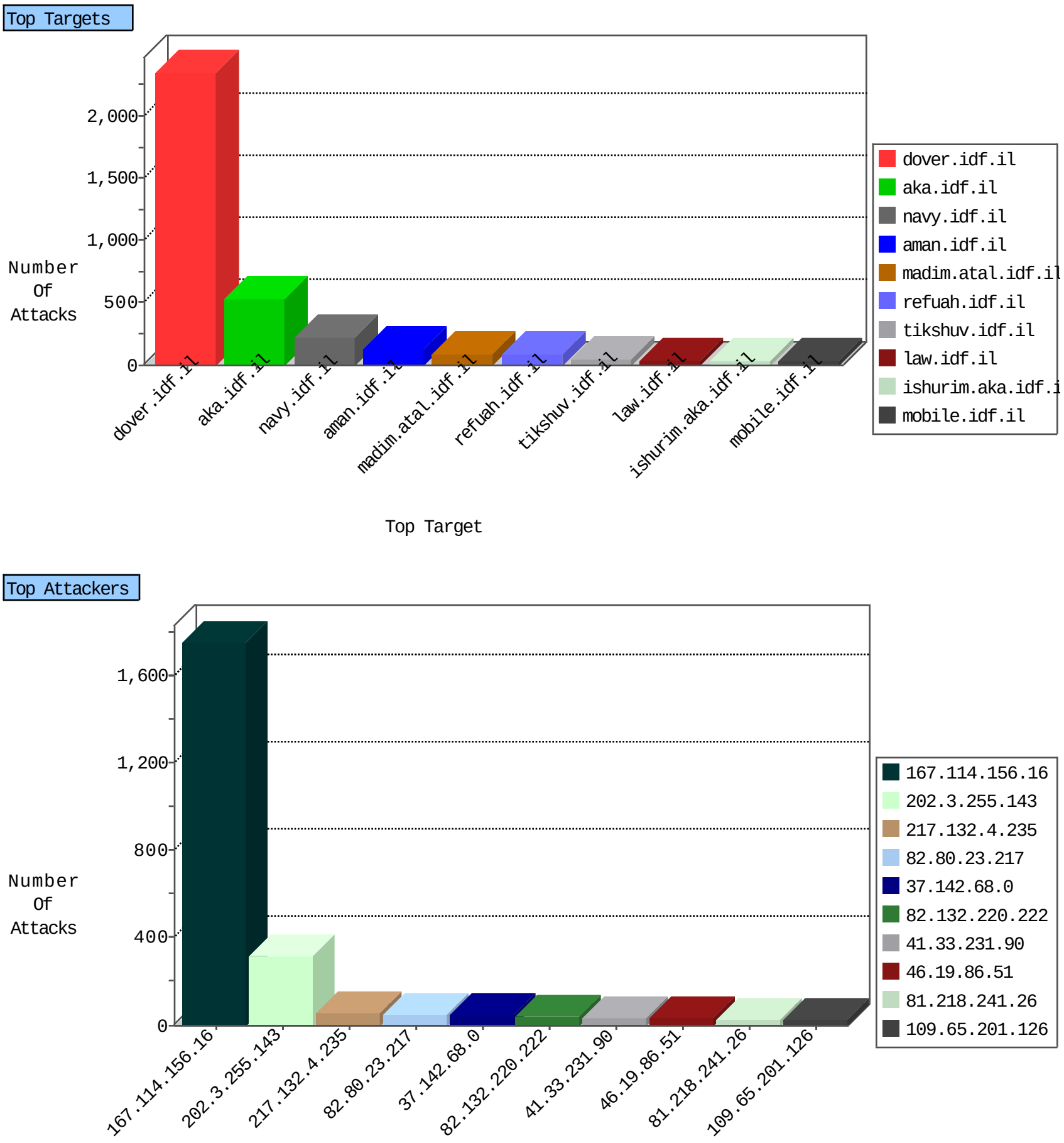
01-18-2016-16:04:05 to 01-18-2016-17:04:05

