Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

4 November 2022

PIN Number

20221104-001

*The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.*

*This PIN has been released* **TLP:CLEAR**

**Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.**

www.fbi.gov/contact-us/field-offices

# Hacktivists Use of DDoS Activity Causes Minor Impacts

## Summary

The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification to highlight hacktivism activity and encourage organizations to implement the recommendations in the Mitigations section to reduce the likelihood and impact of distributed denial of service[1] (DDoS) attacks.

## Threat

The FBI defines hacktivism as a collective of cyber criminals who conduct cyber activities to advance an ideological, social, or political cause. Historically, hacktivist collectives conducted and advocated for cyber crime activity following high-profile political, socioeconomic, or world events. Coinciding with the Russian invasion of Ukraine, the FBI is aware of Pro-Russian hacktivist groups employing DDoS attacks to target critical infrastructure companies with limited success. Hacktivists provide tools and guidance on cyber attack methodology and techniques to anyone willing to conduct an attack on behalf of their cause. DDoS attacks of

[1] Distributed denial-of-service (DDoS) is an unsophisticated cyber-attack frequently carried out when a cyber-criminal actor sends multiple requests to the target website or server, overloading the server with traffic and temporarily disabling legitimate requests for access. Source: https://www.cisa.gov/uscert/ncas/tips

public facing websites, along with web page and social media profile defacement, are a preferred tactic for many operations. These attacks are generally opportunistic in nature and, with DDoS mitigation steps, have minimal operational impact on victims; however, hacktivists will often publicize and exaggerate the severity of the attacks on social media. As a result, the psychological impact of DDoS attacks is often greater than the disruption of service.

Hacktivists often select targets perceived to have a greater perceived impact rather than an actual disruption of operations:

- DDoS attacks require little technical knowledge and hacktivists may leverage a wide range of open source DDoS services and tools to disrupt public facing websites.
- High-profile targets including financial institutions, health and medical facilities, emergency services, airports, and government facilities are common targets of DDoS attacks.
- Hacktivists typically claim responsibility of such attacks on social media to increase their credibility and falsely assert greater impact or disruption than what occurred.
- Hacktivists also recycle previously disseminated information (whether exfiltrated or a compilation of publicly available information) to build credibility and imply a higher level of technical ability.
- Hacktivists may post news coverage about their attacks, which can lead to repeat attacks or copycat attacks on targets that received a large amount of media attention.

## Recommendations

DDoS attacks are of varying lengths of time and can be identified by:

- Unusually slow network performance (opening files or accessing websites).
- Unavailability of a particular website or the inability to access any website.

To mitigate a DDoS attack:

- Enroll in a Denial of Service protection service that detects abnormal traffic flows and redirects traffic away from the network.
- Create a partnership with your local internet service provider (ISP) prior to an event and work with your ISP to control network traffic during an event.
- Create a disaster recovery plan to ensure successful and efficient communication, mitigation, and recovery in the event of an attack.
- During and after a DDoS attack, monitor other network assets for any additional anomalous or suspicious activity that could indicate a secondary attack.

Additional Resources
For additional information regarding hacktivism or DDoS attacks, please see:

- CISA, FBI, MS-ISAC: Joint Guide “Understanding and Responding to Distributed Denial-of-Service Attacks”, 28 October 2022
- IC3.gov: FBI Public Service Announcement “Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting”, September 30, 2020
- IC3.gov: FBI Public Service Announcement “Booter and Stresser Services Increase the Scale and Frequency of Distributed Denial of Service Attacks”, October 17, 2017
- IC3.gov: FBI Public Service Announcement “Hacktivists Threat to Target Law Enforcement Personnel and Public Officials”, November 18, 2015

## Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

## Administrative Note

This product is marked TLP:CLEAR. Subject to standard copyright rules, the information in this product may be shared without restriction.

## Your Feedback Regarding this Product is Critical

***Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey***