

# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023

Passion group, affiliated with Killnet and Anonymous Russia, recently began offering DDoS-as-a-Service to pro-Russian hacktivists. The Passion Botnet was leveraged during the attacks on January 27th, targeting medical institutions in the USA, Portugal, Spain, Germany, Poland, Finland, Norway, Netherlands, and the United Kingdom as retaliation for sending tanks in support of Ukraine.

### Passion Botnet

The origins of the Passion group remain unknown, but they have made their presence known recently, especially since the start of the new year. The group has been associated with defacement and denial-of-service attacks targeting individuals and organizations who do not support the Russian invasion of Ukraine.

Passion has a strong online presence through its Telegram channels, some dating back to March 2022. Other hacktivist groups, such as Anonymous Russia, MIRAI, Venom, and Killnet, have promoted Passion.

The Passion group's tactics, techniques, and procedures (TTPs) resemble those of the other hacktivist groups involved in the Russo-Ukrainian conflict. After conducting a denial-of-service attack, the group typically posts a link to a check-host[.]net<sup>1</sup> page as evidence of their success.

### Defacement Campaigns

The group responsible for the Passion Botnet carried out several defacement attacks over the past month to spread their message and raise awareness. The defacements primarily targeted small organizations in Japan and South Africa. The group's objective appears to be to use these attacks to draw attention to their botnet.

---

<sup>1</sup> check-host[.]net is an online tool for website monitoring and checking the availability of hosts, DNS records and IP addresses. It provides a capability to create permanent links to the check reports, leveraged by denial-of-service actors to prove temporary disruptions or downtime. The nature of a denial-of-service attack is that the impact lasts only while the attack is ongoing, unlike wiping or crypto-locking attacks. Proving the success of such an attack can be tricky. Check-host provides the necessary means to achieve this.

# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023



*Figure 1: Passion Defacement left on the victim's website after a successful attack*

Hacktivists and defacement attacks can pose a serious risk to targeted organizations. They can significantly harm an organization's reputation, causing a loss of trust and credibility with customers and stakeholders. The attacks can escalate to theft or compromise of sensitive information by moving laterally across the infrastructure from the breached web server. The attacks lead to downtime and can disrupt critical business processes, resulting in higher operational costs and impacting the overall efficiency of an organization. Additionally, breaches can lead to financial losses and legal liabilities. The aftermath of these attacks can be challenging. It may take considerable time and resources to discover the full impact and all affected systems after a breach incident. It is essential for organizations to take proactive measures and have complete visibility in their hybrid infrastructure to detect and assess the impact of breaches and defacements.

### DDoS-as-a-Service

The group behind the Passion Botnet is currently offering access to the service, for a fee, to pro-Russian hackers via several Telegram channels. Over the years, DDoS-as-a-Service became a standard tool for hackers because it allows those without the ability to build and manage a botnet to launch significantly larger and more impactful attacks. DDoS services are generally sold as a subscription-based model, allowing customers to choose their attack vectors, duration, and intensity.

# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023

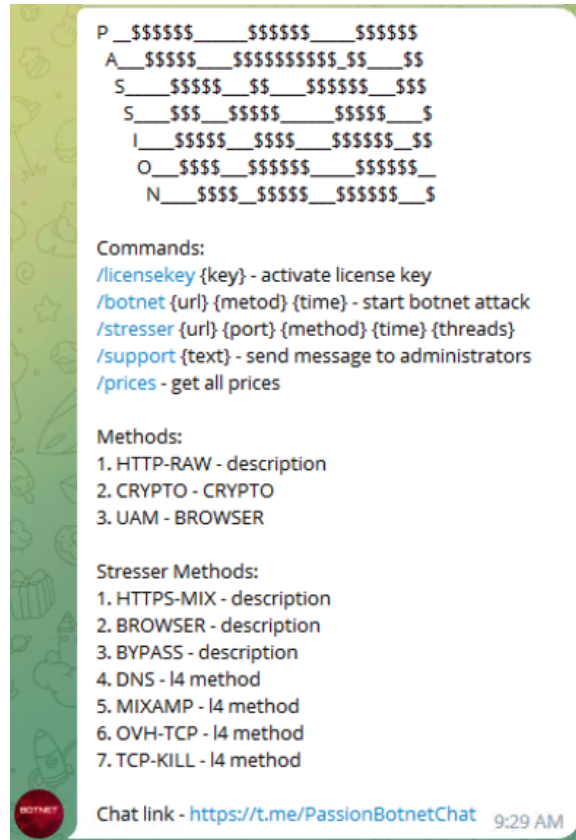


Figure 2: Passion botnet interface on Telegram

The Passion Botnet offers its subscribers ten attack vectors, including application layer encrypted web attacks, L4 attacks, DNS attacks and UDP/TCP floods. By providing various attack methods, Passion enables its subscribers to custom-tailor their attack, increasing the probability of a successful takedown. Additionally, the flexibility to combine and switch attack vectors makes detection and mitigation without automation more challenging for the target.



Figure 3: Passion Botnet Subscription Prices

# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023

@Synmirai, the current merchant behind the DDoS service, is selling subscriptions for Passion Botnet via his Telegram account. Subscriptions range from 7 days of service for \$30 to a full year of prepaid access for \$1,440. Payment is accepted in the form of Bitcoin (BTC), Tether (USDT), and through QIWI, a Russian payment service provider.

Hacktivists and DDoS attacks pose a significant risk to targeted organizations. These attacks can disrupt business operations, leading to loss of credibility, customer trust, and financial damage. In addition, DDoS attacks can be used as a smokescreen for other malicious activities, such as data theft or cyber espionage. Organizations need to implement robust security measures and regularly assess their networks and application to prevent and mitigate the impacts of such an attack.

### Dstat.cc

Dstat.cc is a web service that provides botnet owners to assess the capacity and capabilities of their DDoS attack services. Bot herders use DStat sites to gauge and demonstrate the strength of their botnet, booter, or script against various unprotected and protected targets.

Dstat.cc, based on the collected information from demonstration attacks, provides reviews and contact information for the booter services<sup>2</sup>, allowing potential subscribers to compare and find the best service for their malicious intents.

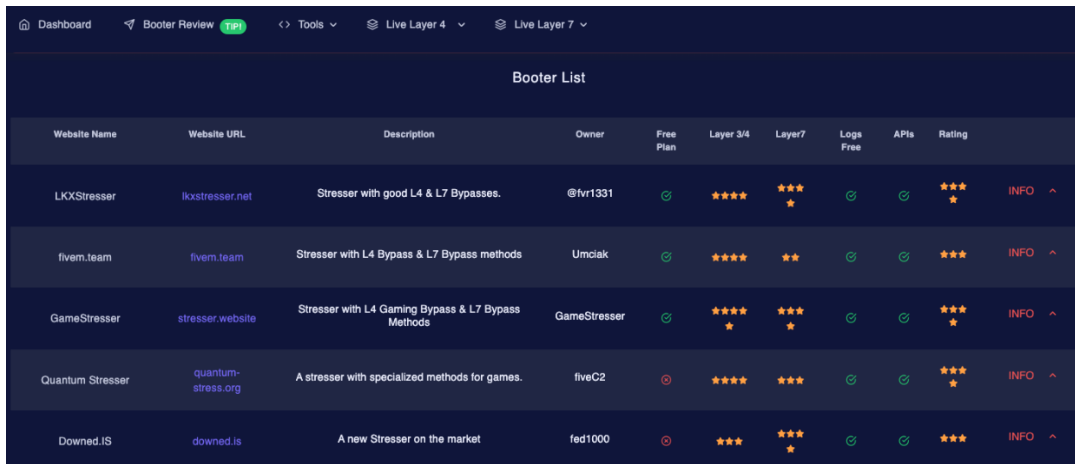
---

<sup>2</sup> DDoS-as-a-Service offerings are also referred to as booter or stresser services

# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023



| Website Name     | Website URL          | Description  | Owner        | Free Plan | Layer 3/4 | Layer7 | Logs Free | APIs | Rating |        |
|------------------|----------------------|--|--------------|-----------|-----------|--------|-----------|------|--------|--------|
| LKXStresser      | lkxstresser.net      | Stresser with good L4 & L7 Bypasses.               | @fvr1331     | ✔         | ★★★★      | ★★★    | ✔         | ✔    | ★★★    | INFO ^ |
| fvem.team        | fvem.team            | Stresser with L4 Bypass & L7 Bypass methods        | Umciak       | ✔         | ★★★★      | ★★     | ✔         | ✔    | ★★★    | INFO ^ |
| GameStresser     | stresser.website     | Stresser with L4 Gaming Bypass & L7 Bypass Methods | GameStresser | ✔         | ★★★★      | ★★★    | ✔         | ✔    | ★★★    | INFO ^ |
| Quantum Stresser | quantum-stresser.org | A stresser with specialized methods for games.     | fiveC2       | ⊘         | ★★★★      | ★★★    | ✔         | ✔    | ★★★    | INFO ^ |
| Downed.IS        | downed.is            | A new Stresser on the market                       | fed1000      | ⊘         | ★★★       | ★★★    | ✔         | ✔    | ★★★    | INFO ^ |

Figure 4: Booter service reviews on Dstat.cc

Bot herders can conduct both Layer 4 and Layer 7 attacks against targets in different countries and assess or demonstrate their performance against mitigation providers like CloudFlare, Google Shield, and protection services from Amazon, Digital Ocean, Microsoft, OVH, and Vultr.

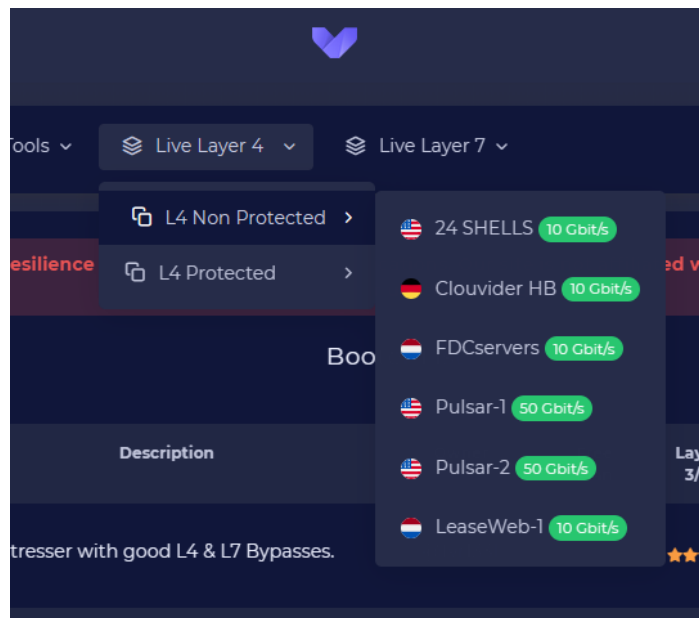


Figure 5: DStat.cc provides several targets for testing L4 attacks, protected and unprotected, with differing capacities

# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023

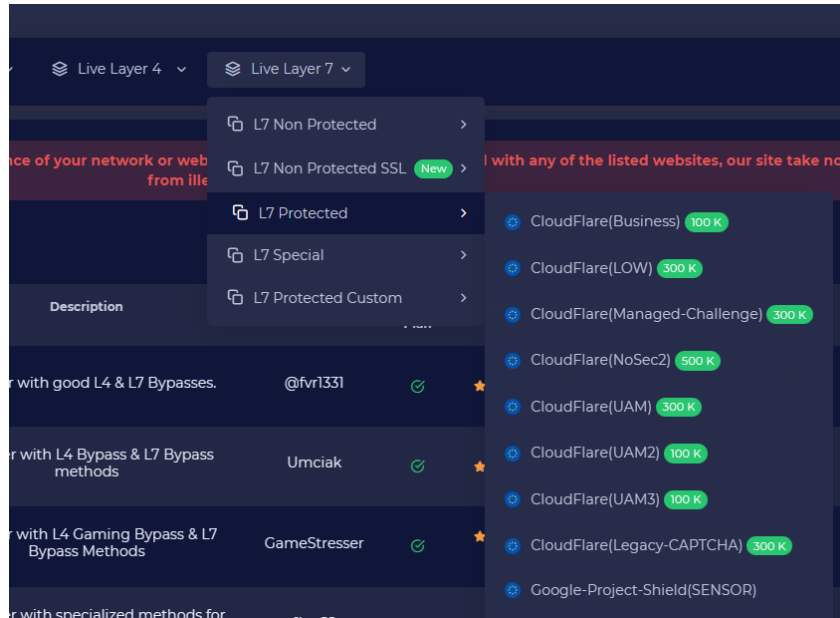


Figure 6: DStat.cc provides many targets for testing L7 application attacks, protected and unprotected, with differing capacities

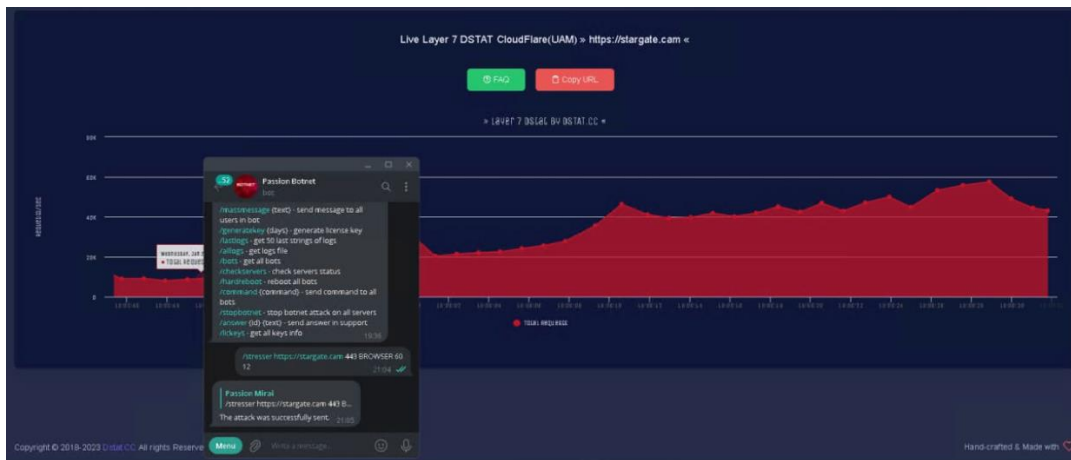


Figure 7: Passion Botnet DStat.cc demonstration

Passion used Dstat.cc to showcase the effectiveness of its Passion Botnet service to prospective customers and advertised it through its Telegram channels. The utilization of Dstat.cc allows the group to demonstrate the capacity and capabilities of their botnet, as well as highlight the strength and efficiency to potential customers.

# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023

### Social Community

The Passion group, like the IT Army of Ukraine and [Project Ddosia](#) by NoName(057)16, is attempting to create a community of patriotic hackers while promoting its DDoS services for financial gain. It has both an [informative](#) and a [chat](#) channel, where the group updates its followers on current campaigns. These types of social communities, such as the one behind Passion, can seriously threaten organizations due to their ability to adapt, work together, and share resources.

### ATTACKS AGAINST MEDICAL INSTITUTIONS

On January 27<sup>th</sup>, KillMilk, the leader of Killnet, [announced](#) a new campaign against medical institutions in the USA, Portugal, Spain, Germany, Poland, Finland, Norway, Netherlands, and the United Kingdom. The operation was carried out against these countries as retaliation for them sending tanks in 'support of the Nazis in Ukraine.'

Since the announcement, several pro-Russian threat groups aligned with Killnet, including Anonymous Russia and Passion, launched DDoS attacks supporting the operation. Specifically, the group behind the Passion Botnet targeted Z-CERT, an emergency response team for the healthcare sector in the Netherlands, after Z-CERT warned that the pro-Russian hacktivist group Killnet was targeting European hospitals.

