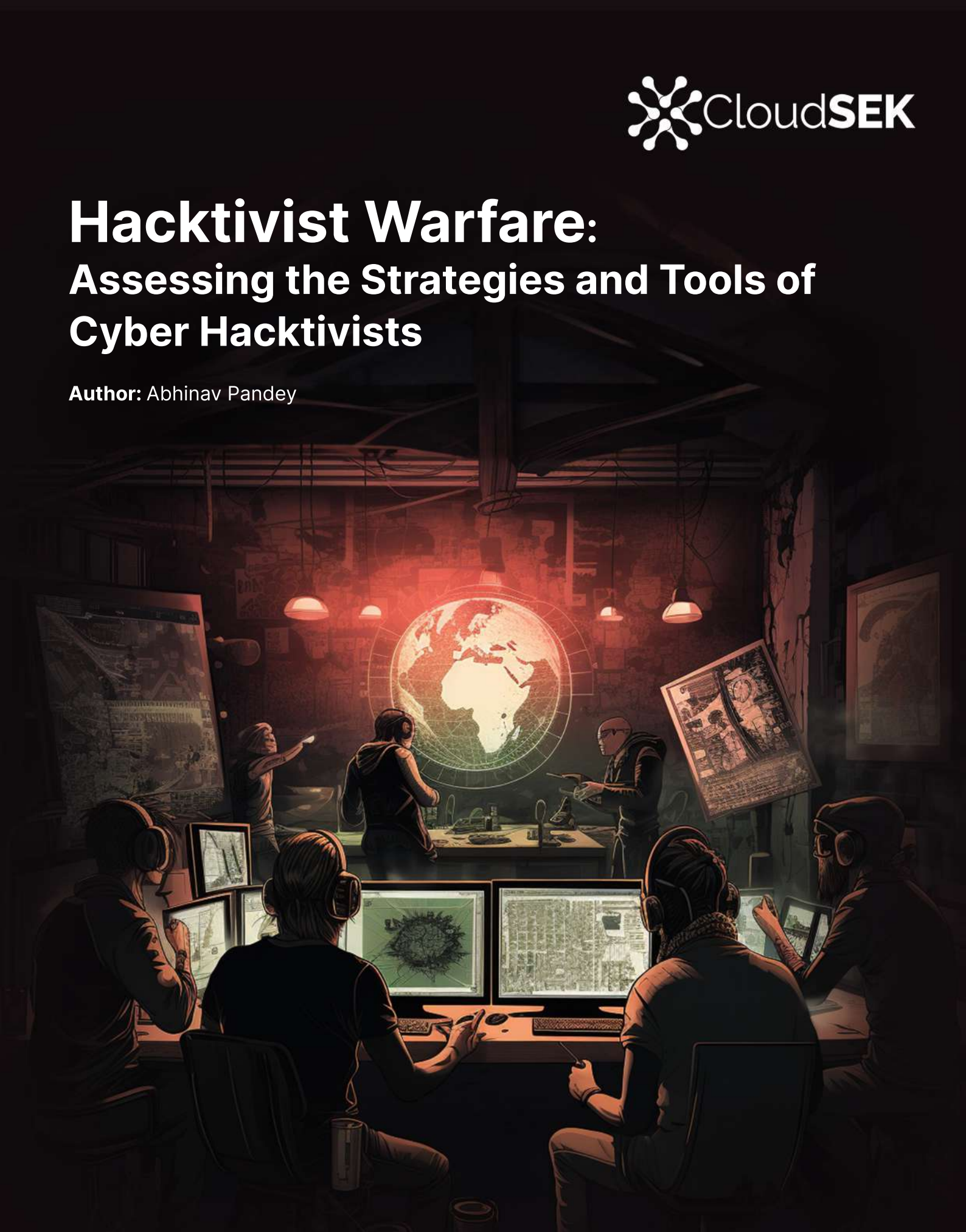
CloudSEK

Hacktivist Warfare:
Assessing the Strategies and Tools of Cyber Hacktivists

Author: Abhinav Pandey



White papers and reports can be downloaded from CloudSEK website by visiting https://cloudsek.com/whitepapers-reports or by mailing to info@cloudsek.com.

Introduction

Hacktivism, a form of cyber attack carried out in support of a social cause, has increasingly become a disguise for state-sponsored cyber attacks. It is the use of technical skills and cyber tools for digital protests and disruption to raise awareness and drive social change. It blurs the lines between cyber warfare and digital dissent, sparking ethical debates about activism in the digital age. A significant surge in such incidents during the recent quarter prompted us to conduct in-depth research on Cyber Hacktivism

This white paper provides a concise analysis of hacktivist warfare, focusing on the strategies and tools employed by cyber activists throughout much of the world. By examining the activities of **45+ hacktivist** groups across regions such as the **Indian Subcontinent, Middle East, ASEAN countries, Oceania, Europe, Brazil, and North America, & more**, we aim to uncover their motivations, techniques, and the impact they have on established power structures.

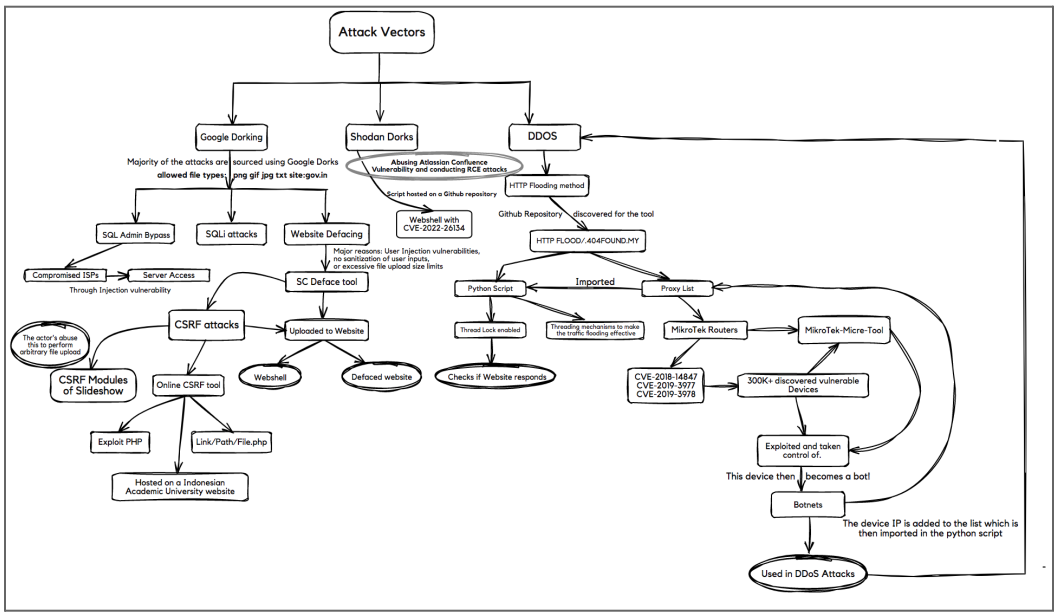


Figure: TTP Analysis of DragonForce Hacktivist Group (Intelligence Report, CloudSEK, 2022)

The paper underscores the increasing importance of hacktivist activities and the heightened threat presented by these groups as they acquire enhanced skills and resources, amplifying their capacity for inflicting greater harm and disruption in the digital as well as physical world. We draw insightful conclusions on the **attack methodologies, capabilities, and infrastructure** employed by hacktivist groups for cyber attacks. It includes an analysis of the **top targeted countries and industry** sectors, along with incident graphs illustrating the overall trends across the years. Additionally, significant instances of attacks are highlighted, providing valuable insights into future trends and predictions.

Motivations & Objectives of Hacktivist Groups

Hacktivist groups have three primary motivations for their cyber attacks: political, religious, and fame/popularity. These motivations can intertwine and change over time, highlighting the complex nature of hacktivist activities.

1. **Political:** Hacktivists target government institutions, political parties, or perceived oppressive organizations to promote their political agendas or ideologies.
2. **Religious:** Hacktivists driven by religious motivations target individuals, websites, or platforms deemed as a threat to their faith or engage in digital activism to promote their religious cause.
3. **Fame/Popularity:** While this can be considered a common motivation, Many entities seek recognition and influence by carrying out high-profile cyber attacks that garner media attention, aiming to increase their visibility and notoriety.

Hacktivist groups may use religious pretexts to cloak political motivations, employing misinformation as a driving force for attacks. These actors display geopolitical understanding, reacting strategically to decisions and initiating cyber operations against specific countries. We delve into targeted countries and industry sectors, showcasing a notable surge in hacktivist attacks recently.

Major Trends Observed in Hacktivism

The premise of the paper was that we observed an exponential increase in hacktivism activity in the Middle Eastern and Asian region followed by Europe post the Russia-Ukraine Conflict. Based on the data from Communication channels of the groups, hacktivist incidents remained below 1% compared to the global average of attacks in 2021 and 2022. **However, there was a significant spike in the first quarter of 2023, reaching up to 35% of total attacks, in April**, followed by a slight decrease in May and similar trends in June. Despite expectations of a notable increase in July 2022 due to the active campaign by the DragonForce group and its affiliates, only a minor spike was observed as the group deleted all the evidence from the communication channels following complaints filed with Interpol.

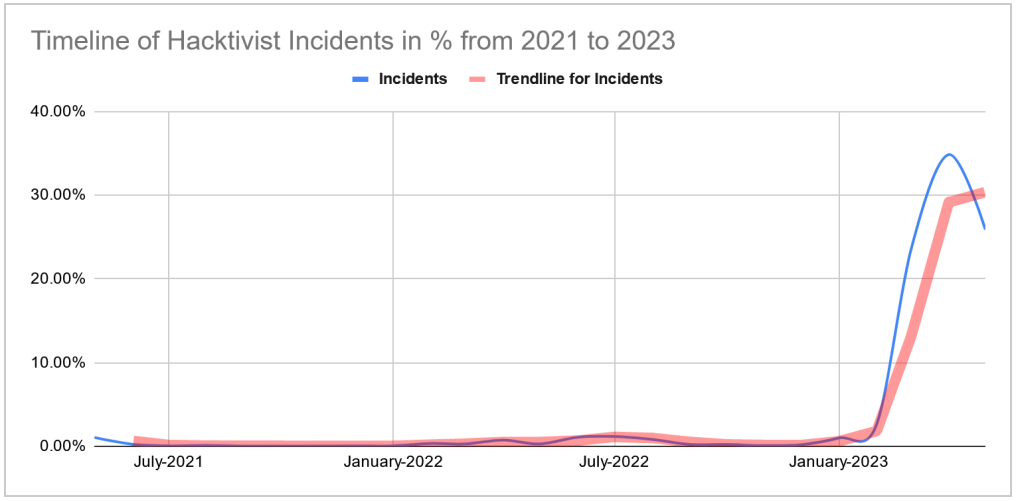


Chart showcasing the distribution of attacks across the Two Years & an Increase in 2023 by hacktivist groups

Countries Most Affected by Hacktivist Activities

Based on the data from Communication channels of the groups, spanning from 2021 to 2023, it was concluded that hacktivist groups have targeted a total of **67 countries** worldwide. Among these countries, **India emerged as the most targeted**, followed closely by **Israel, Poland, Australia, and Pakistan** and impacted various regions across the globe, including Africa, Asia, Europe, North America, South America, and Oceania, indicating a widespread presence of these cyber threats.

Countries such as **India, Israel, Denmark, and Sweden** emerged as prime targets of hacktivism due to religious motivations, while hacktivist attacks on **Poland, Ukraine, Latvia**, and others were primarily motivated by political factors. The former set of countries faced attacks mainly from hacktivist groups based in Pakistan, Bangladesh, Malaysia, and Indonesia. In contrast, the latter witnessed a higher frequency of attacks from Middle Eastern and Russian groups, including Anonymous Sudan and the Russian hacktivist group NoName057, suspected to operate from Sudan and Russia, respectively.

