HC3: Analyst Note
December 22, 2022 TLP:CLEAR Report: 202212221500

Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector

Executive Summary
HC3 is closely tracking hacktivist groups which have previously affected a wide range of countries and industries, including the United States Healthcare and Public Health (HPH) sector. One of these hacktivist groups—dubbed 'KillNet'—recently targeted a U.S. organization in the healthcare industry. The group is known to launch DDoS attacks primarily targeting European countries perceived to be hostile to Russia, and operates multiple public channels aimed at recruitment and garnering attention from these attacks.

Report
KillNet is a pro-Russian hacktivist group, active since at least January 2022, and known for its DDoS campaigns against countries supporting Ukraine; especially NATO countries, since the Russia-Ukraine war broke out last year. DDoS is the primary type of cyber-attack employed by the group, which can cause thousands of connection requests and packets to be sent to the target server or website per minute, slowing down or even stopping vulnerable systems. While KillNet's DDoS attacks usually do not cause major damage, they can cause service outages lasting several hours or even days. Although KillNet's ties to official Russian government organizations, such as the Russian Federal Security Service (FSB) or the Russian Foreign Intelligence Service (SVR), are unconfirmed, the group should be considered a threat to government and critical infrastructure organizations, including healthcare.

Impact to HPH Sector
KillNet has previously targeted, or threatened to target, organizations in the Healthcare and Public Health (HPH) sector. For example, Killmilk, a senior member of the KillNet group, has threatened the U.S. Congress with the sale of the health and personal data of the American people because of the Ukraine policy of the U.S. Congress. In December 2022, the pro-Russian hacktivist group claimed the compromise of a U.S.-based healthcare organization that supports members of the U.S. military and claimed to possess a large amount of user data from that organization. In May 2022, a 23-year old supposed KillNet member was arrested in connection with attacks on Romanian government websites. In response to the arrest, KillNet reportedly demanded his release and threatened to target life-saving ventilators in British hospitals if their demands were not met. The member also threatened to target the UK Ministry of Health. It is worth taking any claims KillNet makes about its attacks or operations with a grain of salt. Given the group's tendency to exaggerate, it is possible some of these announced operations and developments may only be to garner attention, both publicly and across the cybercrime underground.

Mitigations
While it is not possible to fully mitigate the risk of a denial of service attack affecting your service, there are some practical steps that will help you be prepared to respond, in the event your service is subjected to an attack. According to the NCSC, these include 1) understanding your service, 2) upstream defenses, 3) scaling, 4) response plan, and 5) testing and monitoring. Additional guidance from CISA on responding to cyber incidents, such as DDoS attacks, can be found here.

Organizations can take immediate steps to help mitigate a DDoS threat by considering the following:

- Enable web application firewalls to mitigate application-level DDoS attacks.
- Implement a multi-content delivery network (CDN) solution. This will minimize the threat of DDoS attacks by distributing and balancing web traffic across a network.

HC3: Analyst Note
December 22, 2022 TLP:CLEAR Report: 202212221500

Analyst Comment
While senior members of the group likely have extensive experience launching DDoS attacks — leadership has previously operated their own DDoS services and botnets — KillNet has been using publicly available DDoS scripts and IP stressers for most of its operations. On December 14, 2022, the Justice Department announced the court-authorized seizure of 48 internet domains associated with some of the world's leading DDoS-for-hire services, as well as criminal charges against six defendants who allegedly oversaw computer attack platforms commonly called "booter" services. These websites allowed paying users to launch powerful distributed denial-of-service, or DDoS, attacks that flood targeted computers with information and prevent them from being able to access the internet. Despite this success, it remains unknown if (and how) this law enforcement action might impact KillNet, which turned its DDoS-for-hire service into a hacktivist operation earlier this year. Furthermore, it is likely that pro-Russian ransomware groups or operators, such as those from the defunct Conti group, will heed KillNet's call and provide support. This likely will result in entities KillNet targeted also being hit with ransomware or DDoS attacks as a means of extortion, a tactic several ransomware groups have used.

References
Russian hacking group threatens to shut down UK hospital ventilators (May 6, 2022)
https://metro.co.uk/2022/05/06/russian-hacking-group-threatens-to-shut-down-uk-hospital-ventilators-16597589/

Pro-Russia 'KillNet' hackers target Italian institutions (May 11, 2022)
https://www.dw.com/en/pro-russia-KillNet-hackers-target-italian-institutions/a-61764612

Romanian government sites hit by Russian KillNet hacking group (April 29, 2022)
https://www.datacenterdynamics.com/en/news/romanian-government-sites-hit-by-russian-KillNet-hacking-group/

Sinister Russian hacking group threatens to shut down hospital ventilators in Britain after 'officers arrested hacker for helping to cripple Romanian government websites' (May 5, 2022)
https://www.dailymail.co.uk/news/article-10787595/Sinister-Russian-hacking-group-threatens-shut-hospital-ventilators-Britain.html

Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (April 20, 2022)
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

Dark Web Profile: KillNet – Russian Hacktivist Group (December 16, 2022)
https://socradar.io/dark-web-profile-KillNet-russian-hacktivist-group/

AN IN-DEPTH LOOK AT RUSSIAN THREAT ACTOR, KILLNET (October 18, 2022)
https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-russian-threat-actor-KillNet

Meet KillNet, Russia's hacking patriots plaguing Europe (September 9, 2022)
https://www.politico.eu/article/meet-KillNet-russias-hacking-patriots-plaguing-europe/

How one Russian group exposed the soft underbelly of federal cyber defenses (December 6, 2022)
https://federalnewsnetwork.com/reporters-notebook-jason-miller/2022/12/how-one-russian-group-exposed-the-soft-underbelly-of-federal-cyber-defenses/

KillNet DDoS hacktivists target Royal Family and others (November 22, 2022)
https://www.computerweekly.com/news/252527560/KillNet-DDoS-hacktivists-target-Royal-Family-and-others

KillNet targets Eastern Bloc government sites, but fails to keep them offline (November 7, 2022)
https://therecord.media/KillNet-targets-eastern-bloc-government-sites-but-fails-to-keep-them-offline/

Bradley Airport Website Suffers Cyber Attack (March 29, 2022)
https://www.nbcconnecticut.com/news/local/bradley-airport-website-suffers-cyber-attack/2750473/

Russia or Ukraine: Hacking groups take sides (February 25, 2022)
https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/

Who Is KillNet?
https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/KillNet

What Impact, if Any, Does KillNet Have? (October 21, 2022)
https://www.lawfareblog.com/what-impact-if-any-does-KillNet-have

Denial of Service (DoS) guidance
https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/preparing-denial-service-dos-attacks1

KillNet: Russian Hacktivists DDoS US Airports, Government Websites
https://westoahu.hawaii.edu/cyber/uncategorized/KillNet-russian-hacktivists-ddos-us-airports-government-websites/

Federal Prosecutors in Los Angeles and Alaska Charge 6 Defendants with Operating Websites that Offered Computer Attack Services (December 14, 2022)
https://www.justice.gov/usao-cdca/pr/federal-prosecutors-los-angeles-and-alaska-charge-6-defendants-operating-websites

Why organizations should (and should not) worry about KillNet (July 12, 2022)
https://intel471.com/blog/KillNet-xaknet-legion-ddos-attacks

Pro-Russia 'Killnet' hackers target Italian institutions (May 11, 2022)
https://www.dw.com/en/pro-russia-killnet-hackers-target-italian-institutions/a-61764612

HC3: Analyst Note
December 22, 2022 TLP:CLEAR Report: 202212221500

Contact Information
If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback