army of Palestine

On October 7, 2023, in response to Hamas' attacks on cities along the Gaza envelope, Israel declared a state of war and launched a military operation on the Gaza Strip. In the subsequent days, several Telegram channels emerged aiming to take prominent Israeli websites offline in response to Israel's offensive. One such group, the "Cyber Army of Palestine" (hereinafter referred to as the "Cyber Army"), was established on October 14, 2023.

Announcing their mission in Arabic, the Cyber Army declared their preparation for "strong cyberattacks on the technological infrastructure of the Zionist entity," noting that "specialized teams are preparing the necessary tools and instructions to facilitate these attacks for everyone." The Cyber Army embraced the increasingly popular tactic of crowdsourcing DDoS attacks, telling their followers that "anyone with a computer and internet access can participate in the initial campaign," emphasizing that the planned attacks would be simple and straightforward, "requiring no expertise."

Recognizing the inexperience in cybersecurity among many of its thousands of new followers, the Cyber Army began its campaign by sharing infographics explaining essential terms deemed necessary for engaging in cyberattacks. Notably, these infographics and all subsequent ones bear the text logo "Tufan al-Aqsa" in the top left corner. "Tufan al-Aqsa" translates to "al-Aqsa Flood," which is the title used by Hamas to designate its October 7th attack on Israel. This serves as a clear indicator of the Cyber Army's support of Hamas.

Screenshots depicting three educational infographics shared by the Cyber Army. [Source: Telegram]

On October 18, 2023, the Cyber Army announced the release of their Windows tool which helps enable their crowdsourced DDoS attacks. The tool was named after Hamas' operation, with the Cyber Army writing on Telegram:

"A DDoS attack tool will be published shortly. The current version works on: Windows and Linux.

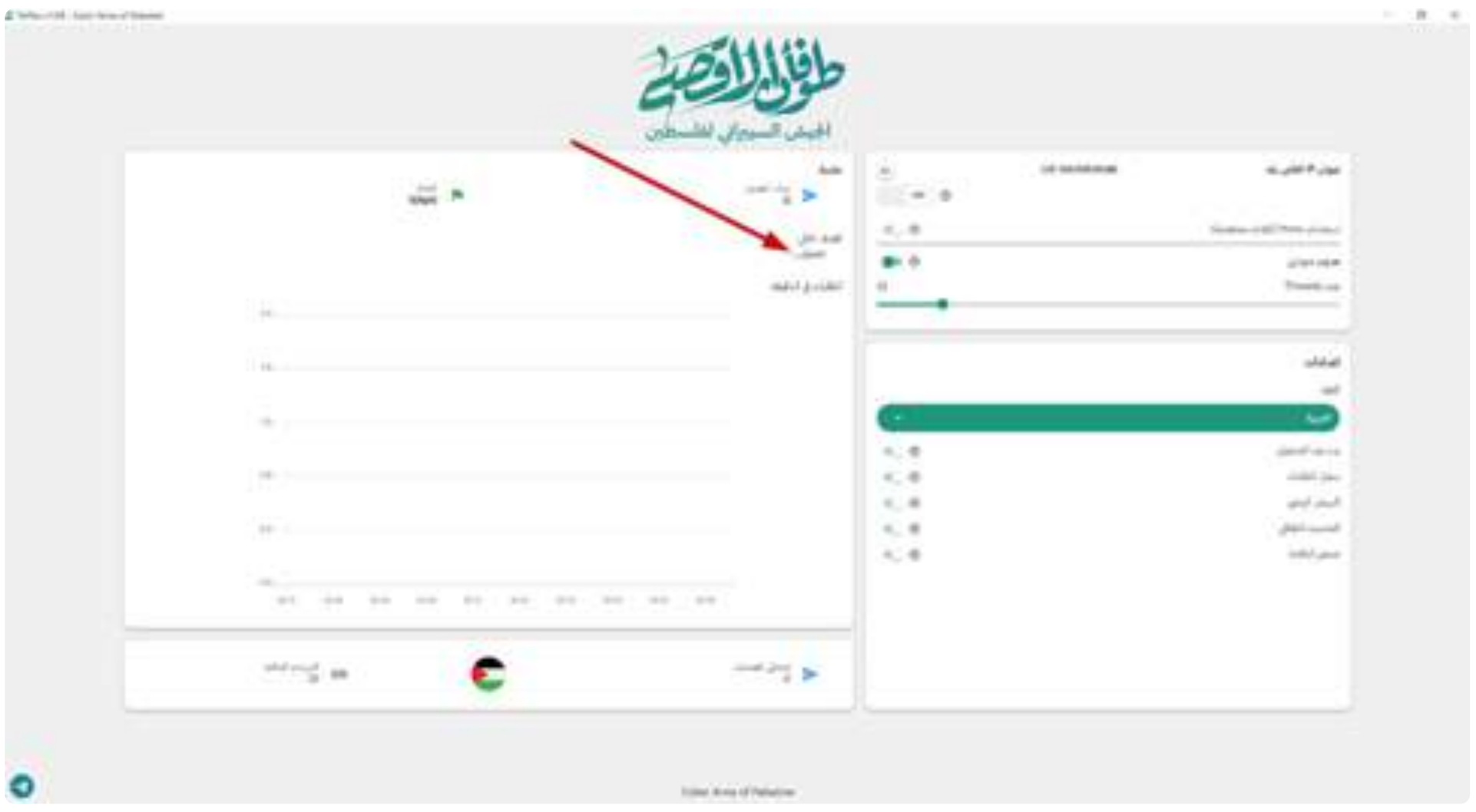
The name of the attack tool is: Toffan [alternate spelling of "Tufan"] version one. The level of tool usage is for: beginners and professionals.

Important notice for successful operations: The tool should continue operating for as long as possible. Use paid VPNs (if available). The attack should involve as many people as possible. If you own a cloud server, the attack will be more impactful.

First target: Ten Israeli news websites and Dubai International Airport's website [likely due to the UAE's recent normalization deal with Israel].

We hope you disseminate this channel widely so it reaches all free people in all Arab countries. The larger the number, and from different locations, the more successful the attack will be."

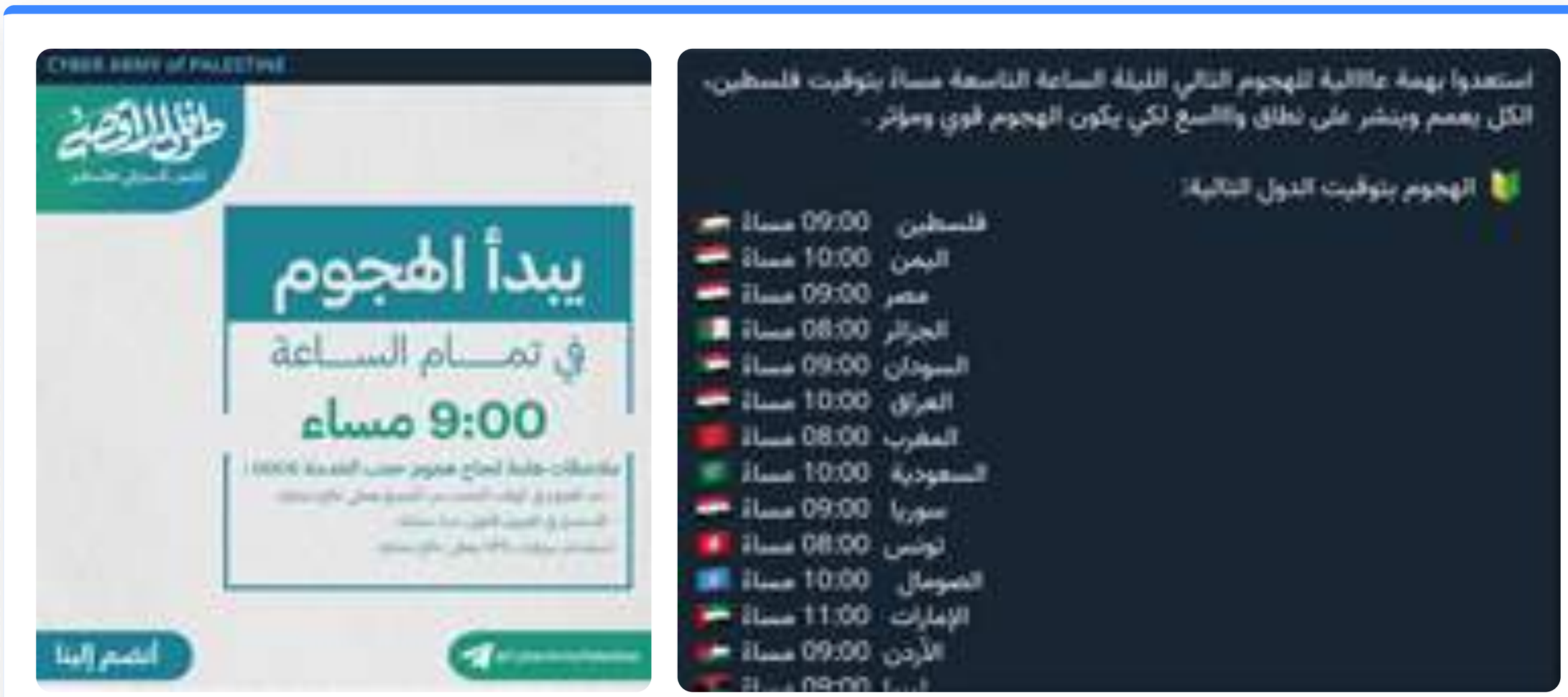
Screenshots depicting three infographics released by the Cyber Army with general installation and usage instructions for Toffan and an overview of the user interface. [Source: Telegram]



Screenshot depicting Toffan's user interface. The red arrow points at "Current Target Loading." The Cyber Army explains: "We control the pool of targets, automatically integrated into the tool. All you need to do is run the tool and keep the attack going as long as possible." [Source: Flare]

The Cyber Army's upcoming attacks are announced to participants via Telegram posts accompanied by infographics specifying the attack time. For example, a post on October 19, 2023, reads: "Alert to all the honorable people of the Arab world! The attack begins today at exactly 10:00 PM Mecca time. Be ready, all of you, to start simultaneously." Another post on November 2, 2023, states: "Get ready for the next attack tonight at 8:00 PM al-Aqsa time. Everyone should disseminate and share this to ensure the attack is powerful and effective."