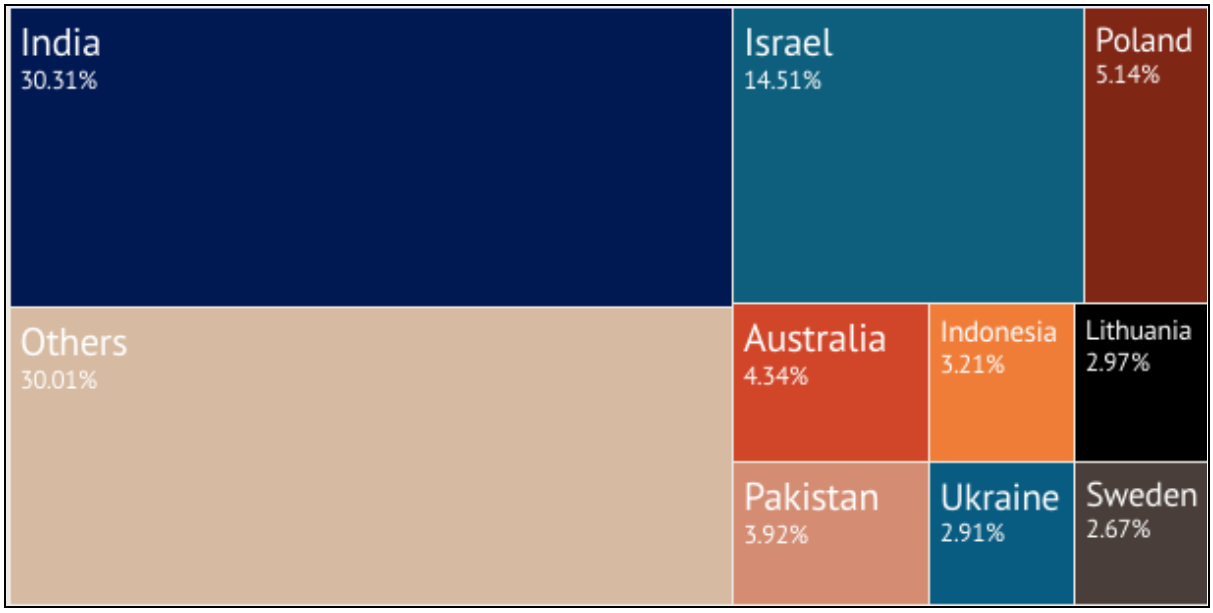
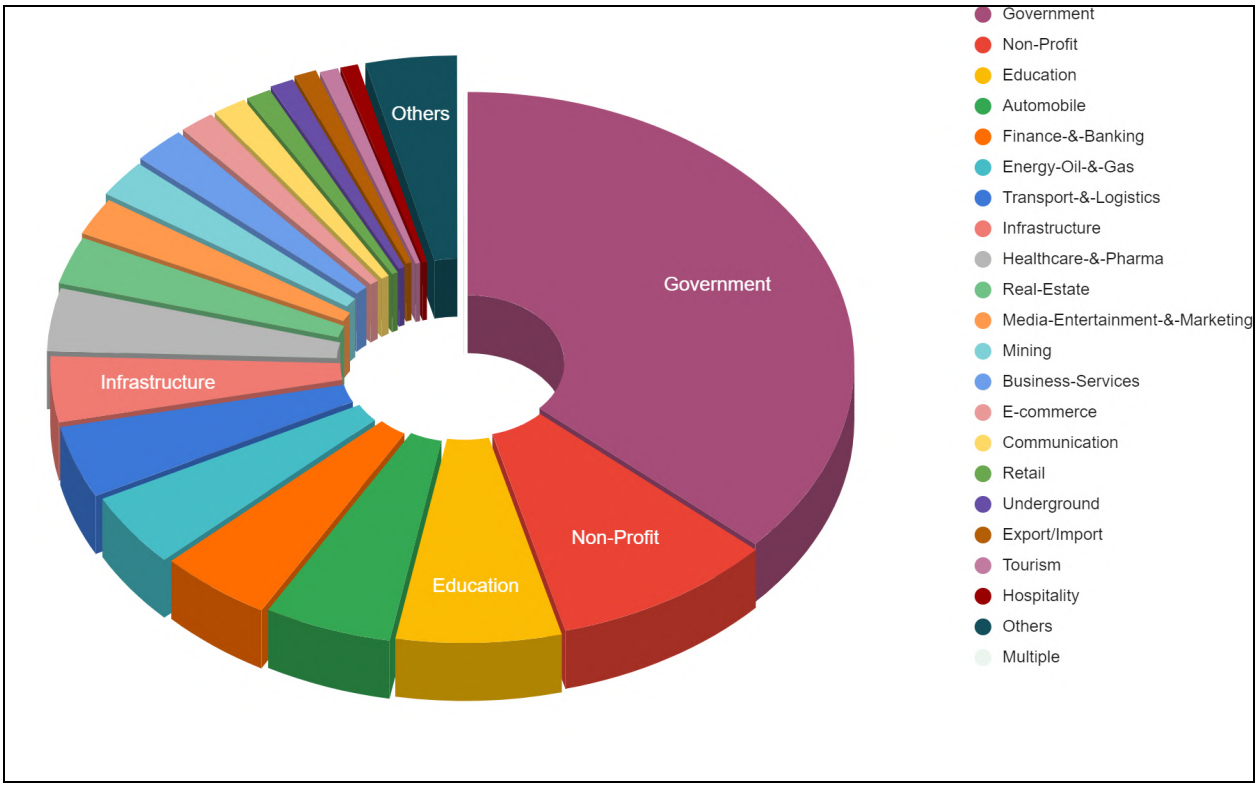


Chart showcasing the distribution of attacks across the top countries by hacktivist groups

Top Industry Sectors Targeted by Hacktivists

The Government sector faced the highest impact of hacktivist attacks, followed by the Non-Profit, Education, Automobile, Finance & Banking, and Energy-Oil & Gas sectors. **The non-profit sector was highly vulnerable and experienced many attacks,** although these attacks had relatively less impact. On the other hand, the automobile and education sectors faced **defacement, DDoS attacks, and occasional instances of alleged data leaks through the exploitation of openly available data using Google Dorking techniques**. For the Finance & Banking sector, DDoS attacks targeted their Internet banking services, while attacks on the energy sector aimed to convey messages to governments and gain popularity.



Pie chart showcasing the distribution of attacks across the top industry sectors by hacktivist groups

Tactics, Techniques, and Procedures

Our research suggests that hacktivist groups employed similar TTPs across regions to target countries, primarily using four primary types of attacks. The image and table below provide a breakdown of these TTPs.

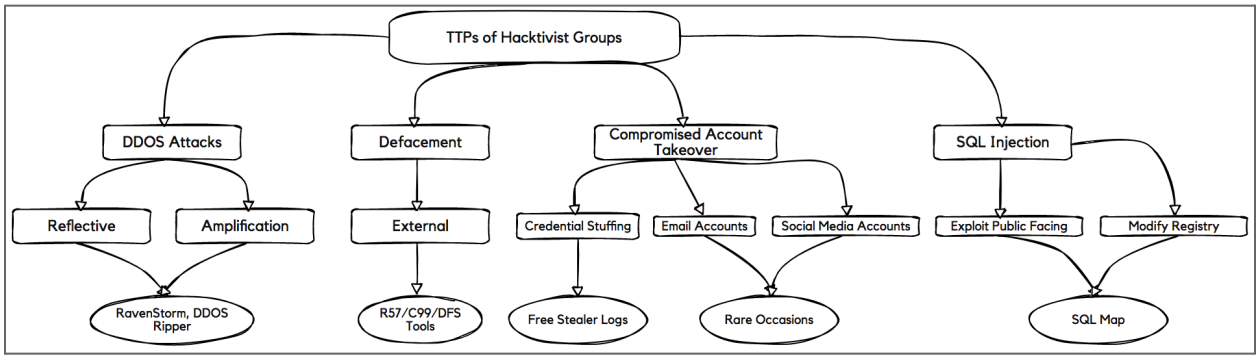


Figure: Overview of TTP of Hacktivist Groups

Attack Type	Information	Mitigation
DDOS Attacks		
HTTP Floods	The attack is generated by sending HTTP GET or POST requests to cause denial on the target webserver.	Track abnormal traffic on the server and implement progressive challenges that can help mitigate the sudden surge of traffic.
DNS Amplification	The attack is generated by turning initially small DNS queries into a much larger payload. Thus taking down the DNS server which enables the resolution of Domain Name.	Rate Limiting or Blocking attacking DNS servers and opening DNS recursive relay servers.
UDP Flood	The attack is generated by connecting random ports with large numbers using the UDP protocol.	Rate limiting the ICMP Responses.
SYN Flood	The attack is generated by exploiting the common TCP three-way handshake.	IPS service should help in detecting and blocking abnormal SYN attacks.
NTP Amplification	The attack is generated by exploiting publically available Network Time Protocol Servers.	Disable NTP server responses to requests from outside the network, enabling rate limiting, and restricting access to trusted clients.
Defacement Attacks		
External Defacement	External defacement involves unauthorized modification or alteration of a target's publicly accessible website or web page to convey messages, spread propaganda, or protest against specific organizations or ideologies.	Implement strict access controls and monitoring mechanisms to detect and prevent unauthorized alterations to the website. Regularly scan and backup website content to quickly restore in case of defacement
Compromised Account Takeover		
Credential Stuffing	Hackers systematically test stolen username and password combinations across multiple platforms and services to gain unauthorized access to accounts usually sourced through Stealer Logs	Enforce strong password policies, implement multi-factor authentication, and monitor for suspicious login attempts to detect and prevent credential stuffing attacks. Enable Visibility over Stealer Logs (Read: Link)
Email Accounts	Hacktivists engage in unauthorized access and control of compromised email accounts, often showcasing their access without further escalation.	Secure email accounts with strong passwords, enable two-factor authentication, and educate users about phishing risks to prevent unauthorized access.
Social Media Accounts	Hacktivists target social media accounts for unauthorized access and control to spread their messages, ideologies, or protests.	Secure social media accounts with strong passwords, enable two-factor authentication, and closely monitor for unusual activities to prevent unauthorized access.
SQL Injection		
SQL Injection	Malicious SQL code is inserted through input fields to manipulate databases and access sensitive data, where targets are sourced using G-Dorks Use of Automated tools such as SQLMap	Use parameterized queries, employ web application firewalls, keep systems updated, conduct security assessments, and educate developers on secure coding practices.

Short Duration DDoS Attacks

The log file analysis confirmed CloudSEK's hypothesis that the hacktivist possesses DDoS capabilities **lasting for 1-2 minutes**, as determined through the examination of the time frame within the log files. This holds true for the majority of the hacktivist groups with a few **exceptions of Anonymous Sudan** and more.

Log File Time Snapshot: The left image shows the start of the attack, while the right image indicates its completion.

- The observed log file timestamps indicate that the attack commenced at 09:19:52 and concluded at 09:20:59, providing evidence of the hacktivist group's ability to execute DDoS attacks within a **timeframe of 1-2 minutes.**
- Furthermore, the groups have demonstrated a tendency to **target Layer 7**, specifically the **application layer** of the OSI model. This choice is based on the effectiveness of DDoS attacks at this layer and the **increased visibility of such attacks** on the Check Host website for monitoring downtime. Likewise, the **presence of GET requests** in the log files **confirms** the execution of a **Layer 7 attack** in this specific instance.

Tools & Techniques

Although the tools and techniques used by different hacktivist groups varied across different regions, however the below table provides an overview of the commonly employed techniques.

DDOS Attacks		
Tool Name	**Employed by**	**Analysis**
Stresser7	Dragon Force & its Subsidiaries	Tool utilized 4300 user agents & SOCKS proxies for anonymous DDoS attacks, with custom packet creation and proxy management.

		Proxies sourced from APIs & GitHub, using code obfuscation for evasion.
ECC Tool	Eagle Cyber Crew & Its Partners	Obfuscated main DDoS function and a proxy text file. Obfuscation used to conceal core functionality, making the tool's purpose and behavior harder to understand.
Raven Storm	Dragon Force, Mysterious Team Bangladesh	Python-based tool for multi-layer DDoS attacks. Supports L3 (ping), L4 (UDP/TCP services), and L7 (Websites) DDoS attacks. Can create a small botnet with a server mode, enabling multiple instances of raven-storm to connect.
Xerxes	Mysterious Team Bangladesh & Its Partners	Simple C program used by 'Jester' to DDoS WikiLeaks. Gained popularity due to its effectiveness. Maintains a full TCP connection and requires only a few hundred requests at regular intervals for the attack.
DDOS Ripper	Team Herox, Team Insane PK	Obfuscated Python Script, Uses predefined user agents and bots. Configurable target IP, port, and turbo (threads). Establishes TCP connections and sends random HTTP GET requests. Supports multithreading for intensified attacks.
Compromised Account Takeovers		
Source Name	**Employed by**	**Analysis**
Stealer Logs (Bradmax, Free Cloud Logs)	Hacktivist Indonesia, Anonymous Operation Vendetta, Kerala Cyber Xtractors	Stealer logs: Malicious tools to steal sensitive data. Capture: Keystrokes, clipboard, browser history, cookies. Hacktivist groups obtain for free from Telegram. Used to gain unauthorized access to organizations. CloudSEK has exclusive stealer log sources for Customers to Monitor
Defacement Attacks		
Tool Name	**Employed by**	**Analysis**
R57/C99 Shells	Ghost Sec, Turk Hack Team, Seiged Sec, KoLzSec, Jambi Cyber Team, 177 Members Team, OneFourOne, Team Insane PK, Dragon Force, Mysterious Team Bangladesh & More	R57 and C99: Web shells for executing commands on compromised servers. R57: PHP-based shell from Russia. C99: Another popular PHP web shell. Dorking: Technique used to search for vulnerable servers. Attackers gain control with R57/C99 to manipulate website files. Actions include injecting malicious code, defacement, and redirection.
DragonForceShell (DFS)	Dragon Force Malaysia & Its Subsidiaries	DF shell script: Scans server directories, retrieves files in tabular format. Allows file uploads with $_FILES variable and validation. Exploited in defacement attacks, enabling image/logo uploads. Includes options for file and directory deletion (unlink() and rmdir() functions). Uses authentication with username and password.
SQL Injection		

SQLMap	Cyber Skeleton, NDT Sec, Anonymous Cambodia, TYG Team, FR3DENS of Security, Indian Cyber Force, Black Dragon Sec, Team Insane PK, Team Herox	Vulnerable Sites sourced using Google Dorks Open-source tool for finding and exploiting SQL injection vulnerabilities. Automates the process of detecting and extracting database information. Supports multiple database systems and offers customizable exploitation techniques.
Proxies for DDoS Attacks		
Tool Name	**Employed by**	**Analysis**
Mikrotik Routers	Dragon Force Malaysia & Its Subsidiaries, Groups in South East Asia	Part of Meris Botnet, Commonly used devices for DDoS routing: Mikrotik Routers, Squid HTTP Proxy V3.3.8. Extensively used MikroTik Products: RouterOS API Service, HTTP proxy, router FTPD, bandwidth-test server, and more. MikroTik bandwidth server vulnerable to multiple CVEs (CVE-2022-0778, CVE-2022-36760, CVE-2022-29404, and others). Previous year's hacktivist campaign exploited CVE-2018-14847, CVE-2019-3977, and CVE-2019-3978.

Discovered Proxy Lists

Free and open APIs and github repositories filled with overlapping proxies were being used by the groups for their attacks, hence we can infer that most of these hacktivism groups are less sophisticated and prefer free tools over paid stresser/DDoS services. While most groups used free and open-source proxies there were exceptions such as Anonymous Sudan and other Russian affiliated hacktivist groups such as NoName057, Killnet, Phoenix etc which exhibited the capacity to run DDoS attacks for multiple hours (in some cases even up to ~10 hrs)

