

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023



Infinity Team, a collaboration between Killnet and Deanon Club, has established its own forum and marketplace called Infinity. The forum offers advertisement spaces, paid status for those who want to perform business on the forum, and is currently offering a variety of hacking resources and services through its hack shop, including DDoS services.

### Background

Hacker forums are online communities, found on both the clear and darknet, where individuals, ethical and malicious, gather to discuss vulnerabilities, exploits, and other tools used for hacking. The information and knowledge gained from these forums can be valuable and used for various purposes, including improving one's security posture or engaging in illegal activities.

#### EXPLOIT FORUM

[Exploit.in](#) is a Russian hacker forum that has been active for almost two decades. It is a platform where individuals can discuss various topics related to computer security, including hacking techniques, exploits, and vulnerabilities. The forum provides a platform for sharing information and tools, allowing members to collaborate and learn from each other. [XSS](#) is another Russian-speaking hacking forum covering similar topics.



Figure 1: Exploit forum

Some of the recent and notable threat actors operating on Exploit and XSS include ransomware operators who are either advertising their operations or engaging in social discussions about trending topics. For example, after the disclosure of the Meris botnet in 2021, a LockBit member going by the alias of LockBitSupp posted a message requesting the bot herder behind Meris to contact him.

#### SEIZURE OF RAIDFORUMS

Last year, the U.S. Department of Justice announced the seizure of [RaidForums](#), a popular forum for cybercriminals to buy and sell stolen data. The founder and administrator of the website, Diogo Santos Coelho, was arrested in the U.K. and is currently in custody awaiting extradition to the U.S. The U.S. government, at the time, had obtained judicial authorization to seize three domains associated with the website, which included [Raidforums.com](#), [Rf.ws](#), and [Raid.lol](#). Before its seizure, RaidForums' members used the platform to sell hundreds of databases of stolen data containing over 10 billion unique records for individuals worldwide.

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023



Figure 2: RaidForums takedown announcement

### SOLARIS DARKNET MARKETPLACE

[Solaris](#) was a prominent darknet marketplace. Online marketplaces allow members to buy and sell illegal goods including narcotics, exploits, and credentials. To ensure everyone's privacy, these marketplaces utilize encryption and other anonymity-enhancing technologies such as [Tor](#) and [I2P](#). Despite the inherent risks, over the last decade, darknet marketplaces have become a popular avenue for criminals due to the ease of access and difficulty for law enforcement to track their activity.

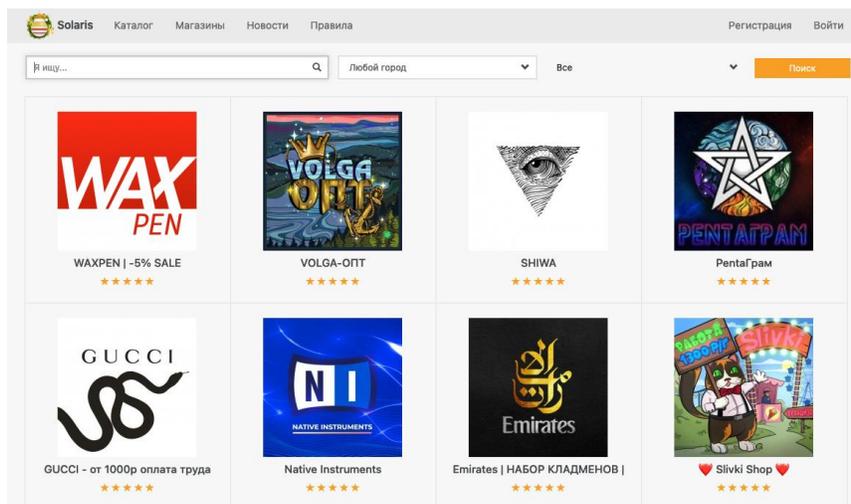


Figure 3: Solaris marketplace

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023

### SEIZURE OF HYDRA

The U.S. Justice Department, in coordination with German law enforcement, announced last year that they shut down the largest darknet marketplace [Hydra](#). The marketplace, used primarily by Russian-speaking members, facilitated the sale of illegal goods and services, including drugs, financial information, and laundering services. Officials, at the time, also announced charges against a Russian resident, Dmitry Pavlov, for conspiracy to distribute narcotics and commit money laundering in connection to his operation and administration of the servers used to run Hydra.



Figure 4: Hydra marketplace takedown announcement

### SOLARIS HIJACKED

On January 13th, 2022, Solaris was hacked and taken over by a rival marketplace, Kraken. Last year, Solaris and Kraken replaced Hydra following its takedown as one of the largest darknet marketplaces. Solaris processed approximately \$150 million in sales of drugs and other illicit goods. Solaris had also previously donated to the pro-Russian hacktivist group Killnet, which allegedly helped Solaris to gain market share on Kraken. The takeover by Kraken, which is also considered a Russian-minded marketplace, was purely driven by market interests and not based on politics.

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023

[https://2krn.at/?mtm\\_campaign=solarisrip](https://2krn.at/?mtm_campaign=solarisrip)



Figure 5: Solaris landing page after Kraken hijacked it

## Infinity Forum and Marketplace

The Infinity Team, which claims to be a team from Belarus, appears to be a collaboration between Killnet and Deanon Club. Infinity Team created a forum and marketplace of their own called Infinity. The domain, [Infinity.in](https://infinity.in), not to be confused with infinity.in, was registered on December 26<sup>th</sup>, 2022, via NameCheap, and its website was protected by Cloudflare.



Figure 6: Infinity forum & marketplace

### ADVERTISING

Criminals often advertise their illegal goods and services on underground forums to generate profits. The advertisements usually offer products like stolen credit card information, drugs, and laundering services. These advertisements aim to attract potential customers who are looking for illegal services and are willing to pay for them.

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023



*Figure 7: Dark Swap advertisement on Infinity*

Administrators behind criminal forums and marketplaces, such as Infinity, typically offer advertisement slots. At the moment, Infinity has one customer, Dark Swap, a cryptocurrency laundering service, but it is looking for more customers. Advertising packages include a main-page banner advertisement for \$1,000 per month, a medium-sized banner for \$500 per month, a small banner for \$300 per month, and a side banner for \$250 per month. Infinity also offers section fixing for \$200 per month, a personal section in "Tested Services" for \$400 per month, a personal section in "Exchange Points" for \$300 per month, and message broadcasting to the whole forum for \$300 per message.

### **BUSINESS STATUS**

Infinity also generates income by selling licenses to those who do business on the forums. These licenses, called statuses, are designated and sold at four different levels. The "Kommersant" status is for entry-level entrepreneurs and costs \$299. The "Businessman" status is for distinguished entrepreneurs looking to stand out and costs \$599. The "God of the market" status costs \$999, and the "Exchange office" status requires a .5 BTC deposit and costs \$1,499 per month.

### **MARKET**

Forums offer sections for criminals selling goods and services to make money through advertising fees or by taking a cut of the transactions on the site. Such forums often cater to a specific niche or audience, like individuals looking to purchase illegal drugs or hacking services and DDoS attacks.

