

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

A micro flood is a flood of unsolicited packets with throughputs below 1Gbps. The goal of a micro flood is not always a denial-of-service attempt. In some cases, the origin of the floods is what we refer to as the grey noise of the internet: port and vulnerability scans. The number of micro floods in Radware's Cloud DDoS Protection Service has increased significantly in 2022, while mid-sized and large-size floods increased only mildly compared to earlier years.

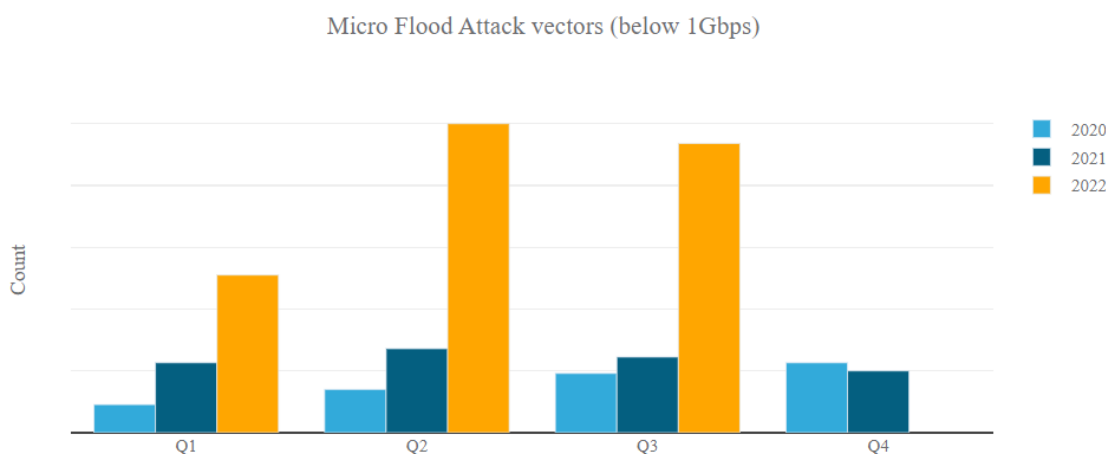


Figure 1: Number of micro floods per quarter (source: [Radware DDoS & Application Threat Analysis Hub](#))

The Grey Noise Of The Internet

In March 2021, Radware issued a [threat advisory](#) about the ProxyLogon zero-day exploits in Microsoft Exchange server. In June 2021, Radware published another [threat advisory](#) about actors actively scanning for critical remote command execution (RCE) vulnerabilities in VMware vCenter servers. In both advisories, Radware observed scanning activity to discover exposed and vulnerable servers only a few hours after a proof of concept for the vulnerability was published. The window between public disclosure and active exploitation of vulnerabilities is shrinking fast, leaving organizations with little time to update or patch their systems.

Malicious actors aren't the only ones who scan the internet. Many researchers and cyber threat intelligence organizations continuously scan the internet to discover vulnerable services to help them assess the risk associated with new vulnerabilities. Organizations such as Shodan, Censys and ZoomEye turned their scanning activities into a service that allow anyone to query specific IP addresses for open ports, services and vulnerabilities or find a list of exposed servers based on specific vulnerabilities.

While it can be useful for organizations to perform periodic assessments of their attack surface, most prefer to keep scanners at bay and block any probes for known vulnerabilities or DDoS reflection and amplification

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

vectors. Well-intended and disclosed scanners can be identified through a DNS reverse lookup on the source IP of the scanner. If the IP has a PTR DNS record, the domain part of the hostname of the scanning server will reveal the originator of the scan and the website associated with the domain might provide more details about the intent and in some cases, an option to opt-out of any future unsolicited scanning activities.

RECYBER.NET

Recyber.net claims to be a project that assists researchers, universities and other educational institutions. The project scans the internet for open ports, and in some cases, vulnerabilities. This actor is anonymous, non-communicative and performs extensive scans. Therefore Recyber.net cannot be confirmed as benign. Several sources on the internet are complaining about the intensity of the scanning performed by Recyber.net ([GreyNoise Trends](#), [Another Legitimate Scanner Testing User Patience? Let's talk about Recyber. \(threatstop.com\)](#), [Many Blocks From the ReCyber Project. : firewalla \(reddit.com\)](#)).

In the last few weeks, Recyber.net is generating a load of 600,000 to 800,000 packets per day, across an average of 120 sensors. The scans are evenly spread across the globe and all sensors, meaning that it is most probably, as it claims, an internet open port and vulnerability scanner. The unsolicited load reaches, on average, up to 6,667 packets per day per sensor. This average does not account for outliers and peaks reaching several billion packets per day.

On several occasions, since April 2022, the Radware DDoS Cloud Protection Service blocked over 1 billion packets per day originating from Recyber.net hosts. On Sept 24, 2022, Radware DDoS Cloud Protection Service blocked close to 3.5 billion packets. Before April, the activity was much lower, amounting to several tens of thousands of packets per day, with two outliers reaching 10 and 20 million packets per day on August 28, 2021 and March 23, 2022, respectively.

Between October 1st and November 14, 2022, Recyber.net scanning activity has been taxing internet services with an average bandwidth of 6Mbps, peaking at 36Mbps and a 95th percentile of 16Mbps while packet rates averaged at 12kPPS peaking at 70kPPS and a 95th percentile of 30k PPS.

The ERT Active Attacker Threat Intelligence Feed blocked almost 75% of all scans. About 20% of the scans were detected and blocked by DefensePro through behavioral analysis, categorized as 'horizontal TCP scanning' and 'random TCP scanning' activity. In addition, between Oct 15th and 21, 2022, a total of 531,000 HTTP scans originating from Recyber.net were blocked by a signature detecting an anomalous User-Agent.

The Recyber.net IP addresses ranging between 89.248.163.0 and 89.248.165.255 are all allocated under the IP Volume Inc autonomous system (AS202425).

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

IP VOLUME INC

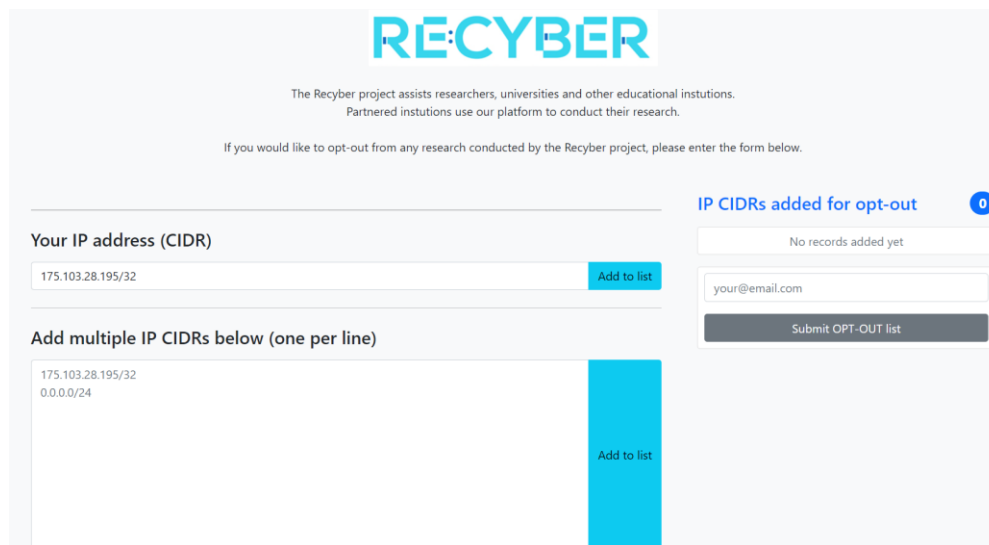
The IP Volume Inc IP address ranges host several global internet scanners, including Shodan.io, Openportstats.com, Criminalip.com and Recyber.net. A good amount of IP addresses from IP Volume are believed to be aggressively scanning the internet. The number of scans per day kept increasing since August 2021 from several hundred packets per day to an average of about 800,000 packets per day by October 11th, and a peak of 2 million packets per day on May 18, 2022.

IMPACT AND MITIGATION

The events have the characteristics of scans, but their aggressive nature leads to potential impacts comparable to DDoS attacks attempting to constrain the resources of servers and network equipment. Radware DDoS Cloud Protection Service customers are protected by our infrastructure that detects and blocks scanning activity as either a known active attacker or leveraging network behavioral and signature-based detections. The ERT Active Attackers Feed accounted for over 83% of all blocked scanning attempts.

Recyber.net scanning activity

Recyber.net claims to be a project that assists researchers, universities and other educational institutions. The project scans the internet for open ports and in some cases vulnerabilities. The project's homepage at recyber.net provides the opportunity to submit IP addresses or subnets for exclusion from future scans. Since the benign nature of Recyber cannot be confirmed, Radware would advise against submitting IP addresses as this could have the opposite effect by providing an important target to focus on.



The screenshot shows the Recyber.net website's opt-out form. The header features the 'RECYBER' logo in blue. Below the logo, a message states: 'The Recyber project assists researchers, universities and other educational institutions. Partnered institutions use our platform to conduct their research.' A sub-message reads: 'If you would like to opt-out from any research conducted by the Recyber project, please enter the form below.'

The form is divided into two main sections. The first section, titled 'Your IP address (CIDR)', contains a text input field with the value '175.103.28.195/32' and a blue 'Add to list' button. The second section, titled 'Add multiple IP CIDRs below (one per line)', contains a text input field with the values '175.103.28.195/32' and '0.0.0.0/24' on separate lines, and a blue 'Add to list' button.

On the right side of the form, there is a section titled 'IP CIDRs added for opt-out' with a blue circle containing the number '0'. Below this title, it says 'No records added yet'. There is a text input field with the placeholder 'your@email.com' and a grey 'Submit OPT-OUT list' button.

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

DECEPTION NETWORK EVENTS

The Radware Global Deception Network is a honeypot network consisting of over 130 honeypots, distributed across the globe. IP addresses of the deception network are not published through any services. This means that any packets hitting the sensor IP addresses are either lost or part of a global, random scanning or exploitation campaign targeting the global internet IP range. In some cases, packets caught in the sensors can be the result of backscatter from DDoS attacks leveraging random source IP spoofing.

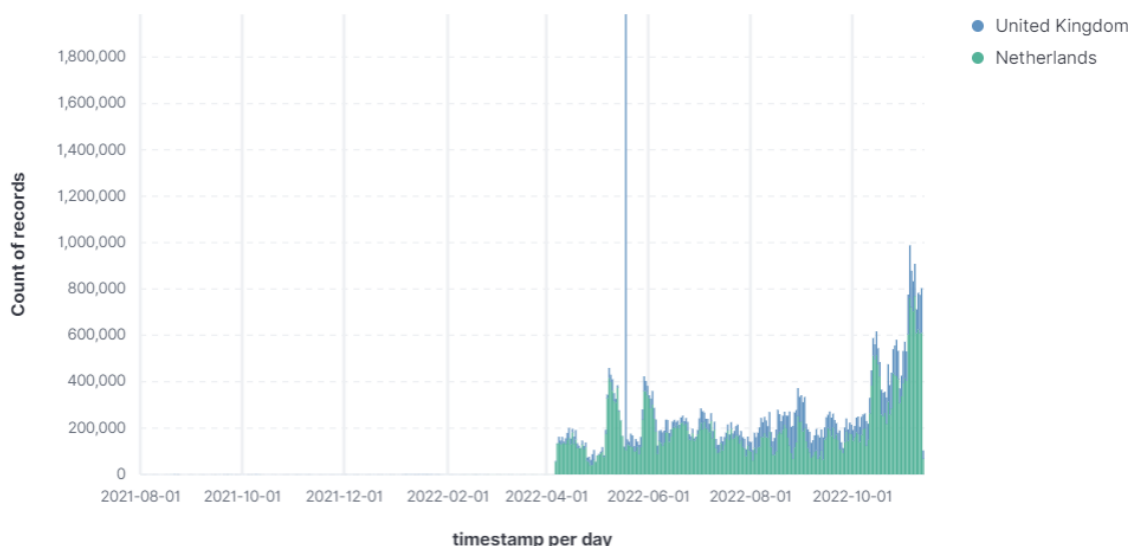


Figure 2: Unsolicited network events originating from Recyber.net since August 2021 (source: Radware Global Deception Network)

Activity from Recyber.net increased significantly starting April 6, 2022 and increased even further and almost exponentially since mid-October.