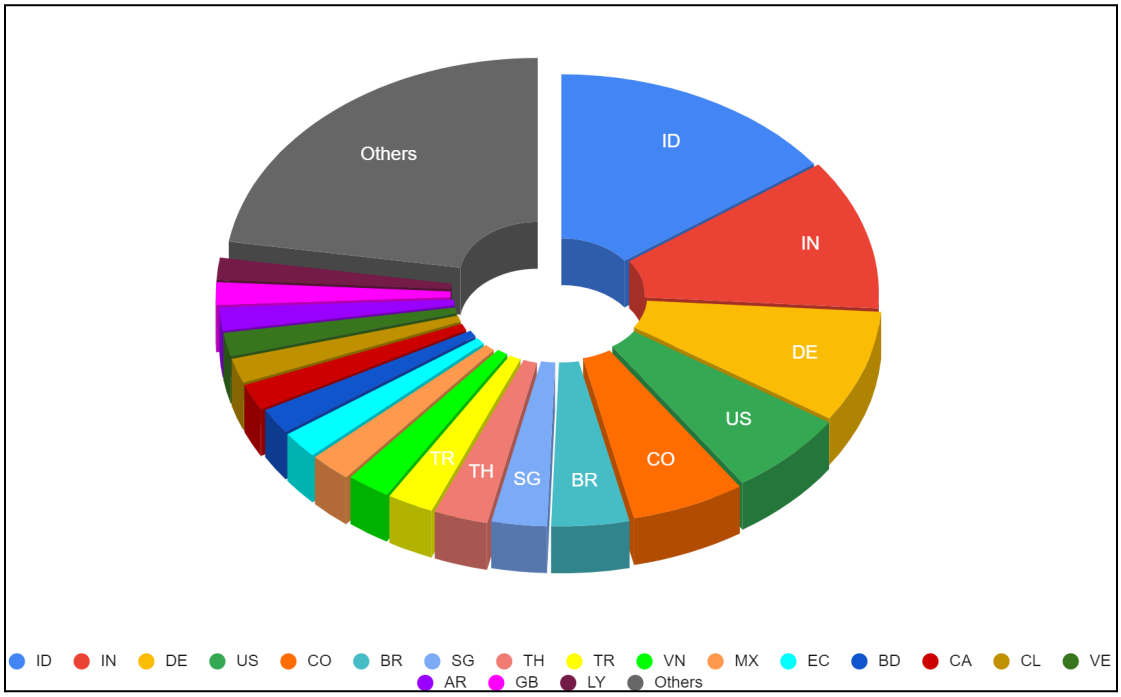
Availability of freely and open source proxies aid the DDoS Ecosystem. Different proxies that we discovered during the course of our research included Sock proxies, HTTP Proxies and more. Some examples are:

- hxxps[:]//api[.]proxyscrape[.]com/v2/?request=getproxies&protocol=socks5&timeout=10000&country=all&simplified=true
- hxxps[:]//api[.]openproxylist[.]xyz/hxxp[.]txt

Please Note: *You can find an exhaustive list of proxy lists we discovered while analyzing tools used by these groups in the Appendix section of this paper. The IP addresses we found can be considered as IOCs.*

Geolocation Patterns & ASN Data:

The geolocation analysis of unique IP addresses from the traffic logs revealed that Indonesia accounted for the largest share, representing 16.8% of the total IPs. Following Indonesia, significant contributions came from India, Germany, Colombia, the United States, and Britain.



Snapshot of distribution of unique IPs based on countries.

In terms of ASNs, the majority of the hosted IP addresses were attributed to DigitalOcean, LLC, comprising 17.3% of the total. Following DigitalOcean, other notable contributors included AS5381, AS262186 TV AZTECA SUCURSAL COLOMBIA, AS45629 JasTel Network International Gateway, and AS13489 EPM Telecomunicaciones S.A. E.S.P.

In the case of ASN & Geolocation data, the data set used for analysis was limited in comparison to the tools & proxies being used and the number of hacktivist groups. This section represents a subset of the complete picture.

Case Studies

In this section, we highlight notable cases of hacktivist campaigns. This includes the attack on SAS airlines, attacks on Microsoft Services, attacks on UAE Infrastructure & Indian banks and police websites.

Attack on the SAS

Scandinavian Airlines, more commonly known and styled as SAS, the flag carrier of Denmark, Norway, and Sweden was targeted with DDoS Attacks by a prominent hacktivist group known as Anonymous Sudan. The group targeted carriers' websites, including baggage reporting and boarding card printing, with DDoS attacks. This case was specifically interesting because general hacktivism activity does not originate from financial motivation.

a. They demanded a ransom that escalated over time, marking the first instance of a hacktivist group seeking payment to cease the attacks. The services were reportedly disrupted for a duration of 9 days.
b. The attack on the airlines was conducted with religious motivations.

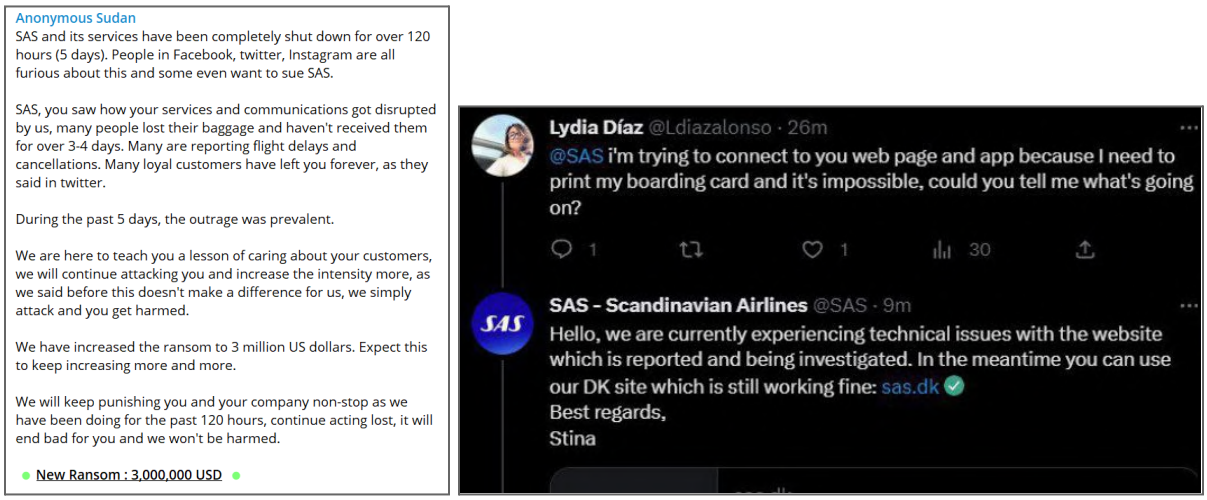


Figure: Snapshot of a ransom note of the group & user complaining about the disruption of service

Attack on Microsoft Services

The same group conducted a campaign against Microsoft services disrupting Microsoft Outlook & Azure majorly in addition to short-term attacks on Bing, Onedrive, & Microsoft sign-up service.

a. The attack initially started with Sudanese hackers supporting Russian hackers but eventually came under the complete control of Anonymous Sudan, which is a member group of Killnet, a prominent Russian hacktivist group.

b. Killnet serves as an umbrella organization for multiple hacktivist groups, and Anonymous Sudan was included as a member group for their targeting of Swedish, Danish, and other European countries.