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023

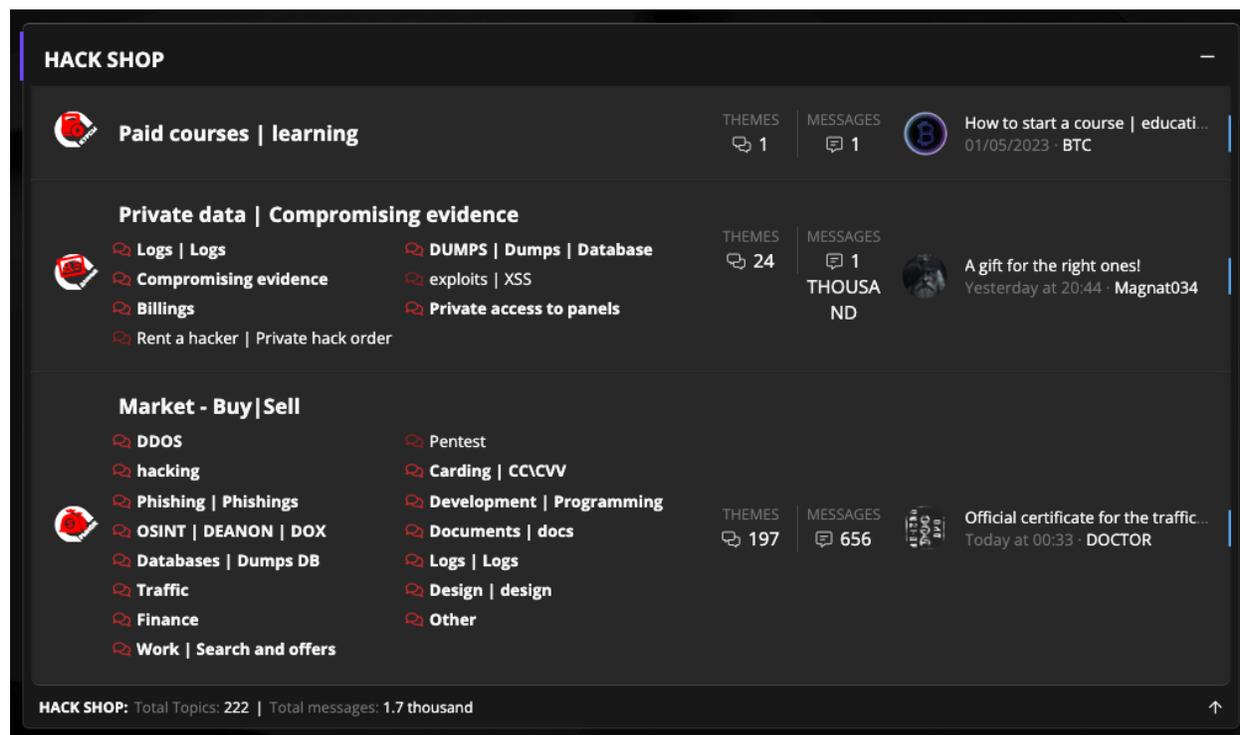


Figure 8: The 'HACK SHOP' on Infinity forum

Infinity is currently offering a number of goods and services through its “HACK SHOP”. The hack shop contains three sections: a section for paid courses and tutorials; a section for selling private data such as logs, dumps, and exploits; and a section for buying and selling DDoS, carding, and phishing services.

### IN THE WILD

Several active members on the Infinity forum share not only tips and tricks for launching denial-of-service attacks but also scripts, attack tools, and information related to their attacks. In a threat called [Chaos Botnet](#), a member going by the alias Mr.DdoS shared images of what appears to be the botnet’s control panel as well as pictures of the botnet’s malware files.

