Radware Cybersecurity Advisory

#OpAustralia / #opsjentik

March 21, 2023

Several Muslim hacktivist groups joined hacktivist crews Team insane pk, Eagle Cyber, and Mysterious Team during a denial-of-service and website defacement campaign targeting Australia that started on Saturday, March 21. The Australian fashion label Not A Man's Dream caused a shock wave across the Muslim community by featuring models wearing designs with the word “Allah” in Arabic inscribed across the fabric. In response, the Muslim hacktivist community aligned forces and started attacking Australian infrastructure and private organizations under the operation tags #OpAustralia and #opsjentik.

As of Friday, March 17, Not A Man's Dream has become a prominent target for Muslim hacktivists and between Saturday and the time of this writing, well over 70 Australian sites—including the public websites of governments, ports, banks, and private businesses—have been the target of denial-of-service attacks.

Background

Not a Man's Dream, the Australian luxury streetwear label, has faced public criticism after displaying clothing with the word “Allah” printed on them in Arabic. On Saturday March 11, 2023, during the final show of the Melbourne Fashion Festival, one of their designs featured a model wrapped in a transparent fabric with the Arabic inscription “Allah walks with me” (الله يمشي معي) across the body. The model's head, neck and ears were also covered with the same fabric, in what some perceived to be a nod to the Islamic headscarf, or the hijab.

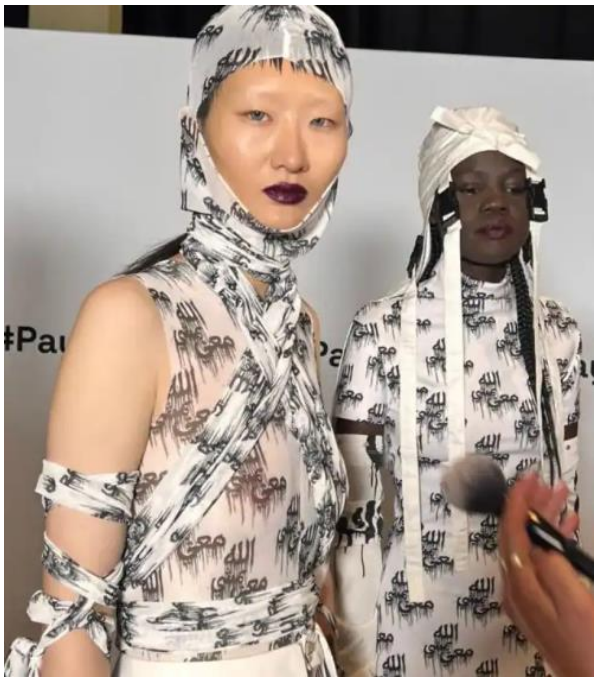

Figure 1: Model wrapped in Arabic-scripted fabric behind the scenes of the Melbourne Fashion Festival runway show
Source: Instagram / PayPal Australia

Another piece featured a layered, short-sleeved dress with a large split and the same inscription. A Melbourne-based Muslim fashion blogger, Mona Khalifa, attended the show and said she was "disturbed" when she saw the design. Khalifa posted to TikTok describing the designs as "blatant disrespect" for Muslims and Arab Christians who share the same Arabic word for ”God.” The video has gone viral.

Figure 2: Melbourne Fashion Festival image carousel featuring the controversial dress
Source: Instagram / Melbourne Fashion Festival

On March 16, 2023, CsCrew posted a message on Telegram that referred to the fashion show incident and threatened Australia. It was forwarded to the Team insane pk Telegram channel.