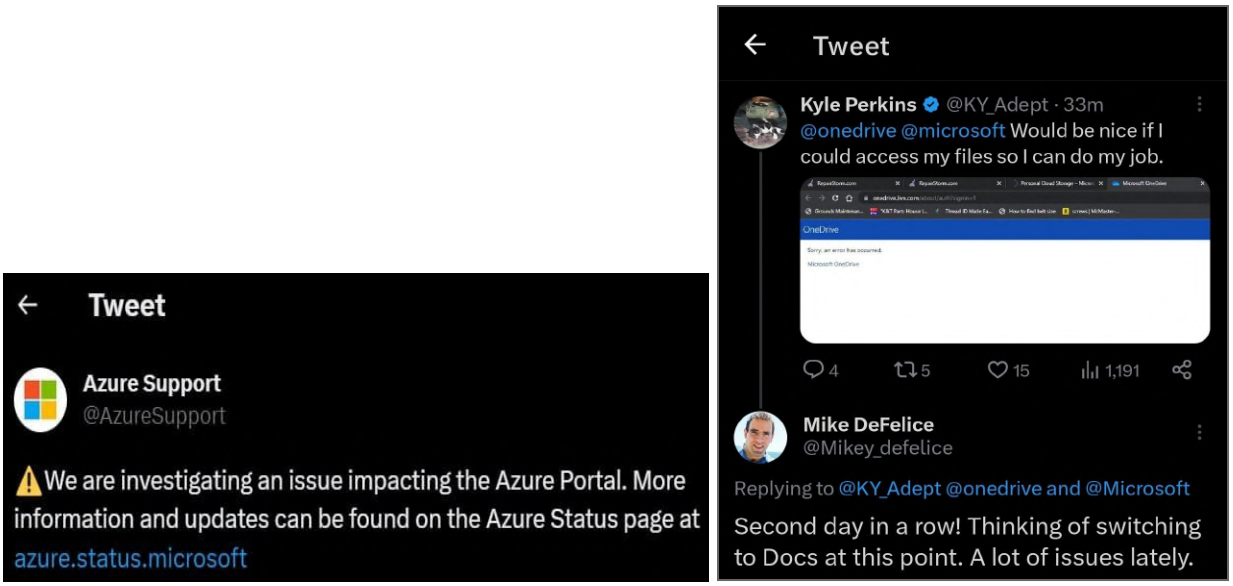


Figure: Snapshot of Azure Support Tweet & User complaining about the disruption of services

Attack on the Indian Banking & Police Infrastructure

A Pakistan-based hacktivist named Team Insane PK conducted a DDoS attack on the Indian banking & Finance and Police infrastructure websites.

a. The hacktivist group claimed responsibility for DDoS attacks on 44 banking and finance websites, although only 16 of them were observed to be actually affected.
b. While a majority of the attacks conducted by the hacktivists are religiously motivated, this attack was likely done in retaliation to the cyber warfare occurring between Indian hacktivist teams like team UCC operations, Indian Cyber Force, and CyberXForce, and hacktivist teams belonging to Pakistan and Malaysia.
c. The same actor conducted a DDoS attack on 23 Indian Police Department websites.

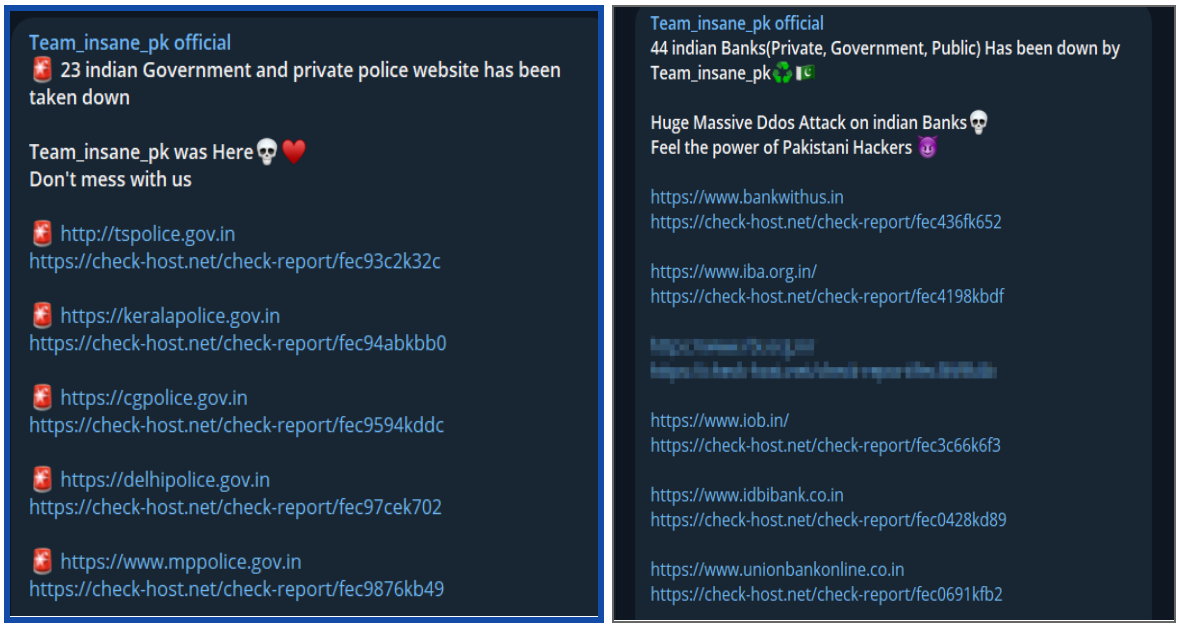


Figure: Snapshot from the group's Telegram Channel (CloudSEK)

Attack on the UAE's Infrastructure

The Anonymous Sudan group conducted a DDoS attack campaign against the UAE's infrastructure in retaliation to the UAE's support for the Rapid Support Forces as mentioned by the Hacktivist Group.

a. This included attacks on numerous government ministries such as the Interior Ministry, health & prevention, education, foreign affairs, and International Cooperation, & the government portal. Other entities targeted included Dubai & AbuDhabi municipalities, police, Dubai Airport, First Abu Dhabi Bank's website and app, Mashreq Bank, RAKBANK & Emirates NBD bank.

