Radware Cybersecurity Advisory

Killnet Threat to Health and Public Sectors

February 4, 2023

Last week, pro-Russian hacktivist groups launched a coordinated series of distributed denial-of-service (DDoS) attacks against medical centers and healthcare facilities in the United States and Europe. KillMilk, the leader of Killnet, coordinated the attacks and provided the targets. Killnet's affiliates, including Anonymous Russia, supported the action by aligning their attack activity. On January 30, the Health Sector Cybersecurity Coordination Center (HC3) **warned** that, "The group should be considered a threat to government and critical infrastructure organizations, including healthcare."

Who is Killnet?

Killnet is a pro-Russian threat group known for launching denial-of-service attacks against those in public and private sectors that directly and indirectly support Ukraine or have in some way offended Russia. The group formed in January of 2022, selling DDoS services, but quickly transitioned into a hacktivist group following the Russian invasion of Ukraine.

The group **grew** its subscribers on Telegram from 34,000 to 85,000 subscribers in less than a week in June 2022 and has kept growing since. For comparison, IT Army of Ukraine, the international volunteer group created by the Ukrainian government to attack Russian targets in support of the war, has almost 200,000 subscribers but has been **losing** subscribers since March 2022.

KillMilk, the founder of the pro-Russian hacktivist group, claims that members of the group are ordinary people and denies any association with the Russian government. To maintain and grow its attack infrastructure, Killnet depends on donations.

Killnet Attacks

Last year, Killnet was behind the attacks against **Romanian** and **Czech** state institution websites in April. In May, it carried out **attacks** against numerous Italian institutional websites, including those of the Ministry of Defense, the Senate, the National Health Institute, and the Automobile Club d'Italia. The Italian Senate Website was disrupted for an hour during the attacks. Later in May, Killnet attacked more sites in Italy, tried to bring down CSIRT Italy but failed, and **attempted** to disrupt the Eurovision Song Contest voting and broadcasts. The group claimed responsibility for the **attacks** against Lithuania's network infrastructure and **targeted** Norwegian organizations in June. Latvia's public broadcaster was **attacked** by Killnet in what was the largest cyberattack in the country's history.

In August 2022, KillMilk claimed responsibility for a cyber-attack on Lockheed Martin as a retaliation for the HIMARS systems supplied by the US to Ukraine. In October, Killnet announced an operation to target civilian network infrastructure in the United States with coordinated DDoS attacks. Several US government and airport websites were **attacked** in the weeks following the announcement.

Radware Cybersecurity Advisory

Killnet Threat to Health and Public Sectors

February 4, 2023

In September 2022, Killnet announced it attacked 23 websites of four ministries and agencies in Japan, the Tokyo Metro and Osaka Metro websites, and the social network service 'mixi.' Killnet declared war against the Japanese government after Russia and Japan had disagreements over the Kuril Islands.

On January 26, 2023, the German Federal Office for Information Security (BSI) **announced** wide-ranging DDoS attacks against various agencies and companies in **Germany**. According to the BSI, websites from airports were particularly affected, but also those of companies in the financial sector and those of federal and state administrations. The attacks were announced in advance by Killnet, as a retaliation for the German government's decision to send Leopard 2 tanks in support of Ukraine.

Cyber Patriots

Killnet transformed from a profit-oriented criminal enterprise to a politically motivated organization funded through donations. The group identifies itself as a coalition of hackers from Slavic nations. Its activities in the context of the ongoing conflict in Ukraine have drawn attention to the role of third-party actors in cyberspace and their potential impact on ongoing conflicts.

The impact of Killnet on the Russian population who supports the invasion of Ukraine is similar to the influence that social activist groups have on their followers. Killnet's work, while questionable to those in the west, is impacting their society, inspiring others to create music and artwork in support of their operations.

Anonymous Russia, Passion Group, Netside, Mistnet, Usersec, and Bear.IT.Army are some of the patriotic hacktivist groups known to be aligned with Killnet. NoName057(16) remains solitary and does not want to be associated with Killnet. NoName057(16) runs its DDoSia project and group with a moderate number of, be it very dedicated, followers.

A Mistake to Underestimate

Killnet has been actively attacking anyone who supports Ukraine or goes against Russia for almost 12 months. They have been dedicated to their cause and have had the time to build experience and increase their circle of influence across affiliate pro-Russian hacktivist groups. We've seen affiliate groups like NoName057(16) exploring crowd-sourced botnets with financial incentives, Passion group providing a botnet as a service for low prices to like-minded groups. Killnet's influence, reach and skills are growing, and they are not showing signs of slowing down or retiring soon.

Every threat needs to be taken seriously and its risk assessed. A few months ago, Radware's assessment of the risk posed by pro-Russian hacktivist groups would have been low. Still, after 12 months of building experience, advancing its tools, and growing its social network, Radware is more likely to increase that risk to moderate. Radware does not see a reason for panic but prefers to err on the side of caution and be prepared.

It is widely known in the security community that disrupting or having an impact on an organization or infrastructure does not require highly skilled or sophisticated actors.

References and Resources

- HC3 KillNet Analyst Note (aha.org)
- Passion: A Russian Botnet (radware.com)
- Exploring Killnet's Social Circles (radware.com)
- US Civilian Network Infrastructure Targeted by Pro-Russian Hacktivists (radware.com)
- Project DDOSIA Russia's answer to disBalancer (radware.com)
- Inside Killnet: Pro-Russia Hacktivist Group's Support and Influence Grows (darkreading.com)
- New DDoS-as-a-Service platform used in recent attacks on hospitals (bleepingcomputer.com)
- Passion botnet cyberattacks hit healthcare, as actors offer threat as DDoS-as-a-service (scmagazine.com)

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection - On-premise and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high volume attacks and protects from pipe saturation

Behavioral-Based Detection - Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation - Promptly protect from unknown threats and zero-day attacks

A Cyber-Security Emergency Response Plan - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – high fidelity, correlated and analyzed data for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate – using negative and positive security models for maximum accuracy

Auto policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options - on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.