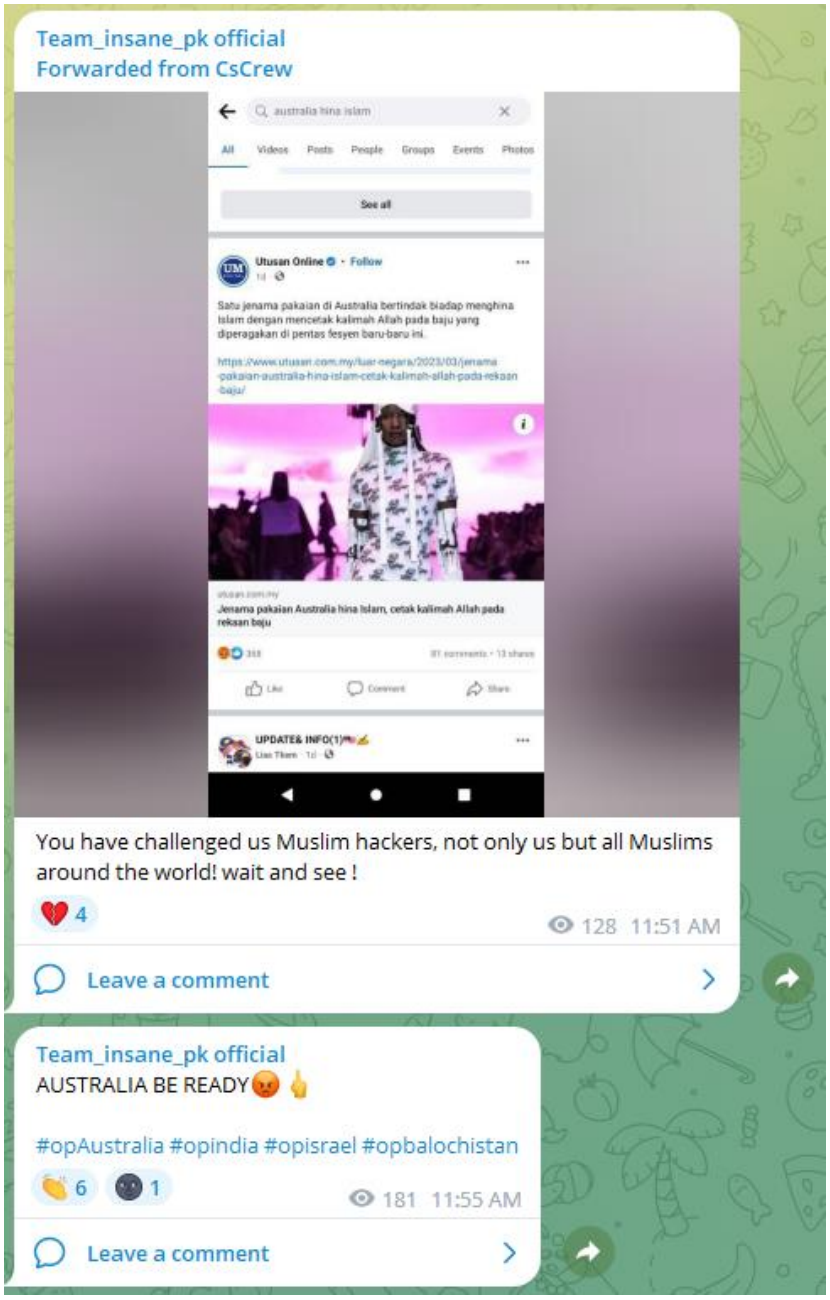

Figure 3: Telegram post forwarded by CsCrew on Team insane pk channel

Hacktivist Following

On Friday, March 17, 2023, Team insane pk posted a message on their Telegram channel providing a list of Australian education sites with alleged logins to be leveraged during the upcoming attacks under the battle tag #OpAustralia.

Figure 4: Team insane pk

The same day, Eagle Cyber Crew announced an operation named #opsjentik, which targeted Australian infrastructure with DDoS attacks and called all like-minded crews and hackers to join their cause.

