Cyber Insight

DarkStorm Team
aka: DarkStrom Team

Cyber Intelligence Bureau
a division of Epidemiology Labs

Cyberdefense

Cyberdefense

Methodology & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

The sources have been correlated, validated and qualified as trusted sources.

This insight is analysis from a strictly cyber perspective.

The whole content strictly respects the principle of neutrality, which is fundamental to the research carried out.

Cyberdefense

Dark Strom Team / Dark Storm Team

- Creation date: September 2023 (Unconfirmed)
- Strategies : Remote access - Data infiltration - Ransomwares - Unpredictable DDoS attacks
- Motivation: Financial, geopolitical, mainly pro-Palestinian - unconfirmed links with Russia highly likely - strong partnerships with other groups
- Characteristics: Ideological and financial threats, targeting of critical infrastructure, possible nation-state links
- Sectors: State organizations, Financial organizations, Air transport
- Financing: Sale of hacking services and data stolen from the dark web, a DDoS service and a target information dumping service

Identification

Coalitions

- Killnet
- Anonymous Sudan
- Ghosts of Palestine
- Bluenet Russia
- SN_BLACKMETA
- Channel DDoS v2
- ZeusAPI Services
- Krypton Networks

Cyberdefense

Key Points

1
2
3
4
5
6

Structure

Horizontal organizational structure (unconfirmed)

Plateform

Telegram: coordination and communication in English and coalitions with other groups

Financing

Financing via services : DDOS-AS-A-SERVICE, Leaks, RANSOM-AS-A-SERVICE

Tools

Remote access tools with RAT (Remote Access Trojan) for data exfiltration

Motivations

Geopolitics: Support for Palestine, Opposition to Israel, Possible links with Russia

Targeting

Targeting state organizations supporting Israel

Cyberdefense

Vectors of Influence

1

Boastfully

The group presents itself as a major player on the hacktivist scene and boasts of its exploits, seeking to impress and intimidate its targets and enable faster recruitment of attacking sympathizers.

2

Resistance

The group justifies its attacks by a strong opposition to Israel, accusing its targets of supporting this country.

3

Self-financing

Dark Storm Team offers hacking services “for hire” and sells stolen data on the darknet

4

Strategies

The group exploits the sense of injustice and anger linked to the Israeli-Palestinian conflict. Confusion and fear: Muddles the waters and maintains the mystery of its links, sowing doubt and amplifying feelings of insecurity among its victims

5

Ideology

To justify its actions, the group exploits political and religious convictions, in particular support for Palestine, to recruit and mobilize supporters..

Cyberdefense

Emotional Intelligence on victims

1 Humiliation by disrupting online services: the group aims to humiliate its victims and undermine their sense of competence

2 Fear through unpredictability: The unpredictability of attacks and potential targets generates a climate of constant fear and uncertainty

3 Anger through provocation: The group's claims and provocative messages are designed to arouse anger and impulsive reactions.

4 Powerlessness through sophistication: Faced with sophisticated attacks, victims can feel overwhelmed and powerless, undermining their confidence in their ability to protect themselves.

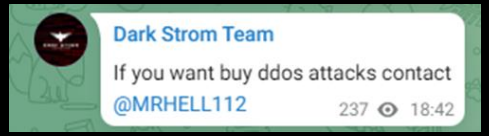
5 Injustice by focusing on sensitive causes: by exploiting them, such as the Israeli-Palestinian conflict, the group amplifies the sense of injustice and anger among its victims.

6 Suspicion and division: By blurring the trail of its real links and motivations, the group sows suspicion and division within its target communities and countries.

Cyberdefense

Tools and services

Proposals and sales of services:



- DDOS-as-a-Service:Platforms such as Channel DDoS v2, ZeusAPI Services, Krypton Networks and InfraShutdown are used.
- Virtual Private Networks (VPN): VPNs and proxy servers to mask identity and location.
- Ransom-as-a-Service
- Telegram and other social networks: These are used to spread propaganda, recruit, coordinate attacks and promote illegal services.
- Darkweb and black markets: Used to sell stolen data and promote hacking services.

Cyberdefense

Professional sectors

List of targeted sectors

- Governments
- Defense
- Airports, transport
- Education
- Financial Services
- EnergyTechnology (eg. Snapchat)
- Sensitive industries
- Media

NOTE

DarkStorm Team targets key business sectors, mainly in Israel and NATO member countries.
Increased collaboration with other hacktivist groups could make attacks more difficult to counter.

Targeted countries

Cyberdefense

The most dangerous hypotheses

Paralysis of critical infrastructures:
Dark Storm Team could paralyze key French infrastructures such as airports, power grids and financial institutions through large-scale DDoS attacks.

Deterioration of digital trust:
Increased cyberattacks and the spread of false information could undermine public confidence in French institutions and online services.

Damage to international reputation:
Successful attacks on French companies and institutions could tarnish the country's international image, affecting tourism, investment and diplomatic relations.

Instrumentalizing social tensions:
the group could exploit social tensions and political divisions in France to stir up discord and discontent, thereby weakening national cohesion

Amplifying Russian disinformation campaigns:
Dark Storm Team's alleged links with Russia could be used to amplify Russian disinformation and propaganda campaigns in France

Cyberdefense

Cyber Intelligence Bureau
a division of Epidemiology Lab

Build a safer digital society

Cyberdefense