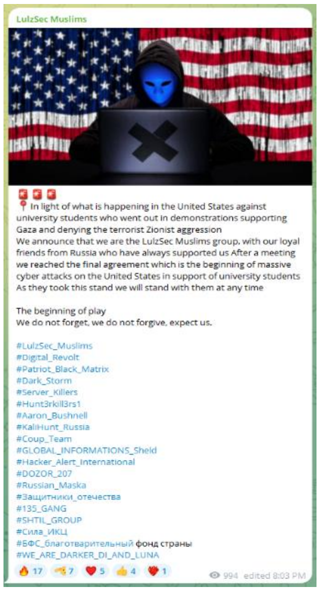
May 6, 2024

Pro-Palestinian Hacktivists Target US Education and Finance Sectors in "Cyber Price Tag" DDoS Campaign

Overview

- Radware assesses with moderate confidence that U.S. universities and financial services may face an increased risk of cyberattacks by pro-Palestinian hacktivist groups including DDoS, defacement and data theft in the coming weeks.
- This assessment is based on recent college campus tensions and protests related to the Israeli-Palestinian conflict, which could potentially motivate retaliatory cyberattacks.
- These cyberattacks aim to disrupt operations and serve as a “cyber price tag" for not aligning with Palestinian interests.



LulzSec Muslims

📍 In light of what is happening in the United States against university students who went out in demonstrations supporting Gaza and denying the terrorist Zionist aggression
We announce that we are the LulzSec Muslims group. with our loyal friends from Russia who have always supported us After a meeting we reached the final agreement which is the beginning of massive cyber attacks on the United States in support of university students
As they took this stand we will stand with them at any time

The beginning of play
We do not forget, we do not forgive, expect us.

#LulzSec_Muslims
#Digital_Revolt
#Patriot_Black_Matrix
#Dark_Storm
#Server_Killers
#Hunt3rkill3rs1
#Aaron_Bushnell
#KaliHunt_Russia
#Coup_Team
#GLOBAL_INFORMATIONS_Sheld
#Hacker_Alert_International
#DOZOR_207
#Russian_Maska
#Защитники_отечества
#135_GANG
#SHTIL_GROUP
#Сила_ИКЦ
#БФС_благотварительный фонд страны
#WE_ARE_DARKER_DI_AND_LUNA

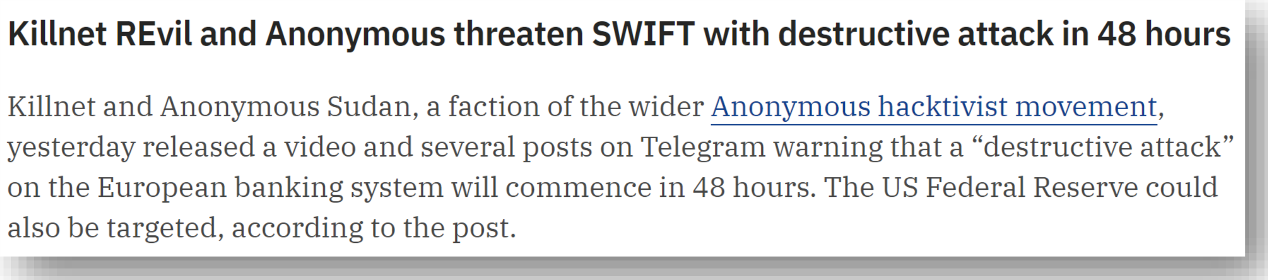
🔥 17 📣 7 ❤ 5 👍 4 ❤ 1 994 edited 8:03 PM

Figure 1: Lulzsec Muslims Telegram post announcing pro-Palestine campaign

Background

KillNet's Reactionary Attacks

On June 14, 2023, the Killnet, REvil and Anonymous Sudan hacker groups announced their plan to launch a major cyberattack on the European financial system. The hackers' motive was political and tied to the ongoing conflict in Ukraine. They aimed to disrupt the financial system by cutting off funds that support Ukraine's military. The alliance reportedly attacked the European Investment Bank.



Killnet REvil and Anonymous threaten SWIFT with destructive attack in 48 hours

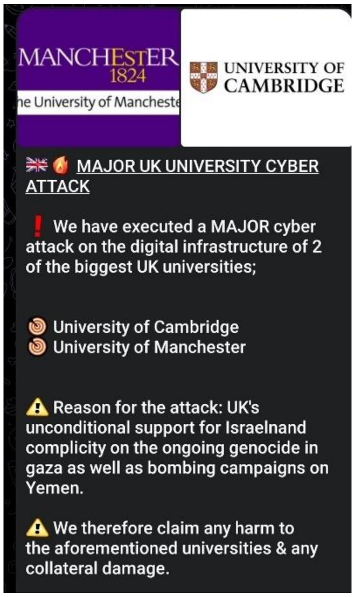
Killnet and Anonymous Sudan, a faction of the wider Anonymous hacktivist movement, yesterday released a video and several posts on Telegram warning that a "destructive attack" on the European banking system will commence in 48 hours. The US Federal Reserve could also be targeted, according to the post.

Figure 2: Tech Monitor report on hacktivist plans to target financial systems

This approach has also been adopted by pro-Palestinian hacktivists, who use distributed denial of service (DDoS) attacks to target institutions in countries that do not align with their geopolitical interests.

Anonymous Sudan's Attack on UK Universities

On February 20, 2024, Anonymous Sudan, a pro-Palestinian hacktivist group, targeted the networks of Cambridge University and the University of Manchester to demonstrate their willingness to attack academic institutions perceived as aligning with Israeli interests.



🇬🇧🔥 MAJOR UK UNIVERSITY CYBER ATTACK

❗ We have executed a MAJOR cyber attack on the digital infrastructure of 2 of the biggest UK universities;

🎯 University of Cambridge
🎯 University of Manchester

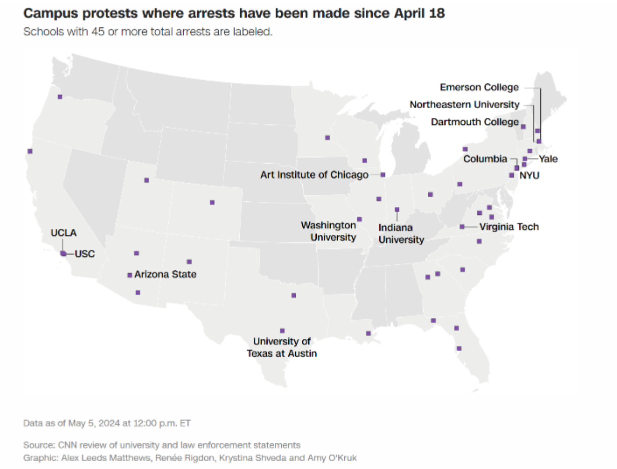
⚠️ Reason for the attack: UK's unconditional support for Israelnand complicity on the ongoing genocide in gaza as well as bombing campaigns on Yemen.

⚠️ We therefore claim any harm to the aforementioned universities & any collateral damage.

Figure 3: Anonymous Sudan post claiming attacks on U.K. universities

April 2024 Pro-Palestinian Protests

In April 2024, significant organized and orchestrated pro-Palestinian protests occurred at least six universities, including Columbia University, New York University (NYU), Northeastern University and the University of Pennsylvania (UPenn). These protests, largely driven by the ongoing conflict in Gaza and broader Israeli-Palestinian tensions, resulted in over 1,200 arrests of pro-Palestinian activists, most of whom were not university students. Demonstrators demanded that universities cut ties with companies connected to Israel and expressed disapproval of U.S. military support for Israel. Demonstrations started peacefully but soon led to clashes with pro-Israel supporters and required forceful police interventions and many arrests.


Campus protests where arrests have been made since April 18

Schools with 45 or more total arrests are labeled.

Data as of May 5, 2024 at 12:00 p.m. ET

Source: CNN review of university and law enforcement statements
Graphic: Alex Leeds Matthews, Renée Rigdon, Krystina Shveda and Amy O'Kruk

Figure 4: CNN graphic indicating campus protest arrests

Failed Negotiations and Expected Increase in Pressure

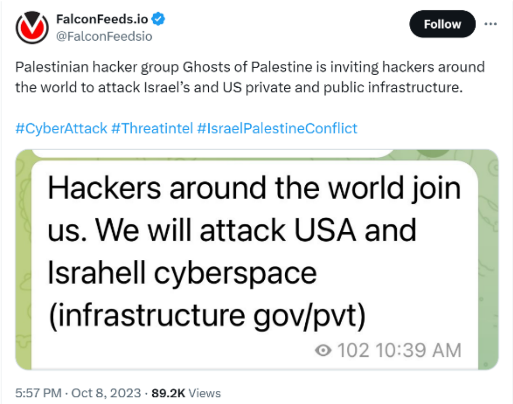
On May 6, ongoing negotiations between Israel and Hamas failed after Hamas refused to accept an American proposal to which Israel had reportedly agreed. The Chief of the General Staff of the IDF announced the beginning of the operation to eradicate the terrorist organization Hamas from Rafah. Consequently, the pressure from hacktivists is expected to increase against Israeli entities, particularly against organizations in allied countries and entities supporting Israel.

Threat Actors Likely to Participate

Anonymous Sudan: This group has actively engaged in multiple DDoS attacks targeting various entities, such as Israel’s top oil refinery operator, BAZAN Group, and the Thuraya Mobile Satellite Communications Company. Their attacks have caused significant network disruptions, confirming their capability and intent to leverage DDoS tactics against high-profile targets (Hackread).