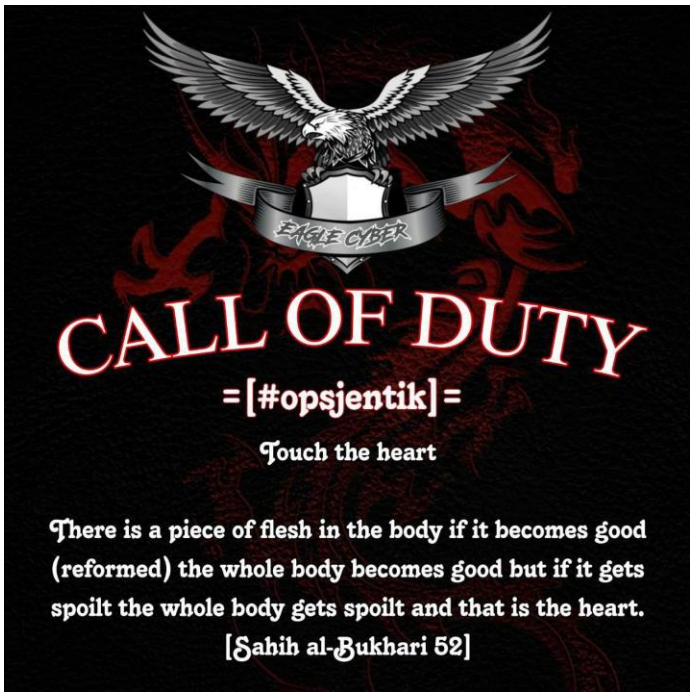

Figure 5: #opsjentik by Eagle Cyber Crew

The message was forwarded to Mysterious Silent Force and Mysterious Team Bangladesh, who called for every Muslim hacktivist, activist, and journalist to join the fight on Saturday, March 18.

Figure 6: Mysterious Team Bangladesh

Australian Fallout

On Friday, March 17, Mysterious Team Bangladesh targeted the website of Not A Man's Dream with DDoS attacks.

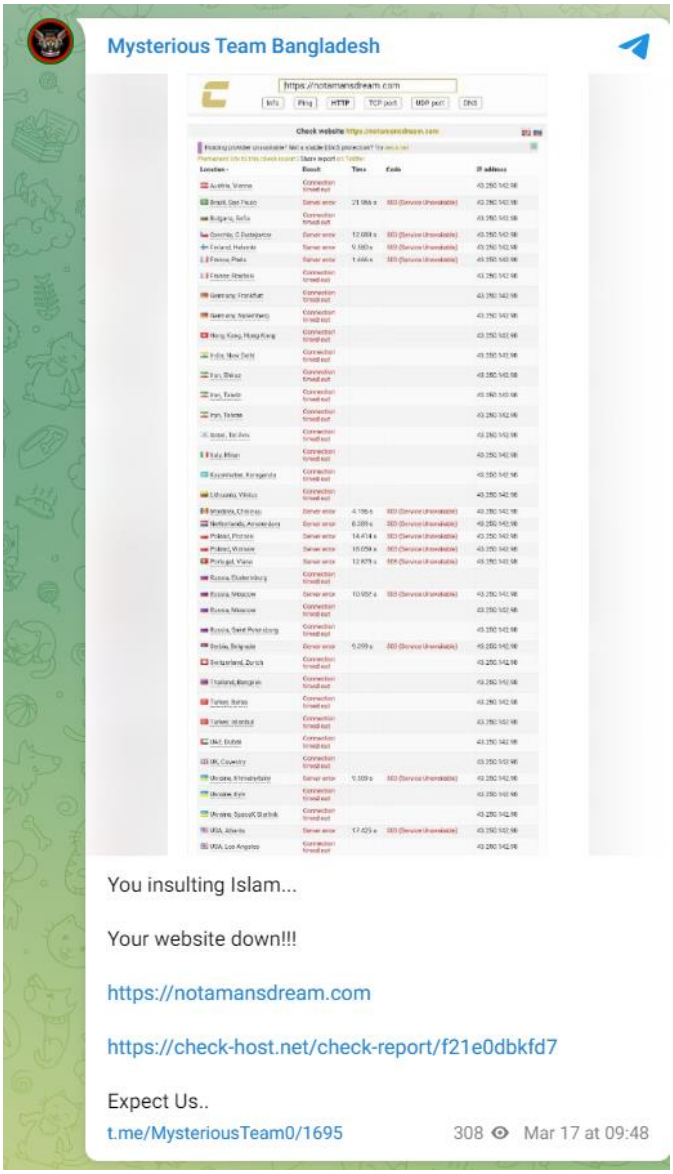

Figure 7: Mysterious Team Bangladesh claiming DDoS attack on Not A Man's Dream website
Source: Telegram

By Saturday, DDoS attacks by Team insane pk targeted several Australian Government websites. On Sunday, Mysterious Team Bangladesh claimed they took the websites of the Australian Police and the Citizen Emergency Health Service offline, while Team insane pk went after IMB Bank and Bank of Sydney and continued the onslaught on Not A Man's Dream.

Radware Cybersecurity Advisory

#OpAustralia / #opsjentik

March 21, 2023

On Monday, March 20, Mysterious Team Bangladesh claimed DDoS attacks on the Port of Portland, Albany Port, Port of Melbourne, the Port Authority of New South Wales, Port of Townsville, Townsville Marine and Educational Sectors and claimed a total of 41 websites were taken offline. At the same time, Team insane pk was targeting government websites and news.com.au.

On Tuesday, a few hours before the writing of this alert, Mysterious Team Bangladesh targeted Southern Ports and Ports North.

Reasons for Concern

Muslim hacktivists have shown to be well connected and have a large circle of influence. Many of the involved hacktivist groups are running multiple concurrent operations, amongst which #OpIndia is a recurring topic. The attacks were motivated by religion, a very common motivation for hacktivists. In other parts of the world, active hacktivist groups are driven by political motivations.

Hacktivists' main objective is getting noticed and spreading their message, either through defacing public websites or making them unavailable through denial-of-service attacks. DDoS attacks are not the hardest to pull off. The hacktivist movements created after the invasion of Ukraine by Russia democratized DDoS attacks and made them more accessible while improving existing tools to make the attacks more sophisticated and more powerful. There's also a good number of supporting services such as free and paying anonymous proxy providers and providers of pay and go DDoS-for-hire services like Clearnet booter and stresser services.

Denial of service has always been an important tactic for hacktivist groups, and this will not change any time soon. As the fallout in Australia has demonstrated, any organization, independent of size and vertical, can become a target of hacktivists. A fashion label made an offensive statement, and governments, ports, banks, and several smaller businesses paid the bill.

There is no reason for panic, but organizations need to be prepared. It is widely known in the security community that disrupting or impacting an organization or infrastructure requires more perseverance than skills or sophistication.

Targeted websites

- notamansdream.com
- guest.police.vic.gov.au
- fed.education.qld.gov.au
- fs.daramalan.act.edu.au
- adfs.loyola.vic.edu.au
- notamansdream.com
- eshealth.com.au
- policehealth.com.au
- pfa.org.au
- www.imb.com.au
- www.banksyd.com.au
- www.news.com.au
- www.portofportland.com.au
- www.albanyport.com.au
- www.cityofalbanyband.org.au
- www.cinestar.com.au
- www.ronmoore.com.au
- parkavenueholidayunits.com
- www.spoonbillsoftware.com.au
- www.omninet.net.au
- www.albanyautos.com.au
- www.vintageblues.com.au
- www.worthley.com.au
- www.evocationdance.org.au
- www.smithsonplanning.com.au
- odin.omninet.net.au
- www.maqohsc.sa.gov.au
- www.portauthoritynsw.com.au
- www.portofmelbourne.com
- sfsh.catholic.edu.au
- www.northshoregp.com.au
- www.nqit.com.au
- www.signsofexcellence.com.au
- www.tsvortho.com.au
- www.alokiskin.com.au
- www.nqmis.com.au
- www.mackeywales.com.au

- bonneyenergy.com.au
- www.wstc.net.au
- www.townsvillemarine.com.au
- www.electrotraining.com.au
- www.apricushealth.com.au
- ryan.catholic.edu.au
- www.picnicbayhotel.com.au
- mmcnq.catholic.edu.au
- sfxnt.catholic.edu.au
- smmc.catholic.edu.au
- www.rapidlegal.com.au
- www.townsvilleconcretesawing.com.au
- sctsv.catholic.edu.au
- www.montgomerysolicitors.com.au
- olltsv.catholic.edu.au
- stbenedicts.catholic.edu.au
- tsv.catholic.edu.au
- sacc.catholic.edu.au
- abergowrie.catholic.edu.au
- hsstsv.catholic.edu.au
- sjbtsv.catholic.edu.au
- smbtsv.catholic.edu.au
- smptsv.catholic.edu.au
- www.acc.qld.edu.au
- www.atouchofsalt.com.au
- www.jcugp.edu.au
- www.westshockey.com
- www.wallace-lawyers.com.au
- www.oakdare.com.au
- www.afcm.com.au
- www.townsvilleenterprise.com.au
- www.pacificmarinegroup.com.au
- www.townsville-port.com.au
- www.southernports.com.au
- www.portsnorth.com.au

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premise 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 through

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

A Cyber-Security Emergency Response Plan - 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 widest 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 - on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

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