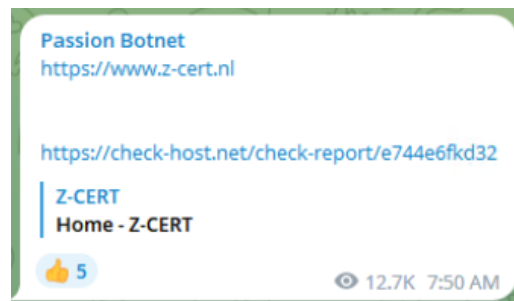


Figure 8: Passion Botnet post announcing the attack on Z-CERT on Telegram with check-host[.]net link

### NOT OUT OF THE WOODS YET

Nearing the end of the attacks targeting hospitals and universities in US and Europe on January 27<sup>th</sup>, KillMilk posted a message addressing the countries that announced sending tanks in support of Ukraine. KillMilk said that the attacks were limited to the public websites of the hospitals and not aimed at the operations and functioning of the medical institutions. But he ended with the threat that he might change his mind in the future and change tactics to target the operations of the hospitals.

# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023

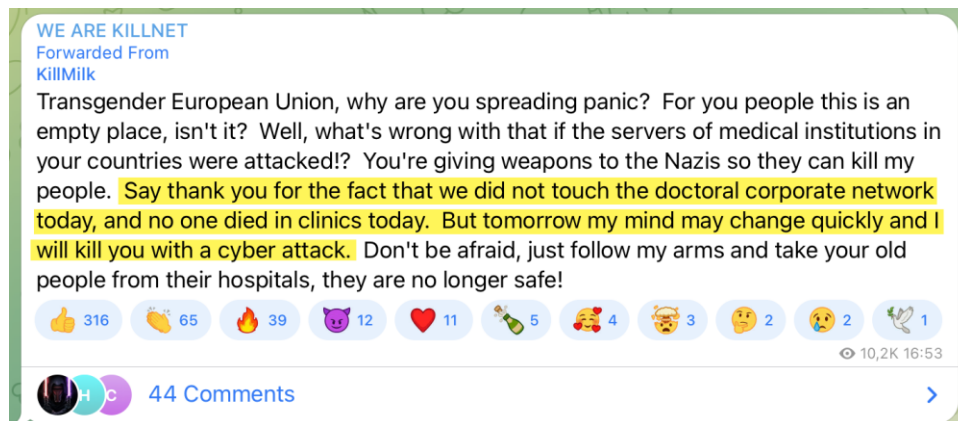


Figure 9: Message from KillMilk addressing the targets at the end of the attack campaign, threatening with potential future retaliations

### Reasons for Concern

The Passion Telegram channel is open to the public and had over 200 members at the time of writing. If the group gains popularity as fast as [Project Ddosia](#) did, it could pose a serious threat to organizations directly and indirectly involved in the Russo-Ukrainian war. The project highlights the desire of Russian hackers to emulate other successful groups involved in the conflict in Eastern Europe. Although Passion Botnet doesn't have a large following yet, the network between Killnet and its affiliates is substantial enough to pose a moderate risk to public and private infrastructure. Additionally, the [pro-Russian hacker community is gaining support](#) from musicians and artists in Russia, both socially and financially, leading to a growing public presence.

While Killnet and its affiliates do not have a track record of inflicting operational impact, they have relied on creating fear, uncertainty, and doubt to deliver their message. But the group had time to gather experience, build tools, gain support, and increase its circle of influence with other pro-Russian groups. Consequently, the threat from KillMilk exploring more impactful campaigns should not be ignored.

The threat is not limited to healthcare. Killnet and its affiliates targeted websites of airports in Germany just last week, websites of airports in the US in October last year and several government websites across the west throughout 2022. In September of 2022, Killnet claimed responsibility for attacks on government websites and public services in Japan. Any public and critical service or infrastructure in Europe and US is a potential target, as are any countries globally that demonstrate support for Ukraine and speak against Russia.



# Radware Cybersecurity Advisory

## Passion: A Russian Botnet

January 31, 2023



### 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-premise, 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.