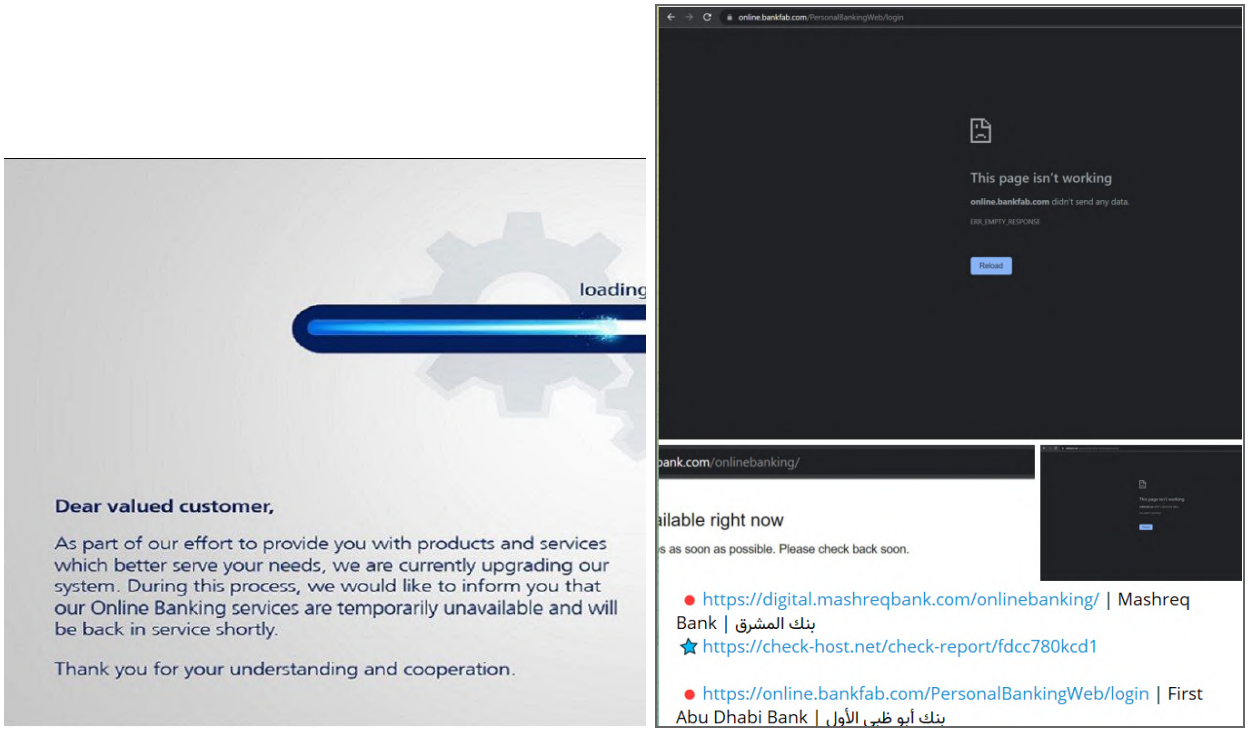


Figure: Snapshot of Emirates NBD bank website disruption & the DDoS attack claim of the hacktivist group

Conclusion

In conclusion, hacktivism remains a significant force in cybersecurity, targeting government agencies, corporations, and high-profile entities through tactics like DDoS attacks, defacements, and data breaches. India, Israel, Poland, Australia, and Pakistan were the most targeted countries, with a focus on government entities and various sectors. Hacktivist groups demonstrate DDoS attack capabilities of 1-2 minutes using current tools with few exceptions

Looking ahead, hacktivists will intensify collaboration, forming alliances and sharing resources for more impactful attacks. Data breaches and leaks will be a growing focus, posing increased risks to organizations. Social media and online forums will play a crucial role in recruitment and coordination. While the hacktivist landscape is ever-evolving, these trends provide valuable insights into the future of hacktivist activities.

Through our research, we extensively examined the tools and technologies employed by hacktivist groups during their campaigns. Additionally, we conducted a time trend analysis, revealing a recent increase in hacktivist incidents. We discussed the impact and consequences of such attacks and provided comprehensive mitigation strategies for DDoS attacks, defacement attacks, SQL injection, and

compromised account takeovers. Moreover, we offered recommended security measures to defend against hacktivist attacks.

To illustrate real-world examples, we examined notable hacktivist case studies, including the attacks on SAS airline, Microsoft, Indian banks, and UAE's infrastructure. These case studies provide valuable insights into the nature and consequences of hacktivist activities.

Hence, the impact of hacktivist attacks can be far-reaching, causing disruptions to services, reputational damage, and financial losses for the targeted organizations. Additionally, compromised accounts and stolen data pose risks to individual privacy and security.

To defend against hacktivist attacks, organizations should implement a range of security measures, including regular security assessments, incident response planning, employee training, network segmentation, threat intelligence, and disaster recovery protocols.
Looking ahead, the hacktivism landscape is expected to witness continued collaboration and coordination among hacktivist groups, leading to larger and more sophisticated attacks. The focus on data breaches and leaks is also likely to increase, making government agencies, corporations, and other entities more vulnerable.

Appendix

Discovered Proxy List
Sock Proxy APIs
https://api.proxyscrape.com/v2/?request=getproxies&protocol=socks5&timeout=10000&country=all&simplified=true
https://www.proxy-list.download/api/v1/get?type=socks5
https://www.proxyscan.io/download?type=socks5
https://raw.githubusercontent.com/TheSpeedX/PROXY-List/master/socks5.txt
https://raw.githubusercontent.com/hookzof/socks5_list/master/proxy.txt
https://raw.githubusercontent.com/andigwandi/free-proxy/main/proxy_list.txt
https://raw.githubusercontent.com/ErcinDedeoglu/proxies/main/proxies/socks5.txt
https://raw.githubusercontent.com/ErcinDedeoglu/proxies/main/proxies/socks4.txt
https://raw.githubusercontent.com/hookzof/socks5_list/master/proxy.txt
https://raw.githubusercontent.com/ShiftyTR/Proxy-List/master/socks5.txt
https://raw.githubusercontent.com/jetkai/proxy-list/main/online-proxies/txt/proxies-socks5.txt
https://api.openproxylist.xyz/socks5.txt
https://openproxylist.xyz/socks5.txt
https://proxyspace.pro/socks5.txt
https://raw.githubusercontent.com/B4RC0DE-TM/proxy-list/main/SOCKS5.txt
https://raw.githubusercontent.com/manuGMG/proxy-365/main/SOCKS5.txt

https://raw.githubusercontent.com/mmpx12/proxy-list/master/socks5.txt
https://raw.githubusercontent.com/roosterkid/openproxylist/main/SOCKS5_RAW.txt
https://raw.githubusercontent.com/saschazesiger/Free-Proxies/master/proxies/socks5.txt
https://api.proxyscrape.com/v2/?request=getproxies&protocol=socks4
https://openproxylist.xyz/socks4.txt
https://proxyspace.pro/socks4.txt
https://raw.githubusercontent.com/B4RC0DE-TM/proxy-list/main/SOCKS4.txt
https://raw.githubusercontent.com/jetkai/proxy-list/main/online-proxies/txt/proxies-socks4.txt
https://raw.githubusercontent.com/mmpx12/proxy-list/master/socks4.txt
https://raw.githubusercontent.com/roosterkid/openproxylist/main/SOCKS4_RAW.txt
https://raw.githubusercontent.com/saschazesiger/Free-Proxies/master/proxies/socks4.txt
https://raw.githubusercontent.com/ShiftyTR/Proxy-List/master/socks4.txt
https://raw.githubusercontent.com/TheSpeedX/PROXY-List/master/socks4.txt
https://www.proxy-list.download/api/v1/get?type=socks4
https://www.proxyscan.io/download?type=socks4
https://api.proxyscrape.com/?request=displayproxies&proxytype=socks4&country=all
https://api.openproxylist.xyz/socks4.txt

HTTP Proxy APIs & Repositories

https://api.proxyscrape.com/?request=displayproxies&proxytype=http,
https://www.proxy-list.download/api/v1/get?type=http,
https://www.proxyscan.io/download?type=http,
https://raw.githubusercontent.com/TheSpeedX/PROXY-List/master/http.txt,
https://api.openproxylist.xyz/http.txt

