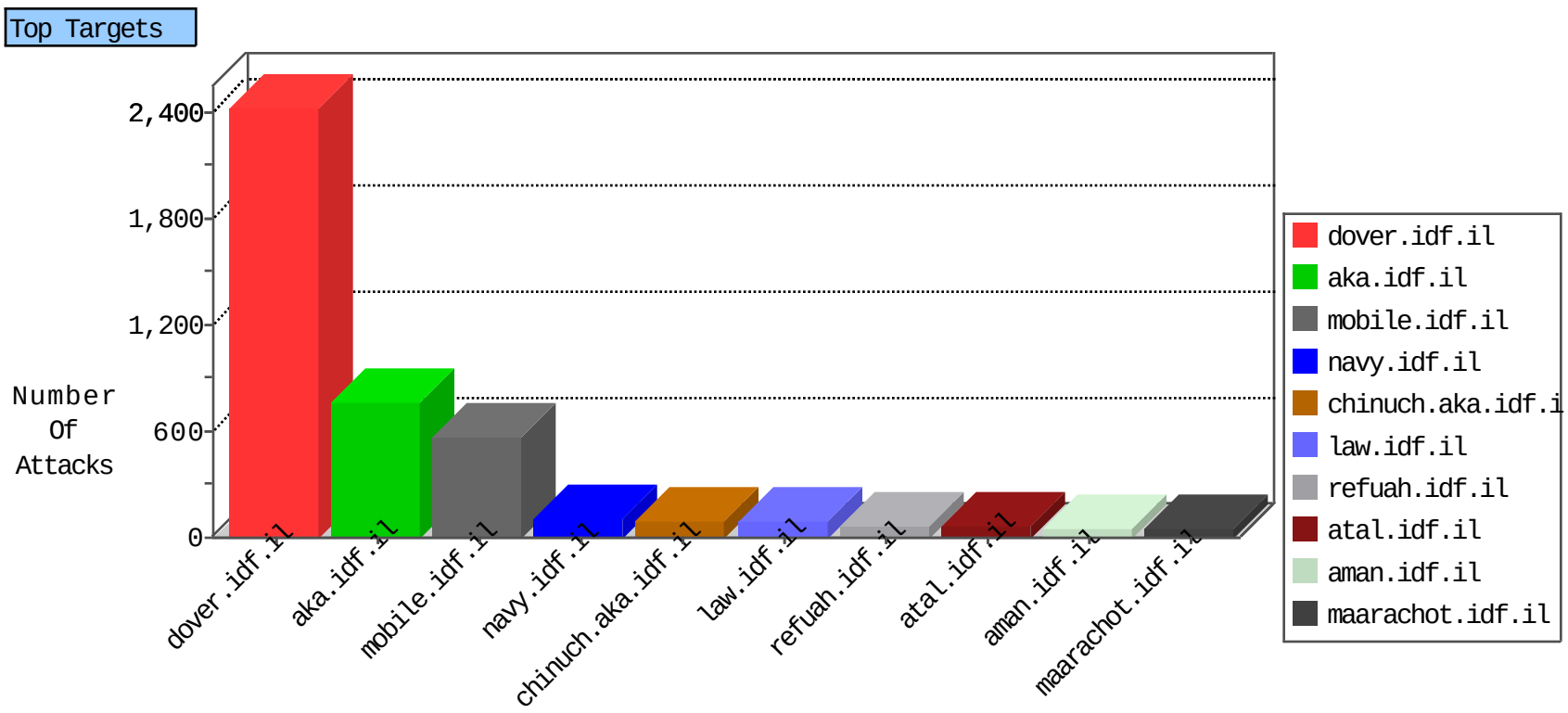
10-30-2015-16:04:02 to 10-30-2015-17:04:02

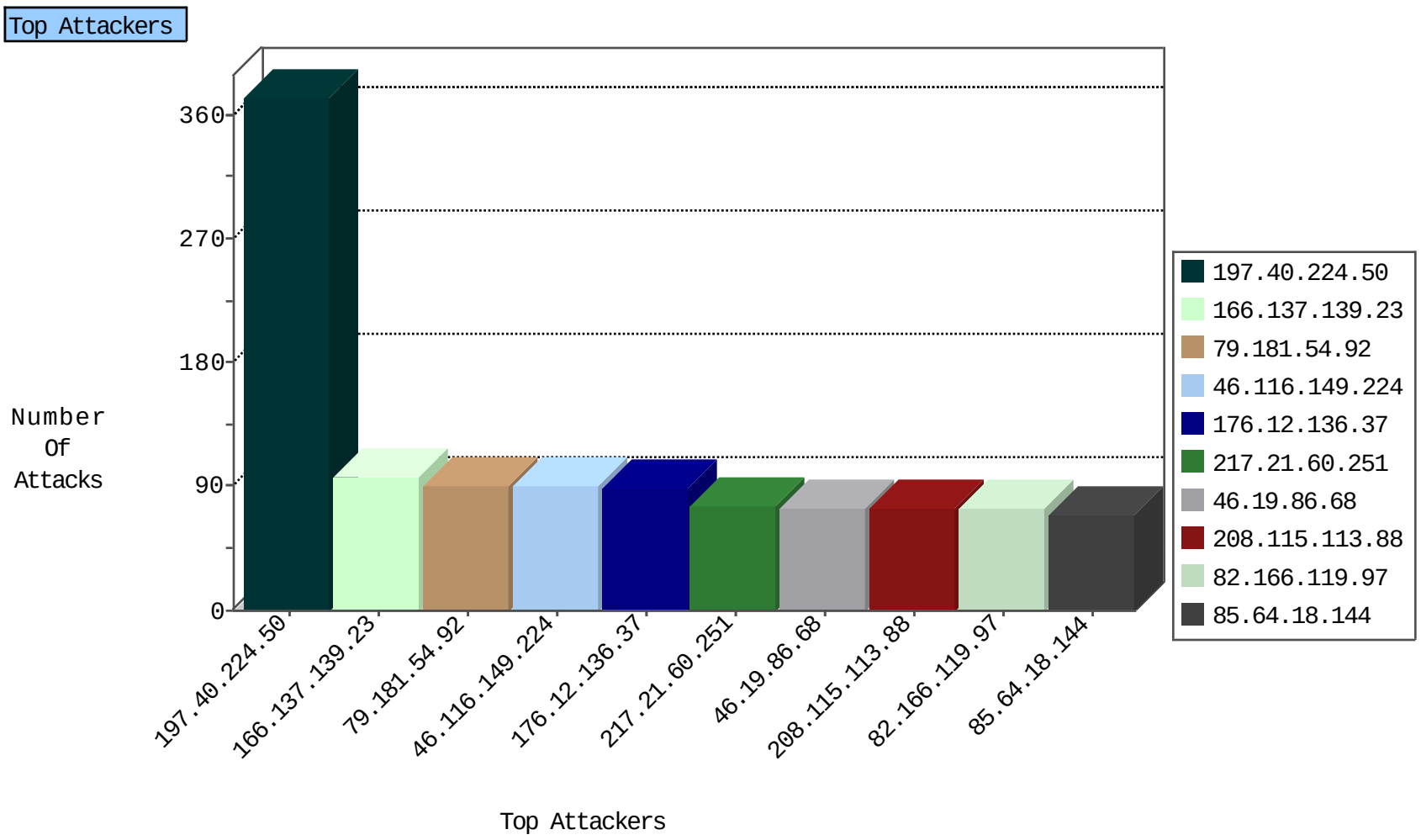
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-30-2015-16:04:02 to 10-30-2015-17:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4826
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3687
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	133
217.21.60.251	Belarus	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
46.19.85.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
24.125.7.0	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
84.190.30.10	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
109.67.207.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
93.173.169.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
31.154.92.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
79.179.179.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
84.108.235.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
66.249.75.60	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.176.29.228	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.219.144.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6
79.179.179.30	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
84.86.229.37	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.54.130.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.172.10.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.177.205.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.120.126.44		147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.172.174.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
85.65.77.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
2.54.182.229	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
82.81.11.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.88.242.19	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.86.229.37	Netherlands	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.1.76	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.26.146.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
149.78.236.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
10.0.0.2		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
85.64.18.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
217.132.232.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
149.88.23.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
98.248.47.127	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
85.64.190.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
84.109.0.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
216.126.81.9	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.187.175	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
86.145.124.56	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.13.5.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.173.230.186	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
37.26.149.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-30-2015-16:04:02 to 10-30-2015-17:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.102.250.133	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

10-30-2015-16:04:02 to 10-30-2015-17:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.75.60	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.25	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
82.102.250.133	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP encoded cross site scripting HTML Image tag attempt	2
66.249.67.27	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
212.7.209.9	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.194	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.239.227	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.102.250.133	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SQL Injection - Select From	1
220.132.29.212	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
219.92.36.38	147.237.0.17	Malaysia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
212.7.209.9	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.7.209.9	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.7.209.9	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.7.209.9	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
184.106.185.15	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
223.4.239.227	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.173.169.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
223.4.239.227	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
219.92.36.38	147.237.0.17	Malaysia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
219.92.36.38	147.237.0.17	Malaysia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
212.7.209.9	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.7.209.9	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-30-2015-16:04:02 to 10-30-2015-17:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.40.224.50	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
166.137.139.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