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023

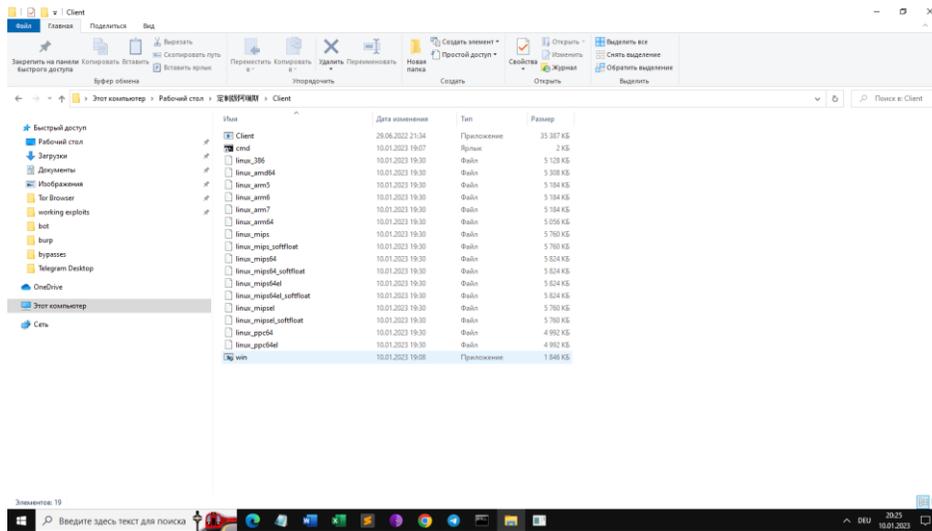


Figure 9: DrDDoS, Chaos Botnet malware screenshot

Running the Chaos Botnet filenames through [URLhaus](https://urlhaus.abuse.ch/), several real-world samples show pro-Russian hackers distributing this IoT-based malware for the purpose of building a botnet. This malware, dubbed Chaos, has tried to infect Radware’s network of honeypots a few times over the last several months.

| Dateadded (UTC)     | URL                                                                                                             | Status  | Tags                         | Reporter         |
|---------------------|-----------------------------------------------------------------------------------------------------------------|---------|------------------------------|------------------|
| 2023-01-20 19:13:29 | <a href="http://46.3.112.238/nmblux">http://46.3.112.238/nmblux</a>                                             | Offline | Chaos elf                    | @RadwareResearch |
| 2023-01-20 19:13:08 | <a href="http://46.3.112.238/win.exe">http://46.3.112.238/win.exe</a>                                           | Offline | Chaos                        | @RadwareResearch |
| 2023-01-08 15:06:10 | <a href="http://45.139.105.143/d/svchost.exe">http://45.139.105.143/d/svchost.exe</a>                           | Offline | 45.139.105.143 Chaos opendir | Anonymous        |
| 2023-01-08 15:06:09 | <a href="http://45.139.105.143/d/svchosts.exe">http://45.139.105.143/d/svchosts.exe</a>                         | Offline | 45.139.105.143 Chaos opendir | Anonymous        |
| 2022-12-10 08:31:16 | <a href="https://zf.gouzapay.cn/muma/386.sh">https://zf.gouzapay.cn/muma/386.sh</a>                             | Online  | chaos kajij                  | @UkyKnight       |
| 2022-10-04 14:58:22 | <a href="http://ares.good1.com:808/linux_mipsel_softfloat">http://ares.good1.com:808/linux_mipsel_softfloat</a> | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 14:58:21 | <a href="http://ares.good1.com:808/linux_mips64_softfloat">http://ares.good1.com:808/linux_mips64_softfloat</a> | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 14:58:16 | <a href="http://ares.good1.com:808/linux_mipsel">http://ares.good1.com:808/linux_mipsel</a>                     | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 14:58:10 | <a href="http://ares.good1.com:808/linux_ppc64">http://ares.good1.com:808/linux_ppc64</a>                       | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 14:57:59 | <a href="http://ares.good1.com:808/linux_mips64">http://ares.good1.com:808/linux_mips64</a>                     | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 14:57:53 | <a href="http://ares.good1.com:808/linux_mips">http://ares.good1.com:808/linux_mips</a>                         | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 14:57:30 | <a href="http://ares.good1.com:808/linux_ppc64el">http://ares.good1.com:808/linux_ppc64el</a>                   | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 11:31:38 | <a href="http://ares.good1.com:808/linux_arm64">http://ares.good1.com:808/linux_arm64</a>                       | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 11:31:35 | <a href="http://ares.good1.com:808/linux_386">http://ares.good1.com:808/linux_386</a>                           | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 11:31:34 | <a href="http://ares.good1.com:808/linux_arm7">http://ares.good1.com:808/linux_arm7</a>                         | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 11:31:34 | <a href="http://ares.good1.com:808/linux_arm6">http://ares.good1.com:808/linux_arm6</a>                         | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 11:31:30 | <a href="http://ares.good1.com:808/linux_arm64">http://ares.good1.com:808/linux_arm64</a>                       | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-04 11:31:08 | <a href="http://ares.good1.com:808/linux_arm5">http://ares.good1.com:808/linux_arm5</a>                         | Offline | Chaos Kajij                  | @UkyKnight       |
| 2022-10-02 11:26:04 | <a href="http://ares.good1.com:808/win.exe">http://ares.good1.com:808/win.exe</a>                               | Offline | Chaos exe kajij              | @UkyKnight       |