The increase since April seems to be mainly originating from the Netherlands. Before February 2022, no unsolicited network events originated from the Netherlands, all originated from the U.K.

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

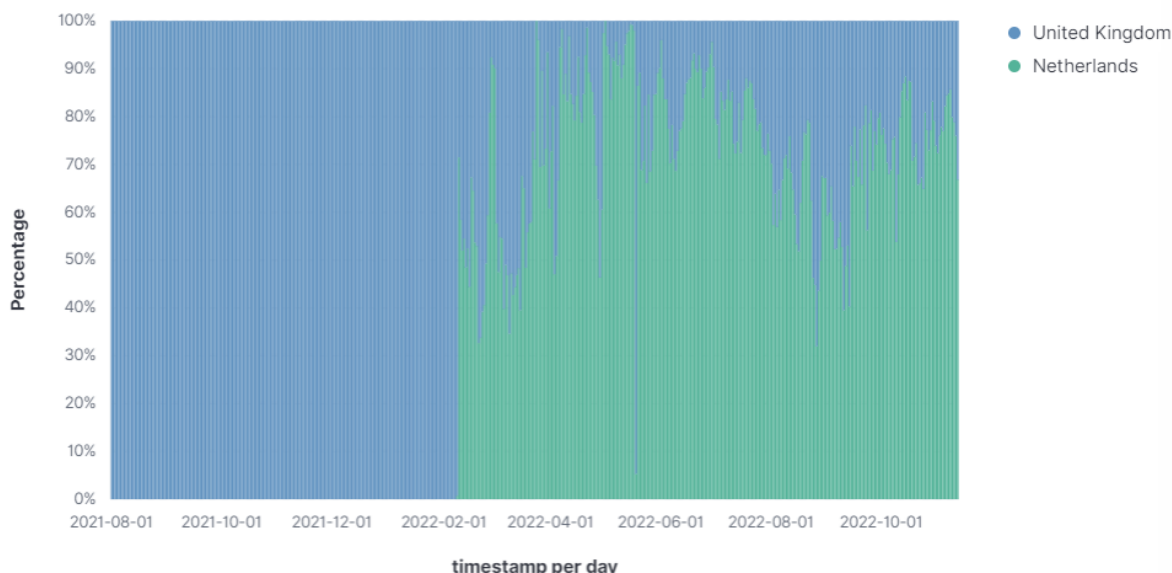


Figure 3: Origin country of Recyber.net unsolicited network events, normalized (source: Radware Global Deception Network)

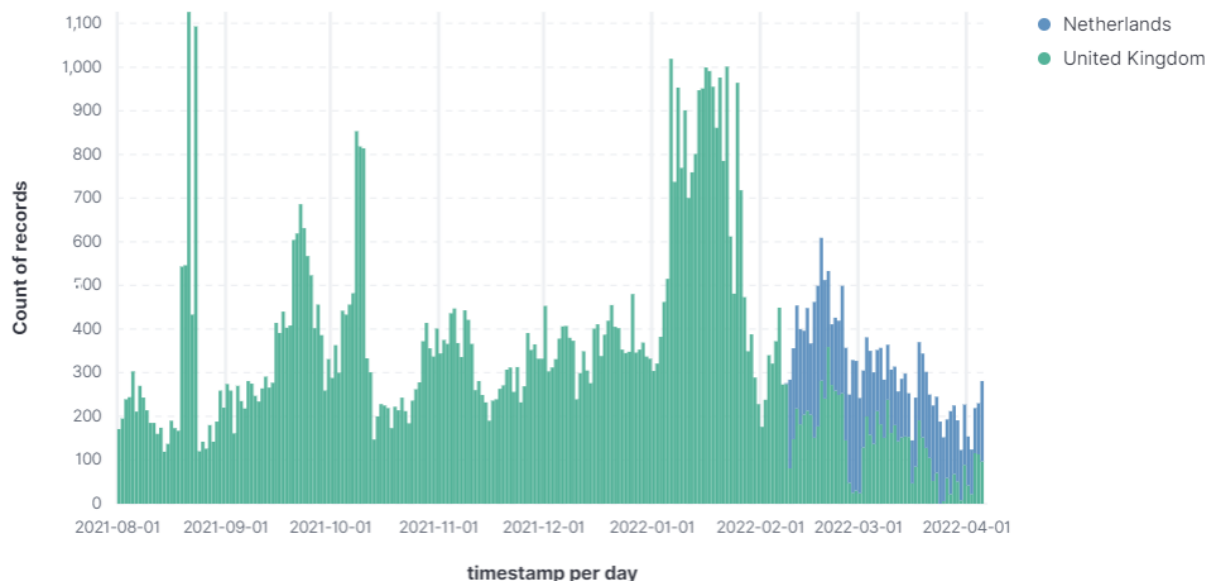


Figure 4: Recyber.net unsolicited network events per day between August 1, 2021 and April 5, 2022 (source: Radware Global Deception Network)

Since April 6, 2022, the deception network detected a total of 59 million unsolicited network events originating from Recyber.net.

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

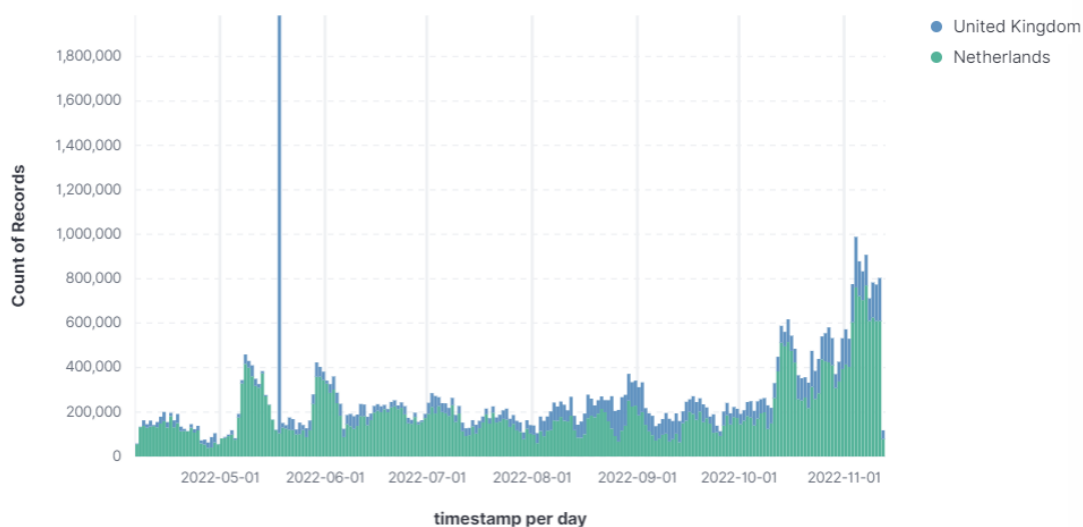


Figure 5: Recyber.net packets since April 6, 2022 (Source: Radware Global Deception Network)

On May 18, 2022, almost 2 million unsolicited network events were detected by the deception network, most of the events originated from the U.K. Since October 11, 2022, the activity increased significantly reaching over 800,000 events per day in the last week of October.

The targets of the Recyber.net events are uniformly spread across the globe and across time. Below is the number of unique sensors triggered per day per region.

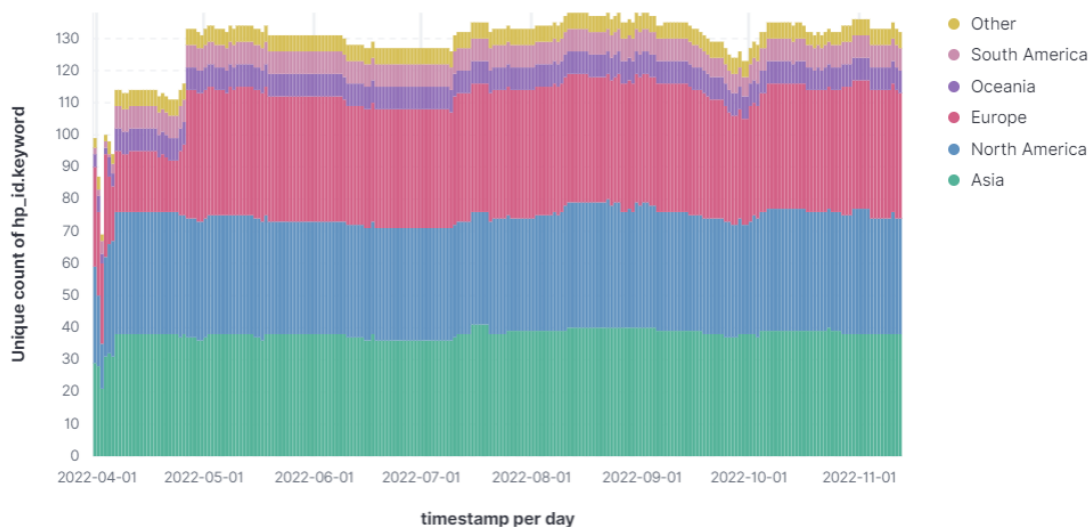


Figure 6: Number of sensors detecting Recyber.net events per day per region (Source: Radware Global Deception Network)

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

CLOUD DDOS PROTECTION SERVICE EVENTS

Malicious events blocked in the Radware DDoS Cloud Protection Service are targeting real services and infrastructures. Compared to the Deception Network, traffic in the DDoS Cloud Protection Service is not considered unsolicited but aimed at services and therefore considered malicious attack traffic that can potentially impact businesses if not mitigated adequately.

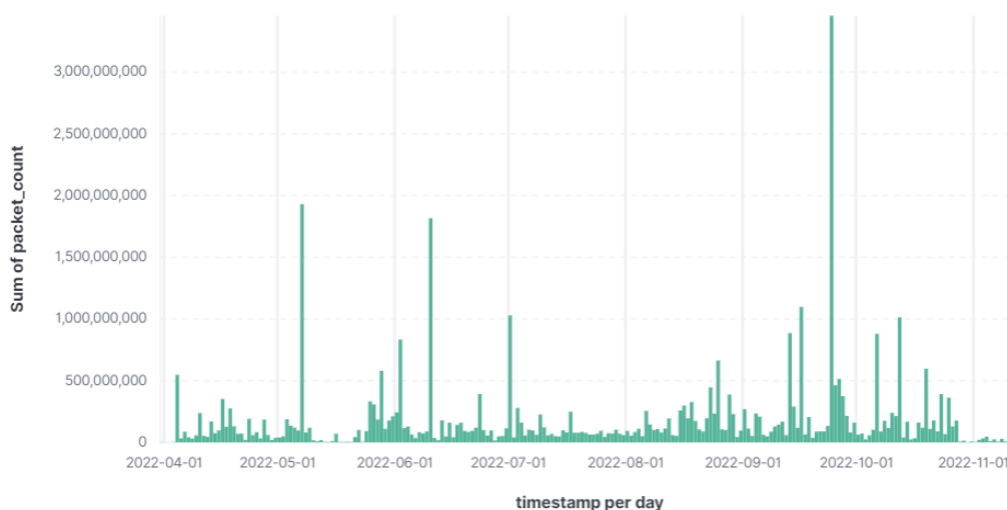


Figure 7: Packets originating from Recyber.net blocked per day since April 2022 (Source: Radware Cloud DDoS Protection Service)

Since April 4, 2022, the service blocked over 1 billion packets per day on several days. On Sept 24, 2022, almost 3.5 billion packets were blocked. Before April, the activity was much lower at several tens of thousands of packets per day, with some outliers reaching 10 and 20 million packets per day on August 28, 2021 and March 23, 2022, respectively.