85.64.18.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
24.218.80.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
79.183.125.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
217.21.60.251	Belarus	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
2.54.25.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
109.66.126.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
46.19.86.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
185.24.76.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
150.131.104.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.224.189.132	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.54.187.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
84.190.30.10	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
223.196.160.1	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
2.52.166.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.180.55.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
145.97.64.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
157.150.193.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
85.64.60.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
82.166.119.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
166.137.252.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.118.11.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.12.136.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.180.170.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.142.68.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
49.169.125.160	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.154.92.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
131.91.4.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.148.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.78.224.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
67.71.28.68	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.202.52.100	Germany	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.40.224.50	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.40.224.50	Block	270
79.181.54.92	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	90
176.12.136.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	75
46.19.86.68	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	75
82.166.119.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	60
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	60
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	45
37.26.149.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
46.116.149.224	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	45
46.116.149.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	45
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	45
176.13.5.211	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
85.65.244.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
84.229.133.95	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.229.133.95	Block	30
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	30
79.181.215.109	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	30
37.26.148.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
201.139.253.209	Mexico	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
2.52.166.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.69.84	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
79.182.121.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
207.46.13.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chinuch/miktzoa/default.asp	None	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10641-he/dover.aspx	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
149.78.242.45	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	15
84.108.41.24	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1151-he/chinuch.aspx	Block	15
77.125.240.36	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	15
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 103 cookies	Block	15
5.29.158.80	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	15
180.76.15.162	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	15
66.249.69.92	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	15
85.250.240.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
64.72.84.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	15
79.183.214.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main/stm	Block	15
41.230.14.222	Tunisia	147.237.77.216	dover.idf.il	Parameter Type Violation a in www.idf.il/	Block	15
207.46.13.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/brothers/skira/default.asp	None	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
213.199.214.20	Poland	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
31.154.7.4	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	15
188.64.102.238	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	15
66.249.75.53	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/templates/searchresults/searchresults.aspx	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
87.68.23.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15