Figure 10: Chaos malware sources on URLhaus

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023

### KILLMILK

KillMilk, Anonymous Russia, and several other pro-Russian hacktivist groups, have listed their crypto wallets on Infinity forums asking for donations from devout followers. When examining one of the Bitcoin [wallets](#) that belongs to KillMilk, the leader of Killnet, it becomes apparent the threat actors received a considerable amount of \$24,950 (1.06 BTC), on January 30<sup>th</sup>, 2022, to be exact.

|                                                                                                                                                                                                               |                                                                                                                                                                                                        |                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
|  ID: 0183-2d63 <br>2/02/2023, 03:36:52      | From bc1q-cchg <br>To 2 Outputs                                                                                       | -0.17002397 BTC • -\$3,998.87<br>Fee 2.4K Sats • \$0.56     |
|  ID: 213f-1835 <br>2/01/2023, 08:20:22      | From bc1q-cchg <br>To 2 Outputs                                                                                       | -0.02171961 BTC • -\$510.83<br>Fee 3.0K Sats • \$0.70       |
|  ID: d88b-35f0 <br>2/01/2023, 03:14:29      | From bc1q-cchg <br>To 2 Outputs                                                                                       | -0.02002272 BTC • -\$470.92<br>Fee 2.3K Sats • \$0.53       |
|  ID: 74ea-18e7 <br>1/31/2023, 24:03:19    | From bc1q-cchg <br>To 2 Outputs                                                                                      | -0.50144000 BTC • -\$11,793.60<br>Fee 144.0K Sats • \$33.87 |
|  ID: 055d-2cc5 <br>1/30/2023, 11:31:59  | From bc1q-cchg <br>To 2 Outputs                                                                                     | -0.04000864 BTC • -\$940.98<br>Fee 864 Sats • \$0.20        |
|  ID: 43f8-7b53 <br>1/30/2023, 09:35:34  | From 1PET-Mdg1 <br>To bc1q-cchg  | 1.06085065 BTC • \$24,950.63<br>Fee 228.3K Sats • \$53.69   |
|  ID: 3da7-b9b9 <br>1/04/2023, 24:47:31  | From bc1q-cchg <br>To bc1q-q5cn  | -0.00034273 BTC • -\$8.06<br>Fee 880 Sats • \$0.21          |
|  ID: 5652-c948 <br>12/22/2022, 12:46:16 | From bc1q-ml56 <br>To bc1q-cchg  | 0.00034273 BTC • \$8.06<br>Fee 2.9K Sats • \$0.69           |

Figure 11: Transactions on KillMilk's BTC wallet address (source: [Blockchain Explorer](#))

### HACKING GROUPS

Infinity is offering all pro-Russian threat groups a special section so they can post their own content. To recruit more threat groups, Infinity Team, via the Killnet Telegram channel, [invited](#) all top pro-Russian threat groups that hadn't joined its forum yet, to create an account. These groups include [Beregini](#), [Zarya](#), [RaHDIt](#), [XakNet](#), [DPR Joker](#), and [NoName 057\(16\)](#).