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

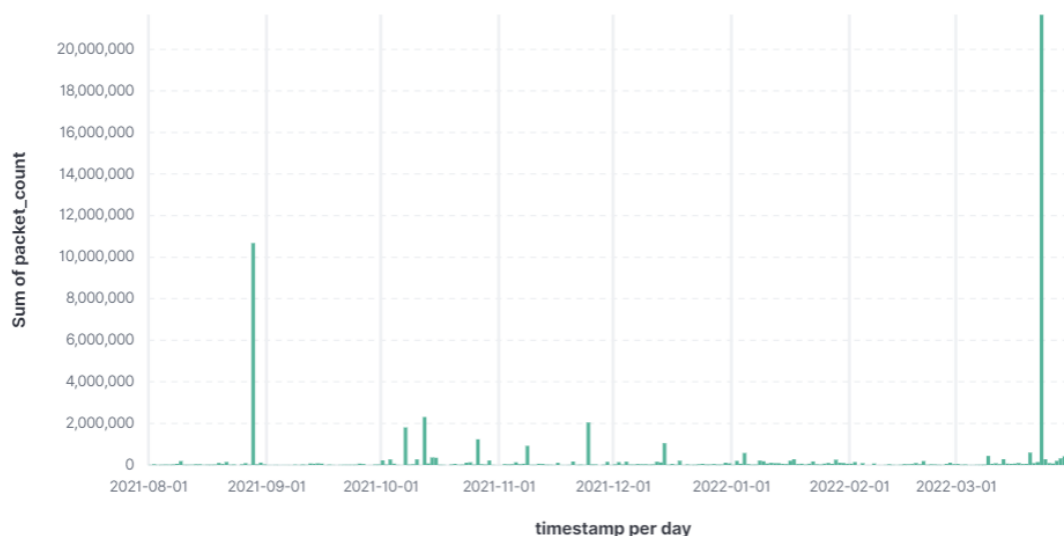


Figure 8: Packets originating from Recyber.net blocked per day between August 2021 and April 2022 (Source: Radware Cloud DDoS Protection Service)

From this point forward, the data set for analysis will only include events between April 2022 and November 2022, the most recent date range and also representing the highest activity.

Almost 75% of the Recyber.net traffic was recognized as active attackers through the Deception Network. A little over 20% was blocked by the anti-scanning detections and the remaining 5% were blocked by traffic filters, behavioral detections, ACLs, anomaly detection and geolocation filters.

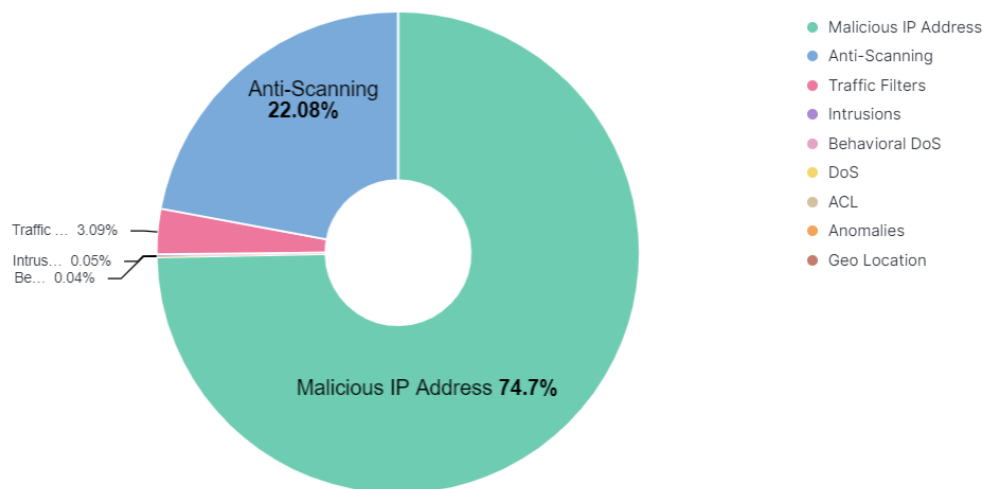


Figure 9: Recyber.net packets blocked by major attack category (source: Radware Cloud DDoS Protection Service)

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

The largest portion, almost 98%, of Recyber.net traffic was TCP based.

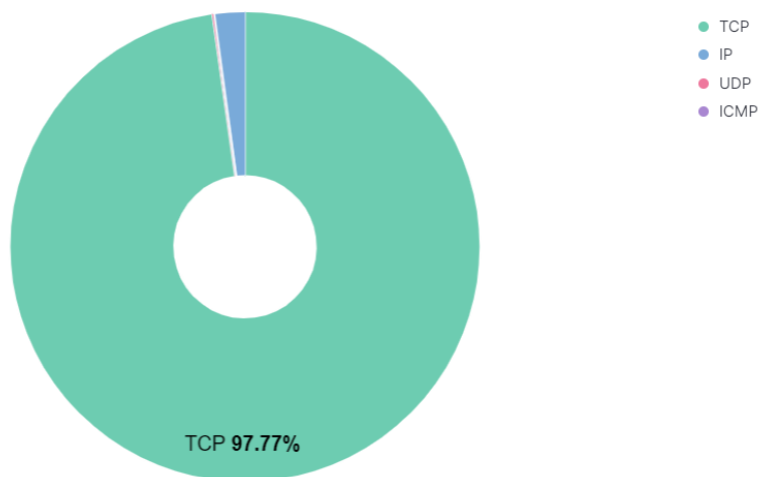


Figure 10: Protocol breakdown of Recyber.net blocked traffic (source: Radware Cloud DDoS Protection Service)

A more detailed breakdown of the attack categories reveals the breakdown between horizontal and random TCP scanning activity detected by the anti-scanning detection.

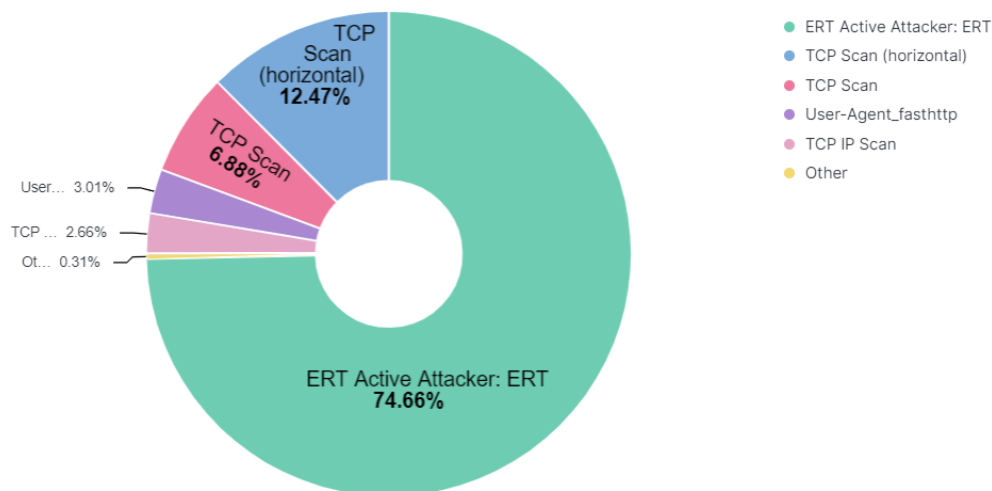


Figure 11: Breakdown of Recyber.net blocked traffic by attack category (source: Radware Cloud DDoS Protection Service)

The 'ERT Active Attacker' category refers to traffic blocked based on IP addresses included in Radware's Active Attackers Threat Intelligence Feed (EAAF). The feed provides a periodically updated list of IP addresses that were detected as top attacking and malicious IPs in Radware's Global Deception Network.

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

The next chart excludes the ERT Active Attacker category to have a better insight on how non-EAAF classified traffic was detected as malicious.

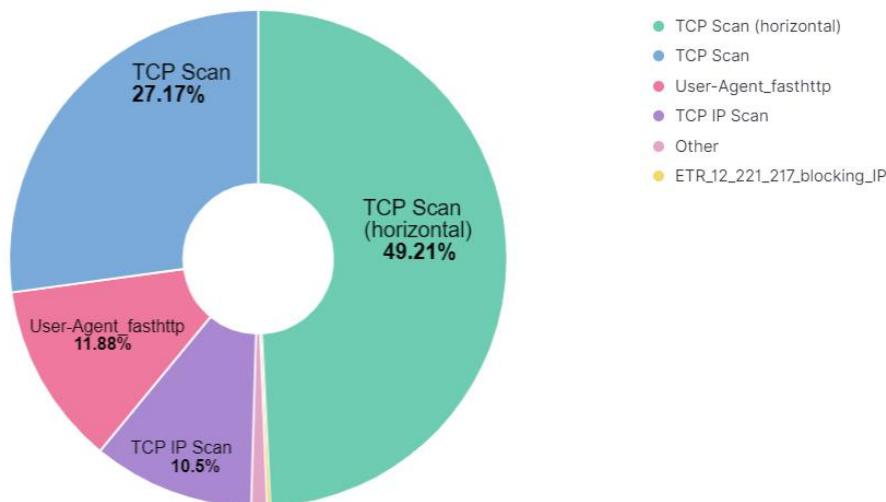


Figure 12: Attack categories of Non-EAAF classified traffic originating from Recyber.net (source: Radware Cloud DDoS Protection Service)

The 'fasthttp' user-agent refers to the [Golang fasthttp module](#). Golang is a development language that is gaining popularity for internet scanning as it provides an ecosystem with many network modules and is typically faster and easier to deploy than Python or Node.js applications. The fasthttp module was designed specifically for high performance and low latency, small to medium, HTTP requests and is able to handle thousands of requests per second.

The HTTP scanning events were all performed between Oct 15 and 21, 2022. A total of 531k request events in a span of six days and all events were targeting port 80.



Figure 13: fasthttp scanning events originating from Recyber.net (source: Radware Cloud DDoS Protection Service)

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

IMPACT ANALYSIS

Between August 1st and October 1, 2022, the average bandwidth consumed by Recyber.net scans was 3Mbps, peaked at 110Mbps and a 95th percentile¹ of 4Mbps. The average packets per second (PPS) was 5k PPS with a maximum of 213k PPS and a 95th percentile of 8k PPS.

Between October 1st and November 14, 2022, the average throughput of Recyber.net scans were 6Mbps, peaking at 36Mbps and a 95th percentile of 16Mbps while packet rates were and average of 12k PPS peaking at 70k PPS and a 95th percentile of 30k PPS.