HTTP API Proxies

https://api.proxyscrape.com/?request=displayproxies&proxytype=all
https://www.proxy-list.download/api/v1/get?type=http
https://www.proxyscan.io/download?type=http
https://raw.githubusercontent.com/TheSpeedX/PROXY-List/master/http.txt
https://api.openproxylist.xyz/http.txt
https://raw.githubusercontent.com/ShiftyTR/Proxy-List/master/proxy.txt
http://alexa.lr2b.com/proxylist.txt
https://raw.githubusercontent.com/jetkai/proxy-list/main/online-proxies/txt/proxies.txt
https://raw.githubusercontent.com/sunny9577/proxy-scraper/master/proxies.txt
https://multiproxy.org/txt_all/proxy.txt
https://raw.githubusercontent.com/roosterkid/openproxylist/main/HTTPS_RAW.txt
https://raw.githubusercontent.com/UserR3X/proxy-list/main/online/http.txt
https://raw.githubusercontent.com/UserR3X/proxy-list/main/online/https.txt
https://openproxylist.xyz/http.txt
https://proxyspace.pro/http.txt
https://proxyspace.pro/https.txt
https://raw.githubusercontent.com/aslisk/proxyhttps/main/https.txt
https://raw.githubusercontent.com/mertguvencli/http-proxy-list/main/proxy-list/data.txt
https://raw.githubusercontent.com/mmpx12/proxy-list/master/http.txt
https://raw.githubusercontent.com/mmpx12/proxy-list/master/https.txt
https://raw.githubusercontent.com/proxy4parsing/proxy-list/main/http.txt
https://raw.githubusercontent.com/saisuiu/uiu/main/free.txt
https://raw.githubusercontent.com/saisuiu/uiu/main/cnfree.txt
https://rootjazz.com/proxies/proxies.txt

Figure: Log Snapshot from Dark Web Russian Marketplace

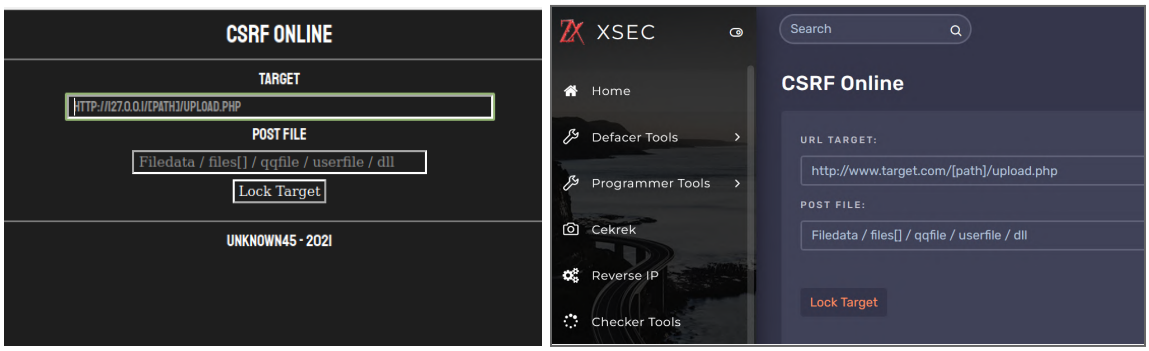


Figure: Tool Snapshot of Deface tools used during the campaign (CSRF Online hosted on Indonesian University website)

Google Dorks	
inurl:/admin/upload/ : Ministry of Knowledge & Resource sharing	inurl: /login/login.php admin: For Admin logins into websites using PHP language
"allowed file types: png gif jpg txt site:gov.in" : Google dork to upload shell html files into the server	php?id= site:in: Indian sites with ID parameter that can be abused and URL manipulation could be performed
inurl/mnux = campus login : Academic institutions with Campus login parameter	inurl/mnux = academic login : Academic institutions with Academic login parameter
inurl/mnux = administrative academic login : Academic institutions with Administrative academic login parameter	inurl: /admin/cp.php : Reveals all sites with Control panel which can provide access to the server.
inurl:admin/upload.php : For sites with upload feature that actors could exploit for shell using script deface	

Figure: Dorks Used by Hacktivist Groups (CloudSEK, 2022)

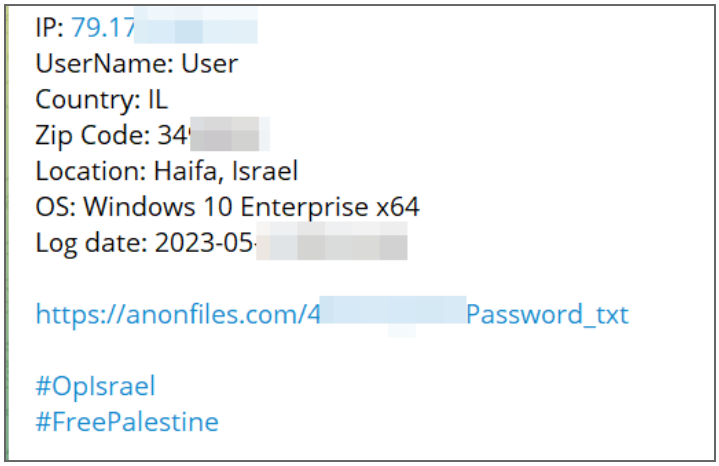


Figure: Snapshot from the Hacktivists Telegram Channel sharing accesses.

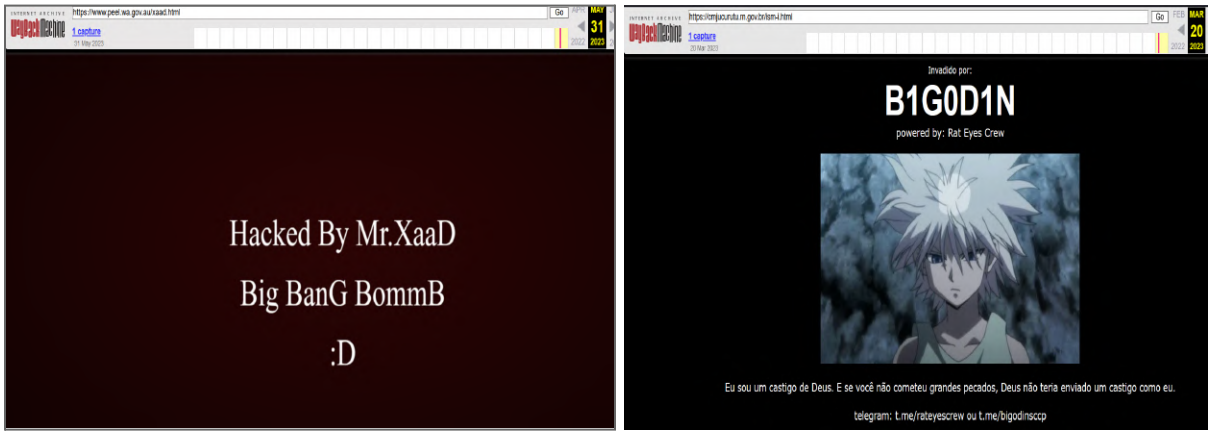


Figure: Snapshot of Web Archive of Defaced Website of Australian & Brazilian Government

CloudSEK

We Predict Cyber Threats

Initial Attack Vector Protection Platform

Founded in **2015**

150+ *CloudSters*

2 Offices *HQ in Singapore and R&D in India*

170+ *Clients Globally*

4 *Products*

We secure some of the Fortune 500 and Unicorns

... And we are backed by eminent investors

Accelerated by

NVIDIA INCEPTION PROGRAM

NETAPP EXCELLERATOR

CloudSEK is a **Customer First** Company

We are a **Gartner Peer Insights Customer First Vendor** for Security Threat Intelligence Products and services.

Schedule A Demo

To learn more about how the **CloudSEK Initial Attack Vector Protection Platform** can strengthen your external security posture and deliver value from Day 1, visit **https://cloudsek.com/** or drop a note to **info@cloudsek.com**.

CloudSEK
www.cloudsek.com
info@cloudsek.com