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 2023

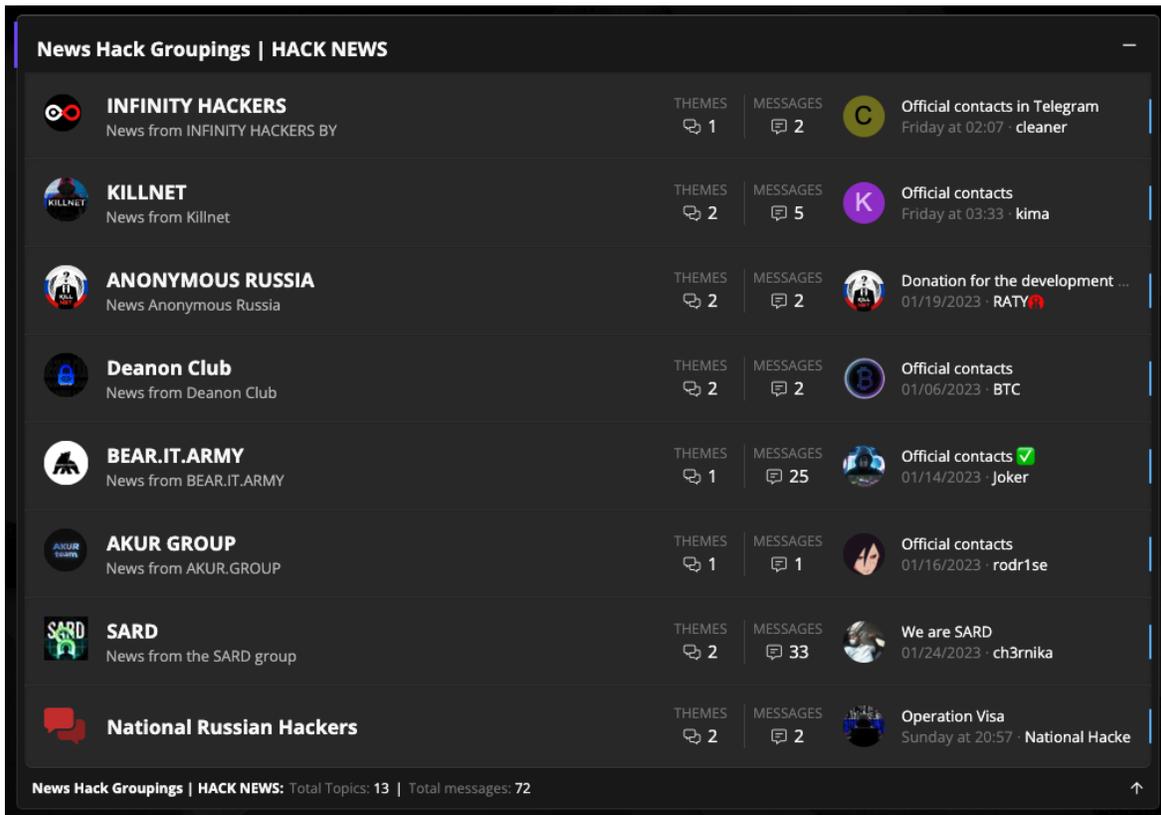


Figure 12: Pro-Russian hacker groups on Infinity

Currently, pro-Russian threat groups [Killnet](#), [Anonymous Russia](#), [Deanon Club](#), [BEAR.IT.ARMY](#), [Akur Group](#), [SARD](#), and [National Hackers of Russia](#) are registered members on the forum with verified links to their telegram channels and contact information.

## Growing Threat

Hacker forums and marketplaces are growing threats as they provide platforms for malicious actors to exchange illegal goods and services, including but not limited to stolen data, hacking tools, and tutorials. They can also generate millions of dollars a year for the owners if ran successfully.

The creation of the Infinity forum highlights a growing and evolving threat from pro-Russian hacktivists. Specifically, KillMilk continued to evolve and expand his social network with other pro-Russian threat groups and those supporting the Russian invasion of Ukraine. If Infinity forum becomes successful, it will produce a windfall of profits for the pro-Russian hacktivist threat groups.

# Radware Cybersecurity Advisory

## Infinity Forum: Another Killnet Social Circle

February 9, 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-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.