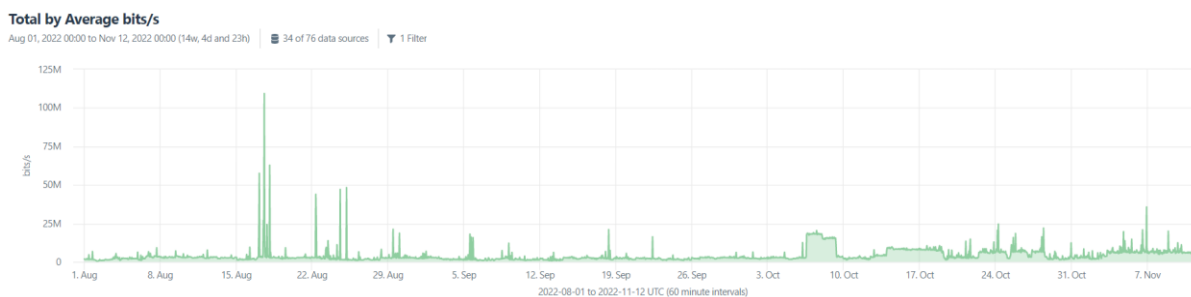


Figure 14: Bandwidth consumed by Recyber.net traffic since August 2022 (source: Radware Cloud DDoS Protection Service)

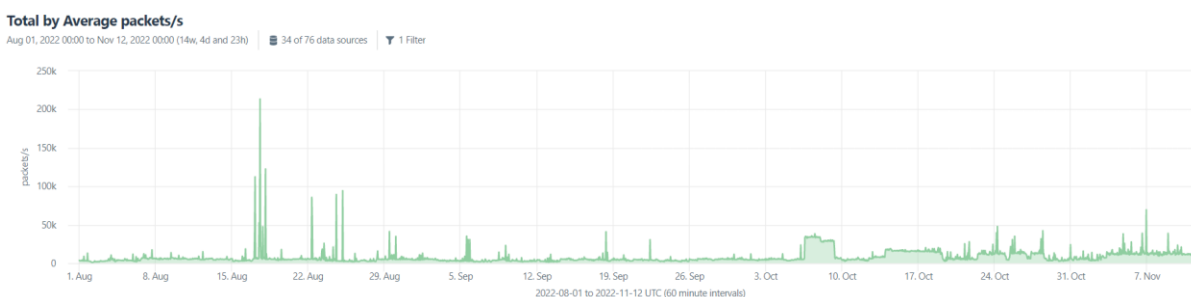


Figure 15: Packet rates of traffic originating from Recyber.net since August 2022 (source: Radware Cloud DDoS Protection Service)

¹ The 95th percentile means that 95% of the time bandwidth or packet rate is below this number, and the other 5% of the time bandwidth and packet rates exceed that number

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

RECYBER.NET SCANNING ACTIVITY

The table below provides the number of ports scanned, the number of detected events, the total number of packets and volume consumed by the scanning activity. The first and last recorded dates provide an indication of when the IP was active.

ip address	# ports	# events	total packets	total volume	first recorded	last recorded	asn	asorg	country	continent
89.248.165.248	3	40	92,206,211	5,511 MB	2022-04-22 11:38	2022-09-29 14:18	202425	IP Volume inc	Netherlands	Europe
89.248.165.24	2	27	50,107,775	3,051 MB	2021-04-16 23:39	2022-09-29 13:32	202425	IP Volume inc	Netherlands	Europe
89.248.165.249	1	9	452,371	25 MB	2022-05-27 06:55	2022-09-23 21:47	202425	IP Volume inc	Netherlands	Europe
89.248.165.14	1	195	201,676,835	11,777 MB	2021-01-06 12:53	2022-09-15 15:30	202425	IP Volume inc	Netherlands	Europe
89.248.165.54	1	344	395,423,555	23,382 MB	2021-01-06 01:58	2022-09-15 04:48	202425	IP Volume inc	Netherlands	Europe
89.248.165.86	2	14	32,074	2 MB	2022-06-11 10:50	2022-09-07 01:08	202425	IP Volume inc	Netherlands	Europe
89.248.165.78	1	73	87,232,537	4,970 MB	2021-06-11 10:36	2022-09-03 16:50	202425	IP Volume inc	Netherlands	Europe
89.248.165.82	1	43	123,786,992	7,215 MB	2021-08-11 20:01	2022-09-03 16:47	202425	IP Volume inc	Netherlands	Europe
89.248.165.43	1	49	15,068,860	878 MB	2022-01-11 15:10	2022-09-03 09:45	202425	IP Volume inc	Netherlands	Europe
89.248.165.214	1	10	957,102	54 MB	2021-05-25 21:16	2022-09-03 01:54	202425	IP Volume inc	Netherlands	Europe
89.248.165.220	1	16	74,296,485	4,528 MB	2021-05-24 21:30	2022-09-02 23:22	202425	IP Volume inc	Netherlands	Europe
89.248.165.224	1	73	12,825,024	724 MB	2021-05-23 21:48	2022-09-02 13:22	202425	IP Volume inc	Netherlands	Europe
89.248.165.218	1	27	29,877,912	1,711 MB	2021-05-24 09:35	2022-09-02 13:18	202425	IP Volume inc	Netherlands	Europe
89.248.165.228	1	22	25,743,994	1,611 MB	2021-06-01 01:57	2022-09-02 03:13	202425	IP Volume inc	Netherlands	Europe
89.248.165.208	1	26	124,570,590	7,396 MB	2021-08-13 23:38	2022-09-01 10:23	202425	IP Volume inc	Netherlands	Europe
89.248.165.101	2	18	583,943	33 MB	2021-02-27 10:19	2022-08-29 19:45	202425	IP Volume inc	Netherlands	Europe
89.248.165.123	1	68	428,797,685	25,192 MB	2021-11-21 17:56	2022-08-29 12:34	202425	IP Volume inc	Netherlands	Europe
89.248.165.210	2	15	1,025,063	64 MB	2021-11-08 14:25	2022-08-19 20:49	202425	IP Volume inc	Netherlands	Europe
89.248.165.38	1	30	3,341,274	191 MB	2020-12-14 18:36	2022-08-19 04:47	202425	IP Volume inc	Netherlands	Europe
89.248.165.222	1	12	4,200,519	253 MB	2021-05-30 15:26	2022-08-18 07:56	202425	IP Volume inc	Netherlands	Europe
89.248.165.244	2	19	24,646,712	1,443 MB	2022-02-06 07:47	2022-08-11 13:11	202425	IP Volume inc	Netherlands	Europe
89.248.165.120	2	57	47,172,907	2,741 MB	2021-03-08 13:59	2022-08-08 14:23	202425	IP Volume inc	Netherlands	Europe
89.248.165.209	1	72	363,832,347	20,981 MB	2022-03-12 08:27	2022-08-07 06:10	202425	IP Volume inc	Netherlands	Europe
89.248.165.21	1	7	3,262,384	203 MB	2022-05-27 01:39	2022-08-04 06:57	202425	IP Volume inc	Netherlands	Europe
89.248.165.207	1	168	136,676,380	8,011 MB	2021-08-19 13:02	2022-07-29 12:03	202425	IP Volume inc	Netherlands	Europe
89.248.165.246	3	53	24,964,243	1,432 MB	2022-04-10 16:05	2022-07-29 00:43	202425	IP Volume inc	Netherlands	Europe
89.248.165.48	1	17	18,878,466	1,103 MB	2021-01-06 12:05	2022-07-28 04:43	202425	IP Volume inc	Netherlands	Europe
89.248.165.252	3	165	129,847,888	7,797 MB	2021-10-11 19:39	2022-07-23 00:05	202425	IP Volume inc	Netherlands	Europe
89.248.165.103	1	197	152,512,969	8,963 MB	2021-01-14 11:44	2022-07-22 09:55	202425	IP Volume inc	Netherlands	Europe
89.248.165.98	2	38	30,348,662	1,788 MB	2021-05-22 08:23	2022-07-19 21:17	202425	IP Volume inc	Netherlands	Europe
89.248.165.105	1	155	100,967,807	6,045 MB	2021-01-17 10:25	2022-07-19 21:16	202425	IP Volume inc	Netherlands	Europe
89.248.165.182	4	116	14,232,450	862 MB	2021-04-30 21:35	2022-07-15 15:27	202425	IP Volume inc	Netherlands	Europe
89.248.165.42	1	29	68,843,138	3,978 MB	2022-04-03 18:40	2022-07-11 12:26	202425	IP Volume inc	Netherlands	Europe
89.248.165.180	3	20	15,120,450	922 MB	2021-03-09 21:32	2022-07-09 17:39	202425	IP Volume inc	Netherlands	Europe
89.248.165.72	1	22	36,540,148	2,220 MB	2021-03-05 05:16	2022-07-09 09:07	202425	IP Volume inc	Netherlands	Europe
89.248.165.225	1	52	19,089,856	1,019 MB	2021-07-19 02:36	2022-07-06 18:30	202425	IP Volume inc	Netherlands	Europe

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022



89.248.165.26	1	8	14,075,608	785 MB	2021-04-27 05:55	2022-07-06 18:28	202425	IP Volume inc	Netherlands	Europe
89.248.165.23	1	12	709,979	44 MB	2021-04-16 06:47	2022-07-01 19:02	202425	IP Volume inc	Netherlands	Europe
89.248.165.13	1	65	20,394,470	1,169 MB	2021-01-11 10:48	2022-06-30 22:28	202425	IP Volume inc	Netherlands	Europe
89.248.165.77	1	154	193,307,173	11,662 MB	2022-03-29 08:33	2022-06-27 06:41	202425	IP Volume inc	Netherlands	Europe
89.248.165.253	1	3	343,325	19 MB	2022-05-02 22:27	2022-06-26 22:54	202425	IP Volume inc	Netherlands	Europe
89.248.165.164	4	72	34,149,494	1,991 MB	2021-03-04 16:17	2022-06-23 19:36	202425	IP Volume inc	Netherlands	Europe
89.248.165.55	1	59	45,963,692	2,738 MB	2021-01-10 02:19	2022-06-23 10:13	202425	IP Volume inc	Netherlands	Europe
89.248.165.247	1	1	4,459,873	271 MB	2022-06-22 04:31	2022-06-22 04:31	202425	IP Volume inc	Netherlands	Europe
89.248.165.102	3	75	59,360,135	3,448 MB	2021-01-15 06:18	2022-06-15 09:07	202425	IP Volume inc	Netherlands	Europe
89.248.165.107	1	68	58,433,620	3,479 MB	2021-08-13 08:32	2022-06-12 08:29	202425	IP Volume inc	Netherlands	Europe
89.248.165.68	1	29	11,111,055	659 MB	2021-01-05 17:19	2022-05-27 10:24	202425	IP Volume inc	Netherlands	Europe
89.248.165.31	1	54	60,047,607	3,531 MB	2020-12-13 15:40	2022-05-24 23:46	202425	IP Volume inc	Netherlands	Europe
89.248.165.8	1	25	17,222,471	1,017 MB	2021-03-08 11:20	2022-05-24 23:36	202425	IP Volume inc	Netherlands	Europe
89.248.165.37	1	20	12,140,910	692 MB	2020-12-15 23:35	2022-05-23 13:33	202425	IP Volume inc	Netherlands	Europe
89.248.165.162	2	45	4,785,166	265 MB	2021-03-25 15:16	2022-05-23 13:13	202425	IP Volume inc	Netherlands	Europe
89.248.165.92	2	93	35,340,925	2,103 MB	2021-01-15 20:04	2022-05-20 05:13	202425	IP Volume inc	Netherlands	Europe
89.248.165.93	3	120	91,430,750	5,341 MB	2021-01-15 00:50	2022-05-17 07:34	202425	IP Volume inc	Netherlands	Europe
89.248.165.19	1	151	96,727,931	5,695 MB	2021-01-13 05:38	2022-05-16 06:41	202425	IP Volume inc	Netherlands	Europe
89.248.165.88	1	35	53,957,585	3,106 MB	2022-01-05 17:33	2022-05-16 02:31	202425	IP Volume inc	Netherlands	Europe
89.248.165.17	3	105	30,291,711	1,747 MB	2021-01-27 03:57	2022-05-16 00:48	202425	IP Volume inc	Netherlands	Europe
89.248.165.2	1	3	2,575,685	142 MB	2022-05-11 00:36	2022-05-15 21:18	202425	IP Volume inc	Netherlands	Europe
89.248.165.16	2	100	15,315,638	854 MB	2021-01-06 13:56	2022-05-15 19:58	202425	IP Volume inc	Netherlands	Europe
89.248.165.12	1	59	221,210,333	12,917 MB	2021-01-06 18:27	2022-05-13 11:04	202425	IP Volume inc	Netherlands	Europe
89.248.165.18	1	38	69,626,275	4,182 MB	2021-01-06 18:26	2022-05-12 19:15	202425	IP Volume inc	Netherlands	Europe
89.248.165.32	1	137	12,807,596	737 MB	2021-01-12 19:34	2022-05-09 03:30	202425	IP Volume inc	Netherlands	Europe
89.248.165.50	1	7	962,724	54 MB	2021-10-02 05:41	2022-05-07 13:09	202425	IP Volume inc	Netherlands	Europe
89.248.165.140	1	5	40	0 MB	2022-05-06 18:53	2022-05-06 18:55	202425	IP Volume inc	Netherlands	Europe
89.248.165.65	1	111	55,773,362	3,278 MB	2021-01-08 09:25	2022-05-02 23:25	202425	IP Volume inc	Netherlands	Europe
89.248.165.6	1	4	127,235	10 MB	2022-04-03 17:18	2022-04-26 11:20	202425	IP Volume inc	Netherlands	Europe
89.248.165.87	1	3	53	0 MB	2022-04-24 08:16	2022-04-24 08:26	202425	IP Volume inc	Netherlands	Europe
89.248.165.71	1	7	3,217,270	200 MB	2022-04-17 20:55	2022-04-18 01:57	202425	IP Volume inc	Netherlands	Europe
89.248.165.76	1	32	53,585,120	3,200 MB	2021-07-25 09:58	2022-04-17 21:22	202425	IP Volume inc	Netherlands	Europe
89.248.165.53	1	25	36,223,282	2,147 MB	2021-01-03 21:14	2022-04-17 18:15	202425	IP Volume inc	Netherlands	Europe
89.248.165.75	1	2	80,466	4 MB	2022-04-16 09:15	2022-04-16 09:20	202425	IP Volume inc	Netherlands	Europe
89.248.165.57	3	71	83,841,500	4,880 MB	2021-01-06 10:50	2022-04-05 19:35	202425	IP Volume inc	Netherlands	Europe
89.248.165.241	1	149	206,826,191	12,388 MB	2021-08-13 23:26	2022-03-29 01:16	202425	IP Volume inc	Netherlands	Europe
89.248.165.245	1	2	20,316	12 MB	2022-03-21 22:29	2022-03-26 20:53	202425	IP Volume inc	Netherlands	Europe
89.248.165.121	1	16	54,846	3 MB	2022-02-26 11:57	2022-03-24 06:21	202425	IP Volume inc	Netherlands	Europe
89.248.165.39	1	324	532,188,425	31,818 MB	2020-12-16 07:57	2022-03-23 16:43	202425	IP Volume inc	Netherlands	Europe
89.248.165.69	1	258	190,448,091	11,246 MB	2021-01-03 18:49	2022-03-23 11:47	202425	IP Volume inc	Netherlands	Europe
89.248.165.44	1	9	9,541,449	550 MB	2021-12-15 09:50	2022-03-09 07:12	202425	IP Volume inc	Netherlands	Europe
89.248.165.74	1	4	8,139,898	496 MB	2022-02-03 08:03	2022-02-27 06:34	202425	IP Volume inc	Netherlands	Europe
89.248.165.60	7	26	6,923,453	412 MB	2021-01-03 15:30	2022-02-27 00:18	202425	IP Volume inc	Netherlands	Europe

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

89.248.165.202	13	13	48	0 MB	2022-01-28 06:28	2022-02-25 20:35	202425	IP Volume inc	Netherlands	Europe
89.248.165.64	1	24	28,116,191	1,564 MB	2021-01-08 09:23	2022-02-05 09:24	202425	IP Volume inc	Netherlands	Europe
89.248.165.5	1	9	14,953,162	801 MB	2020-11-25 15:44	2022-02-02 10:08	202425	IP Volume inc	Netherlands	Europe
89.248.165.206	1	102	33,897,062	2,016 MB	2021-08-22 22:38	2022-01-25 19:26	202425	IP Volume inc	Netherlands	Europe
89.248.165.223	1	46	4,110,024	227 MB	2021-07-15 18:28	2022-01-24 17:37	202425	IP Volume inc	Netherlands	Europe
89.248.165.79	1	5	4,181,229	243 MB	2021-03-04 18:01	2022-01-24 01:18	202425	IP Volume inc	Netherlands	Europe
89.248.165.219	1	64	6,084,889	341 MB	2021-07-13 22:34	2022-01-23 17:42	202425	IP Volume inc	Netherlands	Europe
89.248.165.229	1	59	5,068,744	280 MB	2021-07-14 13:26	2022-01-23 12:05	202425	IP Volume inc	Netherlands	Europe
89.248.165.227	1	52	4,575,268	253 MB	2021-07-29 15:00	2022-01-22 22:02	202425	IP Volume inc	Netherlands	Europe
89.248.165.203	1	1	218,592	13 MB	2022-01-20 13:36	2022-01-20 13:36	202425	IP Volume inc	Netherlands	Europe
89.248.165.217	1	46	4,454,266	245 MB	2021-07-19 09:59	2022-01-20 10:54	202425	IP Volume inc	Netherlands	Europe
89.248.165.215	1	55	4,936,762	275 MB	2021-07-22 05:29	2022-01-19 09:28	202425	IP Volume inc	Netherlands	Europe
89.248.165.221	1	38	3,446,881	191 MB	2021-07-18 19:12	2022-01-18 23:38	202425	IP Volume inc	Netherlands	Europe
89.248.165.212	1	48	4,628,779	253 MB	2021-07-11 21:05	2022-01-18 13:47	202425	IP Volume inc	Netherlands	Europe
89.248.165.84	1	20	53,339,066	3,095 MB	2021-06-28 03:14	2022-01-17 07:13	202425	IP Volume inc	Netherlands	Europe
89.248.165.179	2	127	106,733,411	6,212 MB	2021-04-03 02:56	2022-01-15 23:23	202425	IP Volume inc	Netherlands	Europe
89.248.165.250	1	2	943,603	58 MB	2021-12-30 03:29	2022-01-15 00:18	202425	IP Volume inc	Netherlands	Europe
89.248.165.124	1	12	5,838,279	353 MB	2021-09-23 16:32	2022-01-12 06:28	202425	IP Volume inc	Netherlands	Europe
89.248.165.163	1	3	306,023	19 MB	2021-05-08 21:59	2022-01-01 03:16	202425	IP Volume inc	Netherlands	Europe
89.248.165.119	1	534	319,454,144	18,790 MB	2021-06-12 23:39	2021-12-26 09:42	202425	IP Volume inc	Netherlands	Europe
89.248.165.80	2	236	120,830,367	7,027 MB	2021-03-04 07:58	2021-12-24 02:41	202425	IP Volume inc	Netherlands	Europe
89.248.165.45	2	14	5,941,310	353 MB	2020-12-31 00:02	2021-12-23 13:56	202425	IP Volume inc	Netherlands	Europe
89.248.165.172	1	2	15	0 MB	2021-12-19 10:59	2021-12-19 10:59	202425	IP Volume inc	Netherlands	Europe
89.248.165.96	1	56	38,082,805	2,249 MB	2021-08-15 02:53	2021-12-14 19:17	202425	IP Volume inc	Netherlands	Europe
89.248.165.125	1	193	74,110,788	4,307 MB	2021-05-22 21:55	2021-11-15 02:51	202425	IP Volume inc	Netherlands	Europe
89.248.165.46	1	6	4,204,158	245 MB	2021-02-03 14:08	2021-11-13 13:47	202425	IP Volume inc	Netherlands	Europe
89.248.165.170	1	9	93	0 MB	2021-11-05 08:52	2021-11-06 16:13	202425	IP Volume inc	Netherlands	Europe
89.248.165.63	1	127	242,111,266	14,179 MB	2021-01-08 13:53	2021-11-06 01:48	202425	IP Volume inc	Netherlands	Europe
89.248.165.90	1	56	4,200,946	238 MB	2021-01-18 20:54	2021-10-29 21:19	202425	IP Volume inc	Netherlands	Europe
89.248.165.89	1	37	5,116,636	294 MB	2021-01-17 09:22	2021-10-29 19:35	202425	IP Volume inc	Netherlands	Europe
89.248.165.40	1	46	10,200,287	588 MB	2020-12-14 19:55	2021-10-11 04:41	202425	IP Volume inc	Netherlands	Europe
89.248.165.211	1	3	10,977	1 MB	2021-10-05 03:43	2021-10-05 14:08	202425	IP Volume inc	Netherlands	Europe
89.248.165.94	1	36	88,027,832	5,246 MB	2021-08-21 01:55	2021-10-02 14:38	202425	IP Volume inc	Netherlands	Europe
89.248.165.22	1	33	24,902,420	1,419 MB	2020-12-07 05:02	2021-09-28 13:13	202425	IP Volume inc	Netherlands	Europe
89.248.165.29	1	2	19,051,004	1,180 MB	2021-09-08 15:01	2021-09-26 03:31	202425	IP Volume inc	Netherlands	Europe
89.248.165.183	1	7	4,691,892	364 MB	2021-05-05 01:38	2021-09-25 20:49	202425	IP Volume inc	Netherlands	Europe
89.248.165.91	1	38	2,214,961	124 MB	2021-01-16 15:24	2021-09-22 09:33	202425	IP Volume inc	Netherlands	Europe
89.248.165.58	1	9	18,652,045	1,097 MB	2021-01-08 17:57	2021-09-15 07:41	202425	IP Volume inc	Netherlands	Europe
89.248.165.168	1	23	3,877,931	213 MB	2021-05-22 09:12	2021-09-09 03:16	202425	IP Volume inc	Netherlands	Europe
89.248.165.242	1	1	2,043	0 MB	2021-09-06 00:14	2021-09-06 00:14	202425	IP Volume inc	Netherlands	Europe
89.248.165.213	2	20	22,229,310	1,356 MB	2021-08-14 22:41	2021-09-01 12:51	202425	IP Volume inc	Netherlands	Europe
89.248.165.95	1	14	34,893,059	2,015 MB	2021-08-15 00:11	2021-08-28 15:05	202425	IP Volume inc	Netherlands	Europe
89.248.165.15	1	53	5,500,718	312 MB	2020-12-14 18:46	2021-08-28 15:03	202425	IP Volume inc	Netherlands	Europe

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

89.248.165.7	1	26	103,265,052	5,916 MB	2021-08-05 07:59	2021-08-22 02:10	202425	IP Volume inc	Netherlands	Europe
89.248.165.33	4	103	11,904,942	684 MB	2020-12-14 14:30	2021-08-13 21:40	202425	IP Volume inc	Netherlands	Europe
89.248.165.205	1	1	126,661	7 MB	2021-08-11 21:05	2021-08-11 21:05	202425	IP Volume inc	Netherlands	Europe
89.248.165.216	1	7	500,536	27 MB	2021-05-25 09:27	2021-07-07 02:47	202425	IP Volume inc	Netherlands	Europe
89.248.165.99	1	11	11,058,906	638 MB	2021-05-24 15:57	2021-07-03 08:30	202425	IP Volume inc	Netherlands	Europe
89.248.165.226	1	3	284,809	16 MB	2021-06-17 03:48	2021-06-28 05:08	202425	IP Volume inc	Netherlands	Europe
89.248.165.100	1	33	35,732,499	2,095 MB	2021-05-19 23:07	2021-06-26 10:42	202425	IP Volume inc	Netherlands	Europe
89.248.165.104	1	3	4,578	0 MB	2021-05-29 13:22	2021-05-31 21:00	202425	IP Volume inc	Netherlands	Europe
89.248.165.97	1	25	82,865,769	4,666 MB	2021-04-26 22:11	2021-05-24 21:53	202425	IP Volume inc	Netherlands	Europe
89.248.165.166	1	18	79,345,589	4,531 MB	2021-04-26 22:10	2021-05-23 03:41	202425	IP Volume inc	Netherlands	Europe
89.248.165.35	1	29	2,372,485	131 MB	2021-01-11 20:58	2021-05-17 23:03	202425	IP Volume inc	Netherlands	Europe
89.248.165.201	1	2	115	0 MB	2021-05-17 15:37	2021-05-17 15:37	202425	IP Volume inc	Netherlands	Europe
89.248.165.36	1	22	2,290,303	129 MB	2020-12-16 08:24	2021-05-16 11:57	202425	IP Volume inc	Netherlands	Europe
89.248.165.34	1	3	3,823,288	234 MB	2021-05-15 17:33	2021-05-16 07:42	202425	IP Volume inc	Netherlands	Europe
89.248.165.11	1	30	2,099,436	118 MB	2021-01-15 20:37	2021-04-13 08:46	202425	IP Volume inc	Netherlands	Europe
89.248.165.159	1	3	8,503	0 MB	2021-04-08 20:57	2021-04-08 21:00	202425	IP Volume inc	Netherlands	Europe
89.248.165.61	1	10	10,967,211	632 MB	2021-01-09 04:26	2021-03-17 01:58	202425	IP Volume inc	Netherlands	Europe
89.248.165.59	1	18	15,252,638	906 MB	2021-01-08 17:57	2021-03-15 04:25	202425	IP Volume inc	Netherlands	Europe
89.248.165.81	1	15	2,146,759	120 MB	2021-03-08 23:43	2021-03-15 00:54	202425	IP Volume inc	Netherlands	Europe
89.248.165.52	1	15	13,454,365	779 MB	2021-01-09 03:42	2021-03-06 21:08	202425	IP Volume inc	Netherlands	Europe
89.248.165.10	1	20	530,079	31 MB	2020-12-08 21:12	2021-02-22 02:39	202425	IP Volume inc	Netherlands	Europe
89.248.165.110	1	2	205,254	12 MB	2021-01-26 18:41	2021-01-26 18:52	202425	IP Volume inc	Netherlands	Europe
89.248.165.62	1	7	965,567	55 MB	2021-01-08 13:51	2021-01-24 18:32	202425	IP Volume inc	Netherlands	Europe
89.248.165.56	1	6	10,420,094	612 MB	2021-01-09 20:12	2021-01-23 17:25	202425	IP Volume inc	Netherlands	Europe
89.248.165.67	1	12	3,738,080	220 MB	2021-01-05 10:00	2021-01-19 10:19	202425	IP Volume inc	Netherlands	Europe
89.248.165.66	1	8	1,641,984	93 MB	2021-01-04 00:19	2021-01-18 02:59	202425	IP Volume inc	Netherlands	Europe
89.248.165.51	1	21	3,452,095	200 MB	2021-01-05 12:56	2021-01-15 21:20	202425	IP Volume inc	Netherlands	Europe
89.248.165.20	1	10	27,807,213	1,594 MB	2020-12-06 21:53	2021-01-02 09:07	202425	IP Volume inc	Netherlands	Europe
89.248.165.3	1	9	4,507,274	265 MB	2020-11-25 07:47	2020-12-09 13:07	202425	IP Volume inc	Netherlands	Europe

RECYBER.NET SCANNED PORTS

The following table lists all ports scanned by Recyber.net with their average number of packets per scan event, the average packet size and total packets and volume. The first and last recorded dates provide an indication when the port scans were active.

dst port	proto	# events	avg packets	total packets	total volume	avg packet size	first recorded	last recorded
Multiple	TCP	7,321	953,061	6,977,360,589	410,082 MB	59 bytes	2020-11-25 07:47	2022-09-29 14:18
80	TCP	94	10	962	0 MB	144 bytes	2021-03-09 21:32	2022-08-19 20:49
8080	TCP	15	3	46	0 MB	109 bytes	2022-02-18 23:40	2022-07-23 00:05
13484	TCP	1	1,741	1,741	0 MB	53 bytes	2022-07-10 05:06	2022-07-10 05:06
5060	UDP	30	89	2,675	1 MB	441 bytes	2021-05-10 08:46	2022-06-15 23:20
8443	IP	16	7	110	0 MB	43 bytes	2022-04-22 16:52	2022-06-07 00:07

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022



8080 IP	2	7	14	0 MB	45 bytes	2022-04-22 11:38	2022-04-22 11:39
Multiple IP	1	326,557	326,557	17 MB	53 bytes	2022-04-05 06:36	2022-04-05 06:36
0 ICMP	2	10,158	20,316	12 MB	576 bytes	2022-03-21 22:29	2022-03-26 20:53
33322 IP	1	1	1	0 MB	0 bytes	2022-02-27 00:18	2022-02-27 00:18
9231 IP	1	4	4	0 MB	0 bytes	2022-02-25 20:35	2022-02-25 20:35
9354 IP	1	1	1	0 MB	0 bytes	2022-02-24 16:01	2022-02-24 16:01
9199 IP	1	1	1	0 MB	0 bytes	2022-02-23 02:52	2022-02-23 02:52
7885 IP	1	1	1	0 MB	0 bytes	2022-02-20 21:10	2022-02-20 21:10
10990 IP	1	18	18	0 MB	21 bytes	2022-02-13 00:19	2022-02-13 00:19
10425 IP	1	1	1	0 MB	0 bytes	2022-02-12 19:01	2022-02-12 19:01
10433 IP	1	1	1	0 MB	0 bytes	2022-02-12 08:17	2022-02-12 08:17
5962 IP	1	4	4	0 MB	0 bytes	2022-02-10 19:33	2022-02-10 19:33
10348 IP	1	3	3	0 MB	0 bytes	2022-02-09 09:04	2022-02-09 09:04
4755 IP	1	1	1	0 MB	0 bytes	2022-02-04 14:01	2022-02-04 14:01
4768 IP	1	11	11	0 MB	23 bytes	2022-02-03 23:14	2022-02-03 23:14
37090 IP	1	12	12	0 MB	21 bytes	2022-02-02 05:18	2022-02-02 05:18
24090 IP	1	1	1	0 MB	0 bytes	2022-02-01 19:43	2022-02-01 19:43
16080 IP	1	1	1	0 MB	0 bytes	2022-01-30 15:33	2022-01-30 15:33
36070 IP	1	3	3	0 MB	0 bytes	2022-01-29 08:05	2022-01-29 08:05
1070 IP	1	1	1	0 MB	0 bytes	2022-01-28 06:33	2022-01-28 06:33
65060 IP	1	1	1	0 MB	0 bytes	2022-01-28 06:28	2022-01-28 06:28
4807 IP	1	1	1	0 MB	0 bytes	2022-01-28 06:17	2022-01-28 06:17
5060 TCP	4	250	1,002	0 MB	445 bytes	2021-08-26 22:13	2021-08-26 22:15
520 UDP	86	9	777	0 MB	36 bytes	2021-08-11 02:57	2021-08-13 21:40
443 IP	1	2	2	0 MB	0 bytes	2021-07-22 10:34	2021-07-22 10:34
113 IP	7	16	112	0 MB	50 bytes	2021-07-20 07:40	2021-07-20 08:56
53 TCP	33	43	1,410	0 MB	74 bytes	2021-03-04 16:17	2021-07-15 17:16
389 UDP	5	16,265	81,326	0 MB	0 bytes	2021-04-02 20:19	2021-07-02 21:42

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

IP Volume (AS202425)

According to their website, IP Volume offers over 3Tbps of network capacity and serves over 200,000 users. IP Volume provides an abuse policy on their website ([IP Volume](#)). The website, however, is very scarce in information and only provides an email contact for reporting abuse (abuse@ipvolume.net). Company information such as address and incorporation details are not mentioned on the website.

The domain registration information for ipvolume.net has the registrant's name and organization redacted for privacy. The address of the registrant is Kalkofnsvegur 2 in Reykjavik, Iceland. Might be a coincidence, but the domain 'bulletproof-servers.net' is registered with the same address and phone number as 'ipvolume.net'.

Abuse Policy:

IP Volume and its affiliates respect the Law and reserve the right to disable access to any IP address with immediate effect if it does not comply with its policies:

We do not allow any form of:

- Bulletproof Hosting
- Childporn/CSAM content (see <https://childporn.report>)
- Ddos attacks
- Brute force attacks
- Malware / Ransomware / Spyware (We use Shadowserver reports)
- Spam (We fight against spam with spamhaus.net)
- Phishing

We use Shadowserver for monitoring.

Authorities:

When Law Enforcement is asking about customer details with an official document, we will comply and assist them in their investigation.

Figure 16: IP Volume Abuse Policy (source: IP Volume website)

DECEPTION NETWORK EVENTS

Unsolicited network events registered by the Radware Global Deception Network increased from a few hundred packets per day before April 6, 2022 to several hundreds of thousands of packets per day, with an exponential increase since October 2022.

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

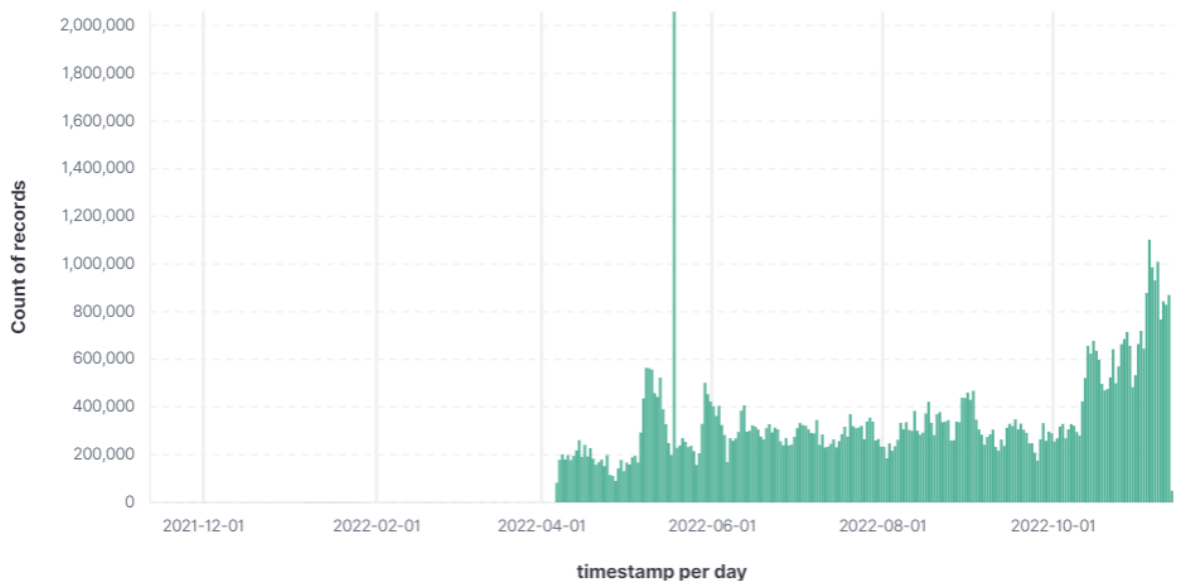


Figure 17: Unsolicited network events per day originating from IP Volume AS (source: Radware Global Deception Network)

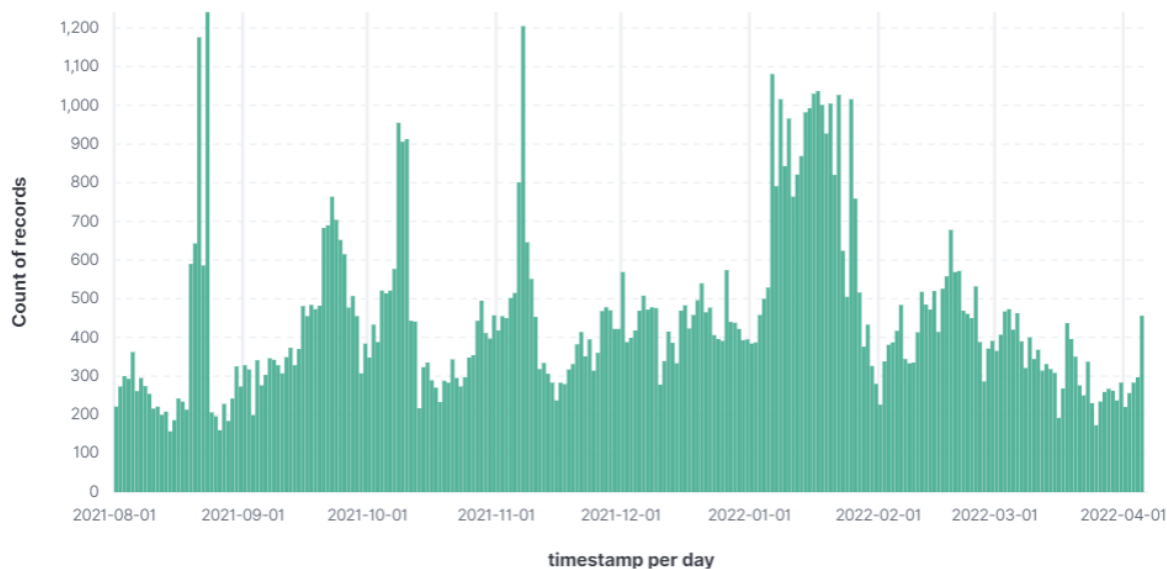


Figure 18: Unsolicited network events per day originating from IP Volume AS before April 2022 (source: Radware Global Deception Network)

