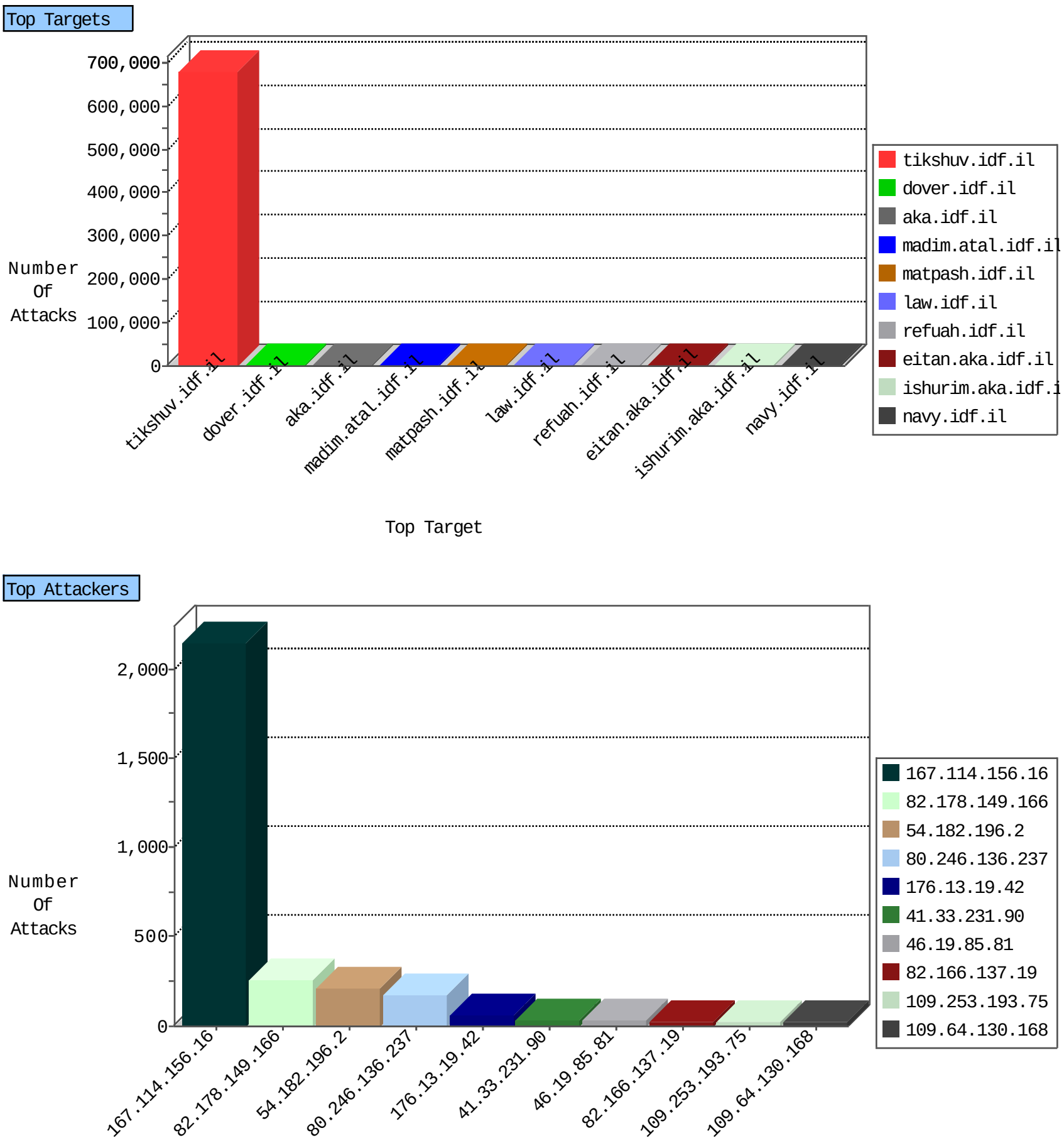
12-28-2015-16:04:01 to 12-28-2015-17:04:01