A list of Israeli website links, including news outlets, law firms, government agencies, and critical infrastructure services, typically follows these postings. Users do not have to copy these links at the coordinated attack time. Instead, target websites are automatically integrated into and updated by Toffan for ease of use, enabling seamless crowdsourced DDoSing.



Screenshots depicting a November 13, 2023, Telegram post by the Cyber Army: "Get ready with high enthusiasm for the next attack tonight at 9:00 PM Palestine time. Disseminate this widely so the attack is powerful and effective." Attack times in various Arab countries are then listed. [Source: Telegram]

After downloading and extracting the password-protected archive from the Cyber Army's Telegram channel, users set up the Toffan DDoS tool with a 184 MB EXE installer. The installer places the primary files of the tool into the C:/AppData/Local/Programs/Toffan folder. Upon inspecting the folder's contents and the application itself, it was evident that the tool is built with Electron, a platform for building desktop applications using technologies such as HTML, CSS, and JavaScript. The source code, assets, and resources of Electron applications are packaged in a single file using the compressed Atom Shell Archive file format, or ASAR.

Unpacking Toffan's ASAR file reveals its Electron application source code. Reformatting the obfuscated and disorganized .js code files returns cleaner code structures, rendering the code more readable and comprehensible. It then becomes evident that the Toffan DDoS tool is not an entirely original creation. Analysis indicates that significant portions of the UAshield tool, developed by the Ukrainian IT Army, appear to have been incorporated into Toffan.

In Toffan, several code segments are identical to those in UAshield, and others are very similar with slight differences. Toffan's author renamed variables and classes into more generic or less meaningful names, and restructured the code's flow without altering the tool's functionality, likely a result of automated obfuscation. There are even spelling mistakes in variable names that are identical, as seen below.

```
setExecutorStartegy (planingStrategyType: PlaningStrategyType) {
  this.executorPlaningStrategy.stop()
  console.log('Changing strategy to ' + planingStrategyType)
  switch (planingStrategyType) {
    case 'manual': this.executorPlaningStrategy = new ManualStrategy(this.executorFactory); break
    case 'automatic': this.executorPlaningStrategy = new AutomaticStrategy(this.executorFactory); break
  }
  this.executorPlaningStrategy.start()
}
```

```
setExecutorStartegy(t) {
  switch (this.executorPlaningStrategy.stop(), console.log("Changing strategy to " + t), t) {
    case "manual":
      this.executorPlaningStrategy = new kt(this.executorFactory);
      break;
    case "automatic":
      this.executorPlaningStrategy = new Pt(this.executorFactory);
      break;
  }
  this.executorPlaningStrategy.start();
}
```

Screenshots depicting UAshield's (top) and Toffan's code (bottom). Both serve the same purpose: altering the "executor planning strategy" based on an input parameter, and they share the same spelling errors, rendering "strategy" as "startegy" and "planning" as "planing." [Source: Flare]

```
const mt = ["yandex.ru", "rostender.info",
"gosuslugi.ru", "kremlin.ru", "government.ru", "pfr.
gov.ru", "rkn.gov.ru", "mvd.gov.ru", "rostender.
info", "cdek.ru", "datrans.ru", "qiwi.com", "svo.
aero"];
```

```
const BACKUP_SERVERS_DOMAINS = ['yandex.ru','rostender.info',
'gosuslugi.ru','kremlin.ru','government.ru','pfr.gov.ru','rkn.
gov.ru','mvd.gov.ru','rostender.info','cdek.ru',
'datrans.ru','qiwi.com','svo.aero'
] as Array<string>
```

The author of Toffan's code (top) did not remove several Russian domains originally hard-coded in UAshield (bottom). Only the variable name was changed, likely due to automated obfuscation. [Source: Flare]

UAshield offers users a ranking system based on the number of "successful attacks" that DDoS participants perform. As seen in UAshield's code, the ranks are structured into levels from 0 to 24, and each level is associated with a specific rank name. Users ascend through the levels based on their contributions to DDoS attacks on IT Army targets. For example, Level 3 is "Potato man," Level 8 is "Pickled cucumber jar," Level 14 is President "Joe Biden," Level 23 is "Valerii Zaluzhnyi" (Ukraine's Commander-in-Chief), and the highest Level 24 is "Volodymyr Zelenskyy" (Ukraine's President).

In yet another display of the Cyber Army's ideology, Toffan replaces this Ukrainian-made list and provides rankings from levels 0 to 24, featuring names of predominantly former senior Hamas members. For instance, Level 12 is designated as "Yahya Ayyash," a Hamas bomb maker known as "The Engineer." Level 17 corresponds to "Mahmoud Al-Mabhouh," a senior Hamas military commander assassinated in Dubai in 2010. Level 23 is "Ahmed Yassin," the founder and spiritual leader of Hamas, killed in an Israeli airstrike in 2004. The highest-performing DDoS attack participant at Level 24 is awarded the rank of "Izz al-Din al-Qassam," the name of an Arab nationalist and Islamic militant leader from the 1930s. The rank "Izz al-Din al-Qassam" serves as a reference to the military wing of Hamas, known as the Izz al-Din al-Qassam Brigades.