Dark Storm Team: Although primarily known for a broader range of cyber activities, this group has claimed responsibility for DDoS attacks against significant targets like John F. Kennedy International Airport in New York. Their operations are indicative of both political and commercial motivations (SecurityScorecard).

Ghosts of Palestine: This hacktivist group has been actively involved in distributed denial of service (DDoS) attacks, particularly targeting Israeli infrastructure. This group is part of a broader movement of cyber activists who have been actively engaging in cyber operations amid the ongoing Israel-Hamas conflict. Their targets have thus far primarily focused on websites of Israeli entities, their Telegram community is closely following the U.S. university's protests and has previously called for attacks on U.S. private and government sectors.



FalconFeeds.io
@FalconFeedsio

Palestinian hacker group Ghosts of Palestine is inviting hackers around the world to attack Israel's and US private and public infrastructure.

#CyberAttack #Threatintel #IsraelPalestineConflict

Hackers around the world join us. We will attack USA and Israhell cyberspace (infrastructure gov/pvt)

102 10:39 AM

5:57 PM · Oct 8, 2023 · 89.2K Views

Figure 5: Report on Ghosts of Palestine's call to hacktivism

Potential Targets

The recent pro-Palestinian protests at U.S. universities have targeted a broad range of companies for divestment, especially those with business or investment ties to Israel's military and financial activities. Therefore, it is likely that financial services institutions may be targeted along with universities if perceived as related to Israel. DDoS attacks could aim to disrupt critical systems such as online banking platforms, payment services and trading systems. Successful attacks may result in prolonged service outages, financial losses, reputational damage and erosion of customer trust.

Potential Impact

- Disruption of critical systems and services, such as online banking platforms, payment gateways and trading systems.
- Prolonged service outages, financial losses, reputational damage and erosion of customer trust.

Reasons for Concern

- **Activist Aspect:** The emotionally charged nature of the Israeli-Palestinian conflict and the recent breakdown in negotiations are likely to fuel hacktivist motivations for disruptive attacks. The mass arrests of pro-Palestinian activists during university protests may further incite retaliatory actions. Ideologically motivated hacktivists may engage in persistent, high-impact attacks aiming for maximum disruption to advance their cause and impose a "cyber price tag" on entities seen as unsupportive of Palestinian interests.

- **Geopolitical Aspect:** The failure of the Israel-Hamas negotiations has led Hamas to apply maximum pressure on Israel and its allies to expedite the end of the conflict in Gaza, which could result in a Hamas victory. As U.S. universities are now at the forefront of public attention, these hacktivist groups will likely attempt to attack them and amplify the "cyber price tag" narrative. This tactic aims to coerce Israel's allies into pressuring Israel to agree to terms favorable to Hamas, aligning with Hamas's geopolitical objectives in the region.

Resources List:

Pro-Palestinians target financial services:

- https://www.lakeshorepublicmedia.org/npr-news/2024-04-30/top-companies-are-on-students-divest-list-but-does-it-really-work
- Beyond Hacktivism: Deanon Club, KillNet, and the Russian Dark Web Market Wars - SOCRadar® Cyber Intelligence Inc.
- https://techmonitor.ai/technology/cybersecurity/killnet-revil-and-anonymous-threaten-swift-with-destructive-attack-in-48-hours

KillNet “cyber price tag” policy:

- https://explore.avertium.com/resource/an-update-on-pro-russia-threat-actor-killnet
- https://www.zerofox.com/blog/flash-report-the-significance-of-pro-russian-killnet-groups-leadership-change/

Pro-Palestinian protests:

- https://edition.cnn.com/2024/04/29/us/pro-palestinian-university-protests-arrests-dg/index.html

Pro-Palestinian hacktivist:

- https://securityscorecard.com/research/hacktivist-involvement-in-israel-hamas-war-reflects-possible-shift-in-threat-actor-focus/

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premises and cloud DDoS protection for real-time DDoS attack prevention that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection – Quickly and accurately identify and block anomalies while allowing legitimate traffic.

Real-Time Signature Creation – Promptly protect against unknown threats and zero-day attacks.

Web DDOS Tsunami Protection – Automated immediate detection and mitigation of Web DDOS encrypted high RPS and morphing attacks.

A Cybersecurity Emergency Response Plan – Turn to a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks.

Intelligence on Active Threat Actors – High fidelity, correlated, and analyzed data for preemptive protection against currently active known attackers.

For further network and application protection measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the broadest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options, including on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE’S SECURITY RESEARCH CENTER.

Visit Radware's Security Research Center to learn more about today’s attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools. Additionally, visit Radware's Quarterly DDoS & Application Threat Analysis Center for a quarter-over-quarter DDoS and application attack activity analysis based on data from Radware's cloud security services and threat intelligence.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILBILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER'S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIREC, INCIDENTAL, CONSEQUENTIAL, OR EXAMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY REALTED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. **CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE.**