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

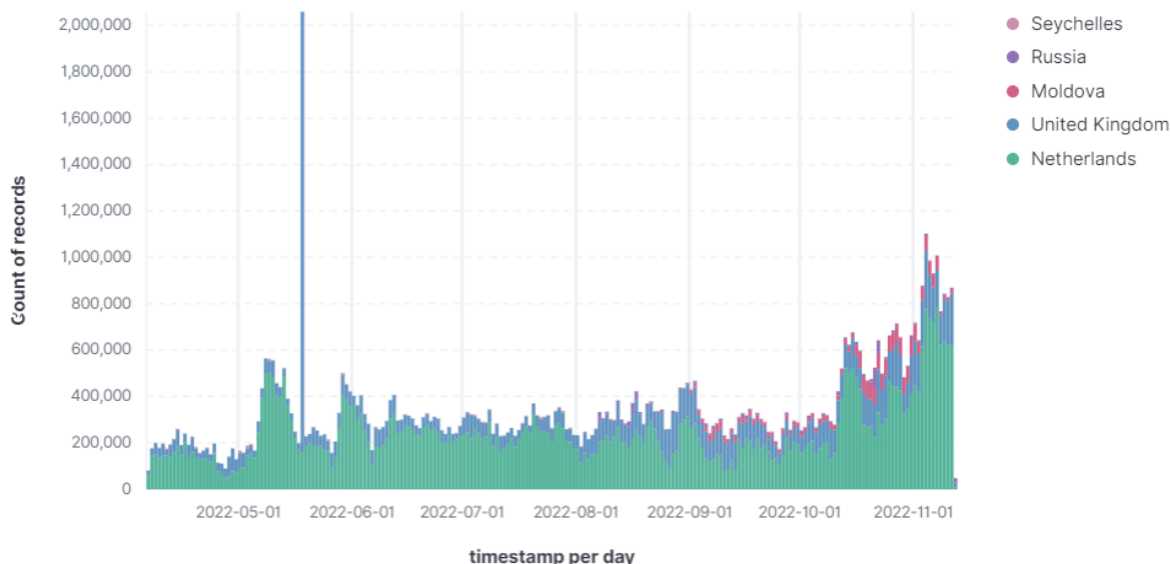


Figure 19: Unsolicited network events per day originating from IP Volume AS since April 2022, categorized by country of origin (source: Radware Global Deception Network)

On May 18, 2022, there was a spike of 2 million events. Starting October 11, 2022, the activity increases from an average of 200,000 events per day to an average of 800,000 packets per day.

Unsolicited network events originating from the IP Volume AS is spread evenly across the globe and across time, which is characteristic for global internet port and vulnerability scans.

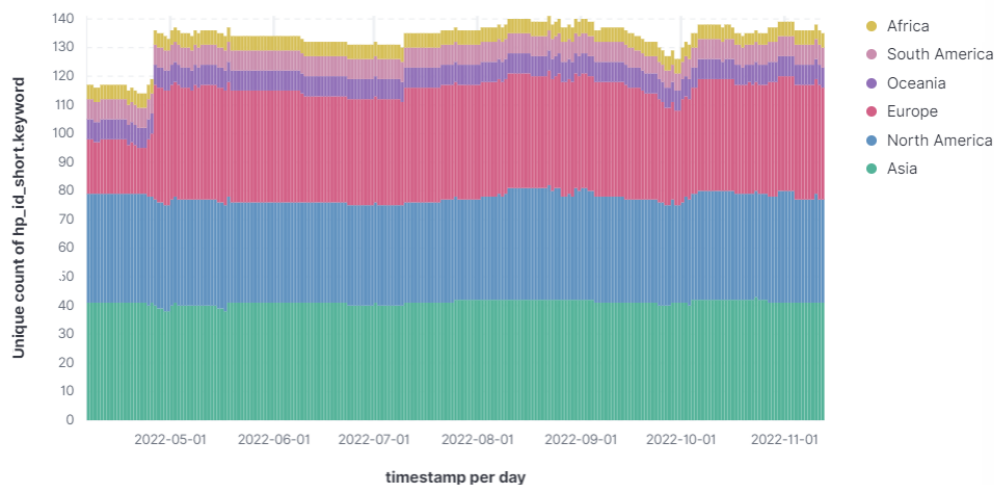


Figure 20: Number of sensors detecting IP Volume events per day per region (Source: Radware Global Deception Network)

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

CLOUD DDOS PROTECTION SERVICE EVENTS

The IP Volume traffic patterns are very similar to the Recyber.net traffic patterns. This is not surprising given that Recyber.net is operating from IP range of the IP Volume AS. Of all blocked packets originating from IP Volume (see paragraph 'Top 100 most intrusive IPs of IP Volume AS' below), 46.44% originated from Recyber.net hosts. The other blocked packets originated from internet scanning engines operated by [Shodan.io](https://shodan.io), [Openportstats.com](https://openportstats.com), [Criminal IP](https://criminalip.com) and [Group-ib.com](https://group-ib.com). Most traffic originating from IP Volume are scans and predominantly TCP port scans. Since April 2022, several days were reaching over 2 billion blocked packets per day originating from the IP Volume AS.

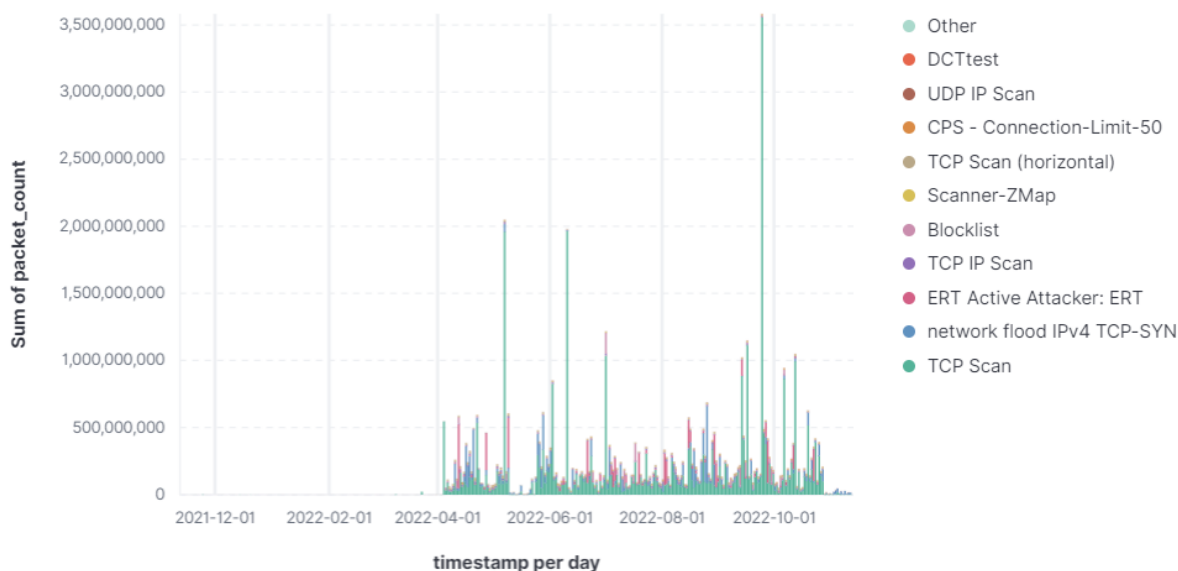


Figure 21: Blocked packets originating from IP Volume AS by attack category (source: Radware Cloud DDoS Protection Service)

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

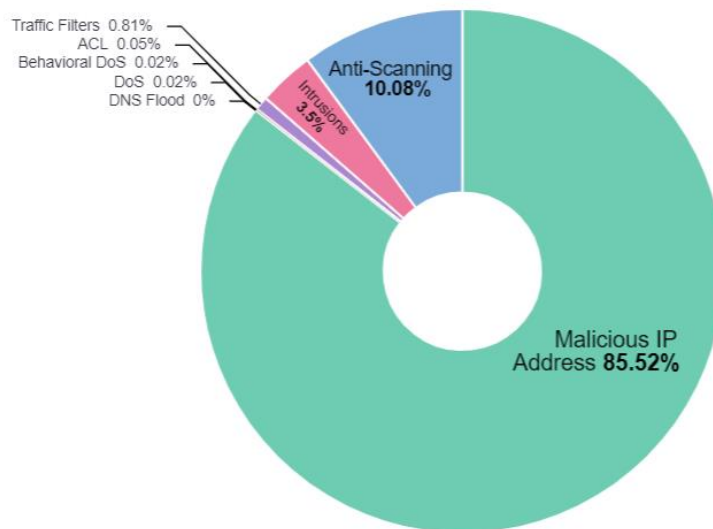


Figure 22: IP Volume packets blocked by major attack category (source: Radware Cloud DDoS Protection Service)

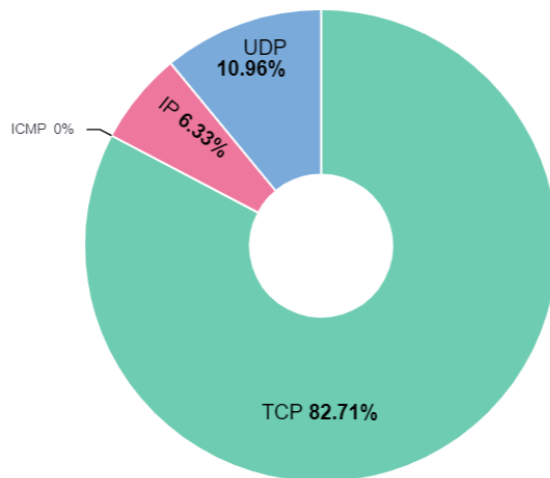


Figure 23: Protocol breakdown of IP Volume blocked traffic (source: Radware Cloud DDoS Protection Service)

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

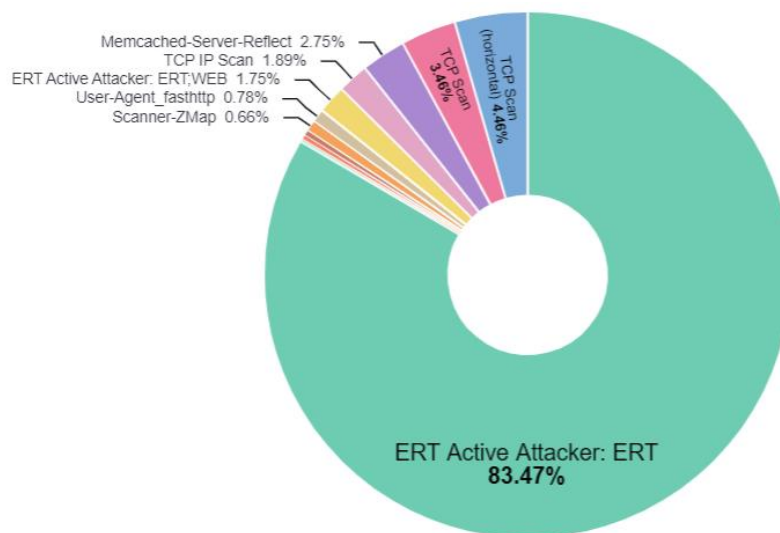


Figure 24: Breakdown of IP Volume blocked traffic by attack category (source: Radware Cloud DDoS Protection Service)

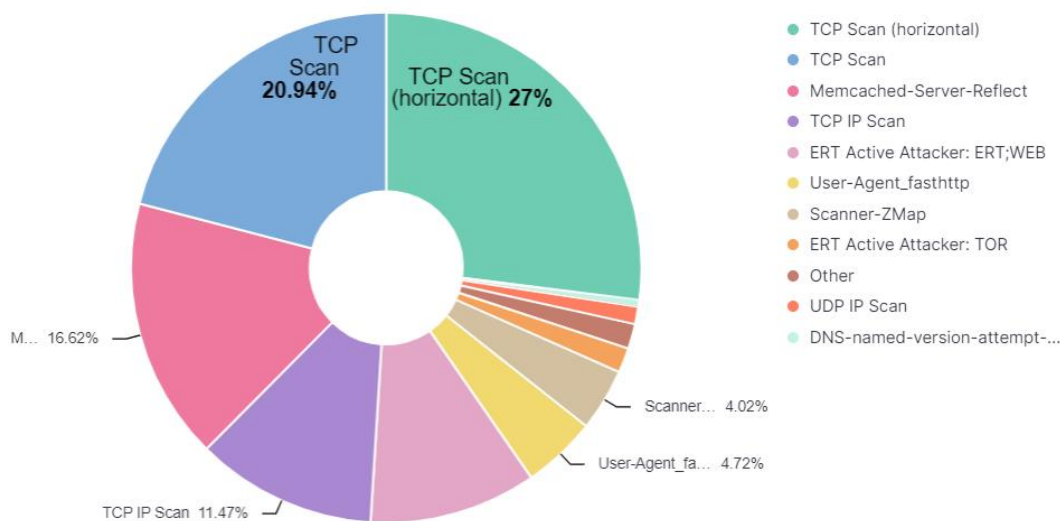


Figure 25: Attack categories of Non-EAAF classified traffic originating from IP Volume AS (source: Radware Cloud DDoS Protection Service)

The fasthttp events originating from the IP Volume AS were all recorded between Oct 15 and 21, 2022 and originated exclusively from Recyber.net.

