THREAT BULLETIN

FA20221010–001: [Flash Alert] Killnet Targeting US Civilian Network Infrastructure To Include The State Of Maryland

TLP White

PUBLICATION STATUS Published

PUBLISHED DATE 16 Nov 2022 15:43:25

SOURCE CREATED 10 Oct 2022 11:31:00

DESCRIPTION

Summary

On October 10, 2022, the self-proclaimed pro-Russian hacktivist group “Killnet” (@killnet_reserves) launched a new campaign of attacks via a Telegram posting. This new campaign targets United States civilian critical infrastructure, including airports, marine terminals and logistics facilities, weather monitoring centers, Health systems, rail systems, financial exchanges, and online trading systems.

Previously "Killnet" claimed responsibility for a series of distributed denial-of-service (DDoS) attacks on the public-facing websites of 12 US states, including:

- Alabama (alabama[.]gov)
- Alaska (alaska[.]gov)
- Colorado (colorado[.]gov)
- Connecticut (portal[.]ct[.]gov)
- Delaware (delaware[.]gov)
- Florida (myflorida[.]com)
- Hawaii (hawaii[.]gov)
- Idaho (idaho[.]gov)
- Indiana (indiana[.]gov)
- Kansas (portal[.]kansas[.]gov)
- Kentucky (kentucky[.]gov)
- Mississippi (mississippi[.]gov)

The updated target list includes a specific reference to the State of Maryland (www[.]bwiairport[.]com)

Threat Actor

KillNet, a Russia-affiliated hacktivist group specialized in distributed denial of service (DDoS) attacks, originally created on the basis of a Russian-speaking DDoS-for-hire group with the same name. On February 26, 2022, KillNet formed an Anonymous-like collective to wage war on Anonymous (a loosely affiliated group of volunteer hacktivists), Ukraine, and countries that support Ukraine in a way hostile to Russia. The group united with other threat groups (XakNet Team), DDoS actors and services

Killnet - (alias "Cyber Army of Russia - CYBER WAR", "Legion - Cyber Special Forces RF")

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 DoS 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.

Indicators of Compromise

Indicator	Type
N/A	N/A

Incident Response

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

1 Immediately isolate affected systems.

2 Collect and review relevant logs, data, and artifacts.

3 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.

4 Report incidents to MD-ISAC via Maryland's 24/7 Operations Center (soc@maryland.gov or (410) 697-9700 - option #5).

References

Original Telegram posting (hxxps://t[.]me/killnet_reservs/3005)