In addition, the author of Toffan did not remove a hard-coded file path from their code, revealing that the DDoS tool's development environment was located within a folder titled "qassam" on Toffan's author's desktop, another reference to the Izz al-Din al-Qassam Brigades. The hard-coded file path as seen in the unpacked Electron application's source code is:

```
"C:/Users/Virtual/Desktop/work/qassam/node_modules/yargs/lib/platform-shims/esm.mjs"
```

It is notable that in Toffan's source code, the Arabic language is configured multiple times across different code files with the locale code "ar-YE," representing the Yemeni dialect of Arabic. Typically, Arabic applications utilize the locale code "ar" or "ar-SA" (Saudi Arabia) to represent the Modern Standard Arabic (MSA) dialect, universally understood across the Arab world. Although not definitive evidence linking Toffan's author to a specific nationality, this prompts questions regarding the configuration of Toffan, specifically with the Yemeni Arabic locale code.No other Arabic locale code exists in the analyzed Electron application source code.

Further analysis of Toffan's code indicates that in version 1, attacks were carried out after targets were automatically pulled from the GitHub profile "@trynothing09," now inactive and unarchived. In version 2, the tool called on the profile "@KareemAdem," also inactive and unarchived, to pull targets. However, in the latest version of Toffan as of late December 2023, the tool calls on the active profile "@hw746159" to pull targets.

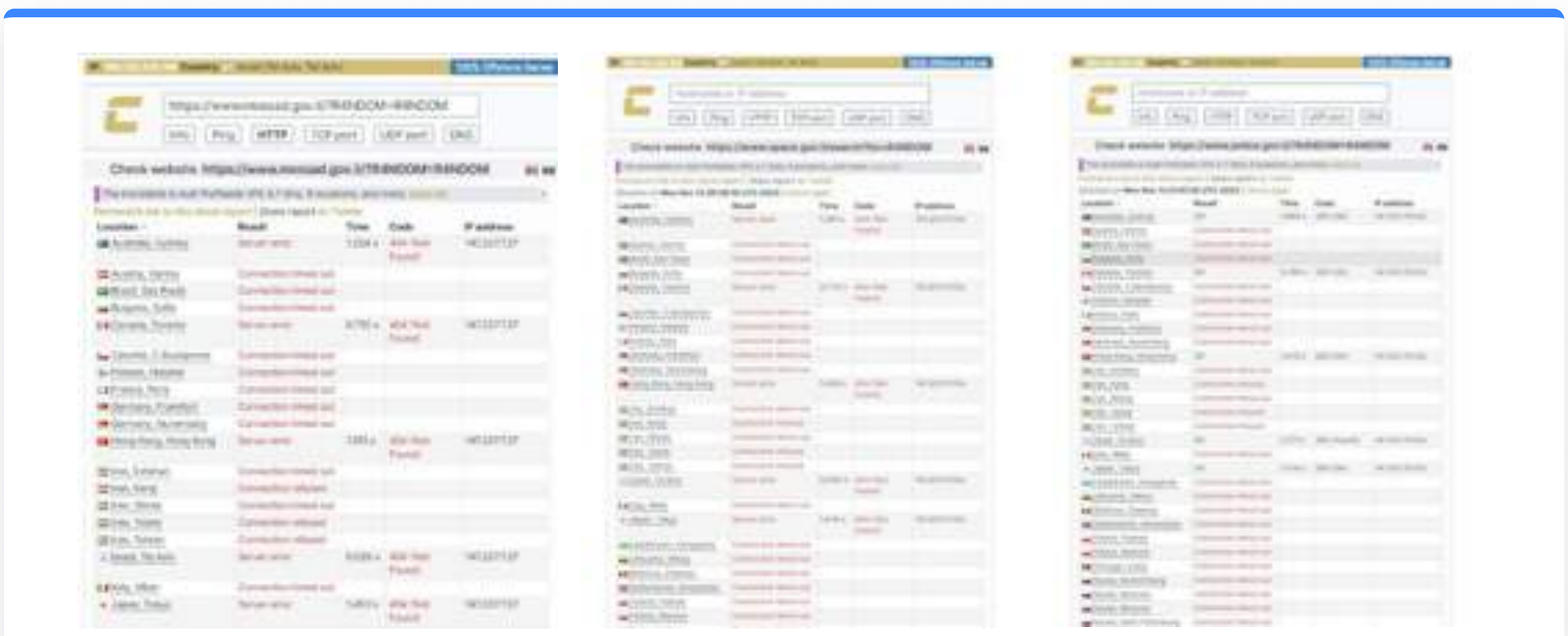
Displayed below are partial screenshots of the original and decoded versions of the "0.json" file on the "@hw746159" profile. This file contains 14 base64-encoded .il (Israel) websites, pulled by Toffan at coordinated attack times, and subsequently flooded by Cyber Army volunteers with HTTP GET requests. These websites span various industries such as banking, government, telecommunications, intelligence, media and news, and investment.

Partial screenshots displaying the original (top) and base64-decoded (bottom) "0.json" file on the active GitHub profile of "@hw746159," featuring targeted Israeli websites. [Source: Flare]

Screenshot depicting Toffan during a French-speaking participant's attack on Israel's Ministry of Health website. This user has sent over 4 million GET requests with Toffan. [Source: Flare]

The Cyber Army also offers an APK for Android users to participate in their DDoS attacks. Basic analysis of the Android application indicates that, like the Toffan tool for Windows, the APK is recycled and not custom-built from scratch. The original application appears to be the "DDoSPacket" tool for Android written by "@blueskychan-dev," who mentions on their GitHub profile: "I make this app since i'm 12 years old and going register to middle school."

With thousands of Telegram followers, and a simple model of crowdsourcing DDoS attacks against Israeli websites, the Cyber Army typically achieves successful attack results just minutes after the announced attack times. Below are sample screenshots posted by the Cyber Army, from Check-Host, a website that offers tools for checking the status of hosts and websites. Many other DDoS groups, including the IT Army and NoName, have previously used Check-Host to demonstrate proof of their attacks and the temporary unavailability of targeted websites.



Screenshots depicting the temporary unavailability of the websites for Israel's Mossad intelligence agency, Israel's Space Agency, and Israel's Police, following Cyber Army attacks. [Source: Telegram]

Conclusion

The rise of crowdsourced DDoS attacks marks an evolution in cybercrime, with geopolitical tensions serving as a catalyst for new threat actors. As seen during the ongoing Russia-Ukraine and Israel-Hamas conflicts, groups like the IT Army of Ukraine, NoName057(16), and the Cyber Army of Palestine capitalize on these events to launch disruptive attacks on large businesses and government entities across the world. These attacks, once the domain of well-resourced malicious actors, now also involve under-resourced novices using readily available open-source tools, and a community of enough people sympathetic to a particular political ideology or cause. The consequences of such attacks go beyond simple disruptions to a website's homepage, with rookies now having the potential ability to impact essential services like hospital portals.

It is important to highlight how these threat actors, like many others involved in DDoS attacks, often announce their targets well in advance. This provides organizations an opportunity for advance preparation by monitoring these discussions in real-time, gaining insights for proactive defense. Post-attack, this monitoring assists in attributing incidents to specific actors and a better understanding of the organization's cybersecurity landscape in terms of particular threats it faces. Given the dynamic nature of geopolitics and the ease of accessing DDoS tools and amassing a community of cybercrime volunteers, continuous surveillance across the clear, deep, and dark web, including illicit Telegram channels, is crucial for early threat detection.

About Flare

Flare is the proactive Threat Exposure Management (TEM) solution that monitors threat actor activities across the clear & dark web and illicit Telegram channels 24/7.

With customized alerts, Flare enables security teams to discover unknown events, automatically prioritize risks, and respond to actionable intelligence. Identify and respond to information relevant to your organization within cybercrime communities in real-time.

Want to learn more about better protecting your digital assets with Flare?

Sign Up for a Free Trial

flare.io

hello@flare.io