# US Coast Guard Cyber Command
# Maritime Cyber Alert 03-22

August 17, 2022

**Information Sharing Protocol: TLP: WHITE** (https://www.us-cert.gov/tlp)

## Threat from Cyber Criminal Group KILLNET.

## Summary:

The Coast Guard is observing malicious activity linked to a cyber-criminal campaign targeting critical infrastructure in Europe and threatening the United States energy sector's segment in the Marine Transportation System (MTS). These threats were discovered via dark-web posts made by the Russian-based cyber-criminal and hacktivist group known as KILLNET. KILLNET is one of many hacktivist groups whose malicious cyber activity increased in the wake of the Russia's invasion of Ukraine. The group gained notoriety for their Distributed Denial of Service (DDoS) attacks against numerous U.S. Critical Infrastructure and Government websites.

## Targeted Applications & Systems:

- Public Facing Websites
- Logistics and Operations support systems
- Internet of Things (IOT) Devices

## KILLNET Tactics:

KILLNET tactics referenced through ATT&CK™ Techniques are linked to previous KILLNET attacks (https://attack.mitre.org/techniques/enterprise):

- **T1110: Brute Force**
    - Brute Force is a tactic where adversaries use techniques to guess login credentials through trial and error when passwords are unknown.
        - KILLNET used brute-force techniques on Transmission Control Protocol (TCP) ports 21, 80, 443, and 22.
- **T1489: Service Stop**
    - Service Stop is a tactic that adversaries use to stop or disable services on an information system. This will render services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop incident response or aid the adversary's overall objectives to cause damage to the environment.
        - KILLNET used this technique to cause further disruption during an attack.
- **T1498: Network Denial of Service (DoS)**
    - Network DoS is a tactic that adversaries use to degrade targeted resources or to block legitimate users. Network DoS can be performed by exhausting network bandwidth services rely on to operate.
        - KILLNET used Direct Network Floods, a sub-technique T1498 that causes a DoS by directly sending a high-volume of network traffic to a target.

## Mitigation Measures:

The recommended mitigating strategies below may be used to decrease KILLNET's opportunity for exploitation.

- **Mitigate the Opportunity for Attacks**
    - **Minimize Public-Facing Attack Surface** - Do not host any internet facing applications that are not essential to business operations.
    - **Require Multi-Factor Authentication (MFA) for Remote Access** - Require users to login to the company network via a secure Virtual Private Network (VPN) service requiring Multi-factor Authentication (https://attack.mitre.org/mitigations/M1032/) in order to access company resources. Strongly recommend network administrators remove exceptions to the MFA requirement for remote access.
    - **Utilize Demilitarized Zone (DMZ) for Public-Facing Servers** - Host all public-facing servers in a segregated, demilitarized zone (DMZ). This can mitigate internal

company network exposure to untrusted Internet traffic. It can also allow for enhanced public-facing service scrutiny.

- **DDoS Attack Mitigation**

    - Accurately profile all your incoming traffic to distinguish bots from humans.

    - Be on alert for:
        - Unusually slow network performance
        - Unavailability of a particular website

    - During an attack, when malicious traffic exceeds the capacity of the targeted network connection, defenders must intercept incoming traffic upstream to filter out malicious traffic from the legitimate. The hosting Internet Service Provider (ISP), a 3rd party Content Delivery Network (CDN) or providers specializing in DDoS mitigations, can provide such defenses.

    - Analyze the risk of critical resources potentially affected by a Network DDoS attack and create incident response and business continuity plans to manage incidents.

If your organization has any questions related to this alert, please contact the U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at 202-372-2904.

# Appendix A: Indicators of Compromise

**Indicators of Compromise:**

| Type | Indicator | Description |
|---|---|---|
| IPv4 Address | 5.2.69.50 | IP address using TTPs similar to KILLNET. |
| IPv4 Address | 92.255.85.237 | IP address using TTPs similar to KILLNET. |
| IPv4 Address | 92.255.85.135 | IP address using TTPs similar to KILLNET. |
| IPv4 Address | 173.212.250.114 | IP address used in KILLNET attacks. |
| IPv4 Address | 144.217.86.109 | IP address used in KILLNET attacks. |
| IPv4 Address | 156.146.34.193 | IP address used in KILLNET attacks. |
| IPv4 Address | 162.247.74.200 | IP address used in KILLNET attacks. |
| IPv4 Address | 164.92.218.139 | IP address used in KILLNET attacks. |
| IPv4 Address | 171.25.193.25 | IP address used in KILLNET attacks. |
| IPv4 Address | 171.25.193.78 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.100.87.202 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.100.87.133 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.100.87.202 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.129.61.9 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.100.241 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.100.242 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.100.243 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.100.248 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.100.250 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.100.252 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.100.255 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.101.15 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.101.35 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.102.242 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.102.243 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.220.102.253 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.56.80.65 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.67.82.114 | IP address used in KILLNET attacks. |
| IPv4 Address | 185.83.214.69 | IP address used in KILLNET attacks. |
| IPv4 Address | 195.206.105.217 | IP address used in KILLNET attacks. |
| IPv4 Address | 199.249.230.87 | IP address used in KILLNET attacks. |
| IPv4 Address | 205.185.115.33 | IP address used in KILLNET attacks. |
| IPv4 Address | 209.141.57.148 | IP address used in KILLNET attacks. |
| IPv4 Address | 209.141.58.146 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.130 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.131 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.132 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.133 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.134 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.137 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.139 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.142 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.147 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.148 | IP address used in KILLNET attacks. |

| | | |
|---|---|---|
| IPv4 Address | 23.129.64.149 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.210 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.212 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.213 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.216 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.217 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.218 | IP address used in KILLNET attacks. |
| IPv4 Address | 23.129.64.219 | IP address used in KILLNET attacks. |
| IPv4 Address | 45.153.160.132 | IP address used in KILLNET attacks. |
| IPv4 Address | 45.153.160.139 | IP address used in KILLNET attacks. |
| IPv4 Address | 45.154.255.138 | IP address used in KILLNET attacks. |
| IPv4 Address | 45.154.255.139 | IP address used in KILLNET attacks. |
| IPv4 Address | 45.227.72.50 | IP address used in KILLNET attacks. |
| IPv4 Address | 72.167.47.69 | IP address used in KILLNET attacks. |
| IPv4 Address | 81.17.18.58 | IP address used in KILLNET attacks. |
| IPv4 Address | 81.17.18.62 | IP address used in KILLNET attacks. |
| IPv4 Address | 91.132.147.168 | IP address used in KILLNET attacks. |

**References:**

Forescout Technologies, Inc. (2022). *Killnet Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group. Forescout Technologies*. Retrieved July 07, 2022 , from https://www.forescout.com/blog/killnet-analysis-of-attacks-from-a-prominent-pro-russian-hacktivist-group/

The Record. (2022, February 25). *Russia or Ukraine: Hacking groups take side*. Retrieved July 6,2022, from https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/

Cybersecurity & Infrastructure Security Agency. (2022, April 20). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*. CISA. Retrieved July 6, 2022, from https://www.cisa.gov/uscert/Ncas/alerts/aa22-110a

Forescout Technologies, Inc. (2022). *Killnet Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group. Forescout Technologies*. Retrieved July 07, 2022 , from https://www.forescout.com/blog/killnet-analysis-of-attacks-from-a-prominent-pro-russian-hacktivist-group/

Cybersecurity & Infrastructure Security Agency. (2019, November 20). *Security Tip (ST04-015) Understanding Denial-of-Service Attacks*. CISA. Retrieved July 14, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST04-015

Cybersecurity & Infrastructure Security Agency. (2022, July 7). *KILLNET: Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group*. CISA. Retrieved July 7, 2022, from https://www.cisa.gov/