



Protecting Against DDoS Attacks

CRITICALITY 

12/10/2023

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

The ongoing Palestine-Israel conflict has sparked a rise in Distributed Denial of Service (DDoS) attacks in the region. This advisory is to outline the protective measures that can be implemented to defend against these attacks.



Threat Details

In recent days, there has been a significant rise in Distributed Denial of Service (DDoS) attacks targeting several sectors in the region due to the ongoing Palestine-Israel war. Therefore, NCSC highly advises all organizations to prioritize the implementation of the following recommendations to ensure the protection of their environment.

Protect your Environment from DDoS attacks:

Protecting the environment from DDoS attacks requires a combination of technical measures, employee education, and collaboration with other organizations. Here are some recommendations to prevent such attacks:

➤ **General Recommendations:**

- Implementing Robust Security Measures to identify and block malicious traffic before it reaches the network.
- Regular security audits are important to identify vulnerabilities in the environment and to ensure that security measures are up to date.
- Monitoring network traffic can help to identify patterns that may indicate a DDoS attack.
- Load balancing is an effective way to prevent DDoS attacks by distributing traffic across multiple servers.
- Employee education is an important part of protecting the environment from DDoS attacks. Employees should be trained on how to recognize and report suspicious activity.
- Collaboration with other organizations can help to share knowledge and resources to prevent DDoS attacks.
- Keeping software up to date is important to prevent vulnerabilities that can be exploited by attackers.
- Implement real-time traffic analysis and filtering to identify and block malicious requests.
- Integrate with Web Application Firewalls (WAFs) to protect against application layer attacks.
- Regularly monitor and analyze DDoS attack data to refine security strategies and improve defenses.



➤ **Cloud Recommendations:**

- Enable auto-scaling for the nodes to seamlessly manage both scale-up and scale-down operations.
- Leverage cloud-based DDoS protection services that offer scalable and resilient defense against attacks.
- Utilize a global Anycast network to distribute and filter incoming traffic.
- Employ automated mitigation techniques, such as rate limiting and traffic redirection, to counter DDoS attacks.

General Protections:

- Ensure that all your systems have endpoint protection software installed and up to date.
- Regularly run vulnerability assessments on your internet facing systems.
- Ensure that all server components are up to date.
- Regularly review your systems, especially internet facing systems, for misconfigurations such as:
 - Ensure that directory traversal is not allowed web sites.
 - Ensure that services are running using service accounts. Never run services using administrator accounts.
- Ensure to backup important data.
- Ensure that all your systems are up to date.
- Make sure to follow OWASP's top 10 to secure web applications.
- Use strong passwords and Two Factor Authentication (2FA).
- Periodically review users' permissions.
- Limit login attempts to prevent Brute Force attack.



Contact Us

Bahrain National CERT - National Cyber Security Center “NCSC”

Email: CERT@ncsc.gov.bh



Appendix A – Best Practices

Bahrain National CERT team recommends organizations to implement the following best security practices.

- Backup daily important new/changed data, software and configuration settings, store disconnected data retained for at least three months. Test restoration initially, annually, and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts to read emails or to browse the web.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Whitelist applications of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- Harden user application. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Activate multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls while prioritizing the implementation of the top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement strategies to mitigate cyber security incidents. (<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Use network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Use The host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Use endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.



- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
- Detect and response to incidents continuously with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
- Refer to MITRE Corporation which provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix B – TLP Definitions

RED

For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that **TLP:AMBER+STRICT** restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

GREEN

Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction