THREAT BULLETIN

AR20221215–004 [Advisory Report] Russian Hacktivist Group Killnet Targeting US Government Network Infrastructure

TLP White

DESCRIPTION

Summary

On December 13, 2022, the self-proclaimed pro-Russian hacktivist group "Killnet" (@killnet_reserves) launched another campaign of attacks via a Telegram posting on the ANONYMOUS RUSSIA channel. In their post, the group claimed responsibility for successful DDoS attacks against three US State websites and provided validation URLs. The group has previously claimed responsibility for DDoS attacks against other United States federal agencies and state governments and continues to remain a threat to MD-ISAC members.

US State Websites Affected 12/13/22:

- https://www.alabama.gov
  - Validation URL: https[:]//check-host[.]net/check-report/de44eefk84e
- https://www.nd.gov
  - Validation URL: https[:]//check-host[.]net/check-report/de449edk3fb
- https://www.virginia.gov
  - Validation URL: https[:]//check-host[.]net/check-report/de44abekc44

Threat Actor

KillNet is a Russia-affiliated hacktivist group specializing in distributed denial of service (DDoS) attacks. The group was originally created on February 26, 2022 on the basis of a Russian-speaking DDoS-for-hire group with the same name. The Anonymous-like collective was formed to wage war on Anonymous (a loosely affiliated group of volunteer hacktivists), Ukraine, and countries that support Ukraine in its war against Russia. The group has united with other threat groups (ex: XakNet Team), DDoS actors, and services to carry out its attacks. Possible targets include governments, civilian critical infrastructure, airports, marine terminals, logistics facilities, weather monitoring centers, health systems, rail systems, financial exchanges, and online trading systems.

Attack Vector

- **DDoS** -- Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications.

MITRE ATT&CK Enterprise Identifier - T1498 (Network Denial of Service)

Detections

- **Network Traffic** -- Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.
- **Sensor Health** -- Detection of Network DDoS can sometimes be achieved before the traffic volume is sufficient to cause impact to the availability of the service, but such response time typically requires very aggressive monitoring and responsiveness or services provided by an upstream network service provider. Monitor for logging, messaging, and other artifacts highlighting the health of host sensors (ex: metrics, errors, and/or exceptions from logging applications)

Mitigations

- **Filter Network Traffic** -- When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.
- **Review Firewall Configurations** -- Review the configurations of web application firewalls and consult with WAF providers on current configurations to ensure proper page caching and DDoS mitigations are in place

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report activity related to this bulletin to the MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).
- Report any incidents to the MDSOC by filling in this form.

Contact Information

To report suspicious or criminal activity related to information found in this Threat Bulletin, contact the Maryland Security Operations Center at (410) 697-9700 or by email at md-isac@maryland.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. Please state in the report if you are requesting incident response resources or technical assistance related to the incident.

References

Original Telegram posting (hxxps://t[.]me/anon_by/2087)

https://md-isac.threatstream.com/actor/232781

https://www.cloudflare.com/static/d442dfee7ea56f899d8df461bb7a077f/BDES-2587-Design-Wrap-Refreshed-DDoS-White-Paper-Letter.pdf