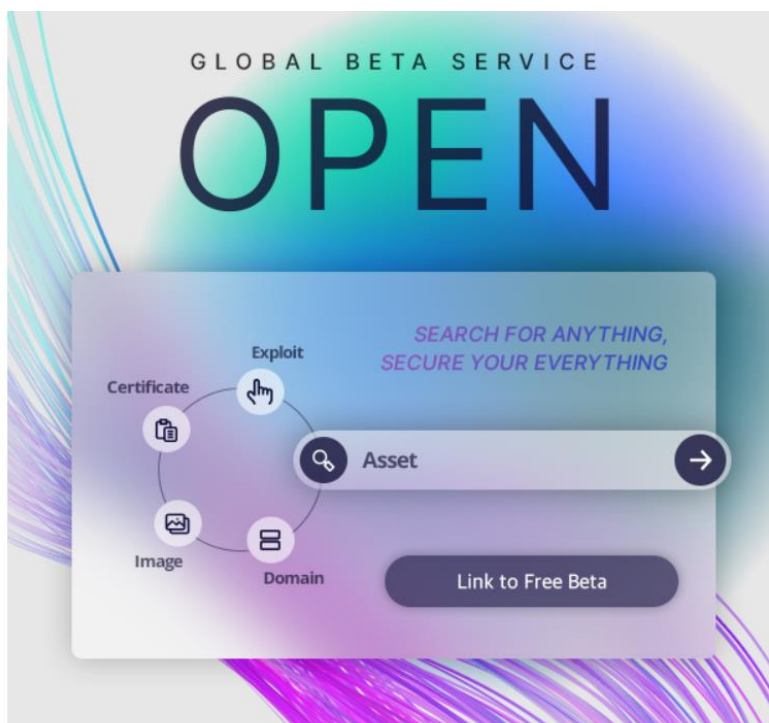
Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022



The Z-Map scans, about 4% of the non-EAAF classified attack traffic, was predominantly originating from IP addresses reverse-resolving to security.criminalip.com.



Criminal IP collects port information for only security/research purposes.

It only reads the response data from basic port requests, and never utilizes vulnerability scanning or other exploit scripts.

Our internet-wide, non-intrusive port scanning does not target specific IP addresses.

It differs from malicious acts such as DDoS attacks in that it simply surveys by knocking on the door(port).

We will permanently whitelist your IP address upon request.

For any inquiries, please contact request@aispera.com

Figure 26: Webpage showing when browsing to security.criminalip.com

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

TOP 100 MOST INTRUSIVE IPS OF IP VOLUME AS

Below is a list of top 100 most intrusive IPs of the IP Volume AS, including packet count and reverse-resolved hostname. Most IP addresses resolve to hosts from internet scanning services.

Client IP	Count	Reverse DNS
80.82.77.33	10,066,294	sky.census.shodan.io
80.82.77.139	9,595,546	dojo.census.shodan.io
93.174.95.106	8,657,862	battery.census.shodan.io
89.248.165.52	8,330,912	recyber.net
94.102.49.193	5,287,050	cloud.census.shodan.io
89.248.165.154	4,787,856	recyber.net
89.248.167.131	3,939,805	mason.census.shodan.io
80.82.70.228	3,586,405	rnd.group-ib.com
89.248.172.16	3,214,033	house.census.shodan.io
94.102.49.190	2,668,115	flower.census.shodan.io
89.248.163.199	2,638,754	recyber.net
89.248.165.199	2,154,899	recyber.net
89.248.163.221	1,865,631	recyber.net
80.82.64.146	1,729,907	no-reverse-dns-configured.com
89.248.165.81	1,519,106	recyber.net
80.82.64.114	1,485,109	no-reverse-dns-configured
5.8.18.8	1,337,114	no-reverse-dns-configured
89.248.165.104	1,335,031	recyber.net
89.248.165.178	1,317,604	recyber.net
89.248.165.121	1,297,468	recyber.net
89.248.165.69	1,264,490	recyber.net
89.248.165.118	1,221,482	recyber.net
89.248.165.59	1,213,998	recyber.net
89.248.165.65	1,154,912	recyber.net
89.248.163.241	1,133,384	recyber.net
89.248.163.240	1,131,738	recyber.net
89.248.165.241	1,075,331	recyber.net
89.248.165.89	1,070,865	recyber.net
89.248.165.73	1,059,609	recyber.net
89.248.165.99	1,037,027	recyber.net
89.248.165.63	1,027,835	recyber.net
89.248.163.237	1,007,976	recyber.net
89.248.165.119	976,561	recyber.net
89.248.165.71	928,154	recyber.net

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

80.82.65.202	887,424	scanner.openportstats.com
89.248.163.247	843,592	recyber.net
89.248.163.145	836,647	recyber.net
93.174.93.227	813,442	sigmax.io
89.248.165.53	811,351	recyber.net
89.248.165.110	807,122	recyber.net
89.248.165.242	796,966	recyber.net
89.248.165.100	780,879	recyber.net
89.248.165.83	771,672	recyber.net
89.248.163.239	741,456	recyber.net
89.248.165.87	734,613	recyber.net
89.248.165.70	732,273	recyber.net
89.248.168.172	706,046	no-reverse-dns-configured
89.248.165.205	703,710	recyber.net
89.248.165.8	692,867	recyber.net
89.248.165.91	673,520	recyber.net
89.248.165.109	665,174	recyber.net
89.248.165.23	651,459	recyber.net
80.82.65.62	603,176	scanner.openportstats.com
89.248.165.31	593,805	recyber.net
89.248.165.68	566,069	recyber.net
89.248.165.195	547,991	recyber.net
89.248.165.54	543,804	recyber.net
89.248.163.149	541,330	recyber.net
89.248.165.193	534,799	recyber.net
89.248.165.184	534,555	recyber.net
89.248.165.186	529,316	recyber.net
89.248.165.187	523,114	recyber.net
89.248.165.17	517,970	recyber.net
89.248.165.22	509,385	recyber.net
89.248.163.200	505,092	recyber.net
89.248.165.76	503,447	recyber.net
89.248.165.43	488,479	recyber.net
89.248.163.215	483,440	recyber.net
89.248.170.29	481,039	no-reverse-dns-configured
80.82.77.144	475,894	no-reverse-dns-configured
80.82.64.100	471,520	no-reverse-dns-configured
89.248.165.90	463,777	recyber.net
89.248.163.150	461,266	recyber.net

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

89.248.165.51	455,515	recyber.net
89.248.163.186	453,351	recyber.net
89.248.165.86	448,016	recyber.net
89.248.165.122	440,019	recyber.net
89.248.165.189	437,275	recyber.net
89.248.172.95	435,599	no-reverse-dns-configured
89.248.165.74	409,251	recyber.net
89.248.165.120	405,553	recyber.net
89.248.165.85	400,380	recyber.net
94.102.61.4	379,564	security.criminalip.com
89.248.163.187	371,427	recyber.net
89.248.165.203	368,891	recyber.net
80.82.64.72	363,574	no-reverse-dns-configured
89.248.165.24	358,958	recyber.net
89.248.173.131	358,356	no-reverse-dns-configured
89.248.163.252	349,369	recyber.net
89.248.163.251	347,902	recyber.net
89.248.163.140	345,865	recyber.net
89.248.165.108	331,574	recyber.net
94.102.61.3	315,009	security.criminalip.com
89.248.165.151	314,006	recyber.net
89.248.163.227	299,583	recyber.net
94.102.61.44	285,218	security.criminalip.com
89.248.165.75	280,781	recyber.net
94.102.61.28	269,322	security.criminalip.com
89.248.165.60	264,976	recyber.net
94.102.61.47	258,731	security.criminalip.com
Other	19,432,728	

Reasons for Concern

Radware is a supporter of global internet scans to assess the risk of new vulnerabilities and publicly exposed services that might impact the integrity of the internet and could be abused to compromise online services. Scanning needs to be performed responsibly and respect the targeted infrastructure. Most white hat internet scanning services do provide the ability for organizations to opt-out. However, the proliferation of scanning

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022

services and, in some cases, information provided by the scanners is dubious at best that opting-out is just not a manageable option of organizations.

In the case of Recyber.net the scanning activity results in an average load of 6Mbps and a 95th percentile of 16Mbps on the network and server infrastructure of organizations globally. The average 12k packets per second and 95th percentile of 70k PPS at best convolute event detection and correlation with a risk of misclassification and wild goose chases by security operating centers and researchers. When scans are that aggressive, the packet rates reach levels comparable to micro flood DDoS attacks and can impact resources of servers and network infrastructure. Given that organizations are not directly benefiting from the activity performed by most scanning services, the lost bandwidth and processing cycles come at a financial cost. As such our advice is to block scanning attempts as early as possible in the network infrastructure.

Every scanning service operates independently and considers its scanning information intellectual property that will not be shared. More organizations are seeing benefits and a need for scanning the global internet for different reasons. By consequence, the resulting grey noise of the internet is not going anywhere and if we consider our micro flood statistics, the speed at which new vulnerabilities are exploited and the rate of accidentally exposed services on the internet, the grey noise will all but increase in the future.

Mitigating the impact of grey noise

Managing the process of opting-out of all internet scanning services is close to impossible for organizations. Additionally, not all scanning activity can be identified as responsible or white hat scanning with benign objectives, black hats are continuously performing automated exploiting and scanning for vulnerabilities or exposed services. The only way to manage the noise resulting from black and white hat scanning activity is by detecting and blocking the activity as early as possible when it reaches the network infrastructure of the organizations.

Statistics from Radware's Cloud DDoS Protection Service demonstrate that 75 to 80% of this grey noise can be blocked with a low overhead by leveraging an IP intelligence feed that tracks active attackers. The Radware ERT Active Attackers Feed (EAAF) has been designed for the purpose of detecting and blocking the most intrusive hosts on the internet, based on a global deception network and several correlation and cross-validation algorithms to ensure there are no false positives. EAAF is available as a subscription for on-premise DefensePro customers as well as our cloud customers.

For global internet scanners that are less intrusive, the behavioral detection algorithms in Radware's DefensePro on-premise DDoS protection will detect and block scanning attempts and keep the network and servers free of unsolicited traffic.

Radware Cybersecurity Advisory

Internet noise is taxing online services and businesses – Recyber.net use case

November 16, 2022



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.