IDF Under Attack Daily Report



12-28-2015-16:04:01 to 12-28-2015-17:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	6539464
52.84.198.222	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1877522
0.0.0.0		147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	193999
52.33.60.210	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	4596
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3717
54.247.183.198	Ireland	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1371
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	188
176.34.50.221	Japan	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	98
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
82.178.149.166	Oman	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	56
52.35.63.176	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	4
54.192.231.7	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	3
82.178.149.166	Oman	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
54.165.160.169	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	2
184.73.224.217	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	2
54.231.224.113	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	2
52.76.204.23	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.86.175.18	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.182.146.40	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
54.210.216.171	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.240.251.66	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
107.22.176.161	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
52.2.211.99	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
52.30.97.210	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1
54.75.240.4	Ireland	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.154.136.21	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.193.59.55	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.229.130.180	Ireland	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.251.109.155	Singapore	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
46.137.215.249	Singapore	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
52.11.96.41	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.68.241.221	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.152.43.214	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.192.68.240	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
54.225.232.166	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.247.190.152	Ireland	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
46.51.240.71	Japan	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
198.48.92.104	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
52.10.19.10	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
52.76.14.9	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.85.184.112	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
54.175.22.191	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.209.10.186	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
54.238.177.251	Japan	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
107.20.169.18	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
52.1.140.228	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
52.26.255.28	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.173.25.82	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	1
54.205.67.69	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1
54.234.192.188	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-SYN-ACK	drop	1

12-28-2015-16:04:01 to 12-28-2015-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-28-2015-16:04:01 to 12-28-2015-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.178.149.166	147.237.77.216	Oman	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	190
132.70.66.14	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
85.250.122.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.76.30		himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
81.132.120.232	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.72.167		ishurim.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
79.180.203.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.8.24		e.lifestyle.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
77.125.140.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.97.185	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
62.90.49.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
89.139.224.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.95.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.77.234		halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.80.219.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.72.217		e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.243.75.37	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.72.156		aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.180.8.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.97.185	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
66.36.130.181	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.97.185	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
109.253.193.75	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
94.29.192.153	147.237.76.202	Kuwait	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.8.204.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-28-2015-16:04:01 to 12-28-2015-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
54.182.196.2	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	214
82.178.149.166	Oman	147.237.77.216	dover.idf.il	drop	SAM rule	drop	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.13.19.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	33
176.13.19.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
109.64.130.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
54.164.56.167	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	20
54.153.185.23	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	20
54.175.88.213	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	20
54.174.206.126	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	19
54.172.34.228	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	18
54.164.177.123	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	18
54.152.8.7	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	18
54.164.64.13	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
52.91.189.183	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
54.66.223.160	Australia	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
52.1.101.25	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
52.0.30.2	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
54.165.150.23	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
54.84.0.137	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
54.79.17.199	Australia	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
54.79.104.76	Australia	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
54.84.200.56	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
54.85.175.218	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
54.243.142.164	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
107.23.179.15	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
109.253.193.75	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
107.21.8.119	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
107.21.200.45	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
107.22.107.56	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
107.23.3.120	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
107.23.12.111	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
107.23.124.184	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
174.129.231.219	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
175.96.141.224	Taiwan	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
184.72.238.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.173.88.253	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.85.94.50	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.165.1.150	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.165.221.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.174.23.174	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.174.92.47	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.175.192.8	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.152.10.55	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.85.7.191	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.86.48.154	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.173.41.192	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
52.3.41.89	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
52.3.250.160	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
23.21.196.145	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15

12-28-2015-16:04:01 to 12-28-2015-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
80.246.136.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.130.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.180.162.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.145.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.110.145.113	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	3
2.52.39.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.138.45.16	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.90.241.164	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
80.246.136.91	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
180.76.15.5	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.108.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
149.78.30.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
37.46.39.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
79.178.151.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl89 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.116	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.160.206.149	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
37.187.114.171	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/irj/portal	Block	1
94.242.250.117	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
183.138.168.11	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1391-en/shared/usercontrols/headerupper/	Block	1
37.26.146.214	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
84.109.179.56	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/1.he/langstyle.css	Block	1
46.121.92.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.16.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.179.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
78.47.17.5	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
217.132.15.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.48.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.119.41.5	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
37.26.149.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
85.64.19.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.217.35	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	1
54.81.87.21	United States	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
176.13.16.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.179.26.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	1
46.19.85.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.93.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/forgotpassword.aspx	Block	1

12-28-2015-16:04:01 to 12-28-2015-17:04:01