IDF Under Attack Daily Report



01-18-2016-16:04:05 to 01-18-2016-17:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3119
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
77.153.148.47	France	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
142.54.169.162	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
104.236.110.113		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.165	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1

01-18-2016-16:04:05 to 01-18-2016-17:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.224.24	Israel	147.237.77.74	law.idf.il	C157: HTTP: Access to GetFile.aspx	Block	24
109.226.45.219	Israel	147.237.0.34	tikshuv.idf.il	C208: HTTP: Range in the Header	Block	15
85.250.135.24	Israel	147.237.77.170	maarachot.idf.il	C208: HTTP: Range in the Header	Block	12
180.245.57.195	Indonesia	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	8
132.74.58.146	Israel	147.237.77.170	maarachot.idf.il	C208: HTTP: Range in the Header	Block	6
109.64.204.145	Israel	147.237.76.30	himush.idf.il	C208: HTTP: Range in the Header	Block	6
62.0.54.2	Israel	147.237.76.31	nakchal.idf.il	C004: HTTP: options method (Microsoft)	Block	6
85.250.170.7	Israel	147.237.0.34	tikshuv.idf.il	C208: HTTP: Range in the Header	Block	4
77.127.177.251	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
93.172.131.51	Israel	147.237.0.34	tikshuv.idf.il	C208: HTTP: Range in the Header	Block	3
197.38.205.20	Egypt	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	3
31.13.112.118	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	3
212.179.79.250	Israel	147.237.77.170	maarachot.idf.il	C208: HTTP: Range in the Header	Block	3
109.253.145.196	Israel	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	2
2.54.29.116	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
104.131.147.112	United States	147.237.77.74	law.idf.il	C157: HTTP: Access to GetFile.aspx	Block	2
46.38.63.9	Russian Federation	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	2
31.13.112.122	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	2
89.138.119.74	Israel	147.237.77.74	law.idf.il	C157: HTTP: Access to GetFile.aspx	Block	1
46.19.85.142	Israel	147.237.77.226	www.chamatz.aka.idf.il	C208: HTTP: Range in the Header	Block	1
31.13.100.113	Ireland	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	1
79.181.181.170	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
31.13.112.117	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	1
173.252.74.113	United States	147.237.76.30	himush.idf.il	C208: HTTP: Range in the Header	Block	1
46.19.85.171	Israel	147.237.77.233	atal.idf.il	C208: HTTP: Range in the Header	Block	1
31.13.100.114	Ireland	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	1
79.182.17.38	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
2.54.63.146	Israel	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	1
173.252.74.114	United States	147.237.76.30	himush.idf.il	C208: HTTP: Range in the Header	Block	1
31.13.100.116	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	1
142.54.169.162	United States	147.237.0.19	madim.atal.idf.il	C098: Block - dns poisoning	Block	1
31.13.100.112	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	1
173.252.90.96	United States	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	1
31.13.109.120	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	1
149.210.158.71	Netherlands	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	1
31.13.113.86	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	1
31.13.100.113	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	1
176.13.18.208	Israel	147.237.77.233	atal.idf.il	C208: HTTP: Range in the Header	Block	1
31.13.110.106	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	1
173.252.74.99	United States	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	1

01-18-2016-16:04:05 to 01-18-2016-17:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	282
168.62.238.153	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.127.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.56.221.222	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.14.173.65	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.13.13.8	147.237.76.86	Israel	navy.idf.il	GPL SCAN myscan	1
109.65.97.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.i	ET SCAN NMAP -sS window 1024	1
46.19.86.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.117.148.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.13.8	147.237.76.86	Israel	navy.idf.il	INDICATOR-SCAN myscan	1

01-18-2016-16:04:05 to 01-18-2016-17:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.132.4.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
82.80.23.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.142.68.0	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
109.65.201.126	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.142.68.0	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
185.89.217.234		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
46.117.157.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	19
185.89.217.231		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
37.8.78.97	Palestinian Territory, Occupied	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
185.89.217.227		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
109.66.101.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.89.217.225		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
79.177.168.16	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
185.89.217.232		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
185.89.217.226		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
46.19.86.3	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.235		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
109.67.60.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
93.173.189.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
93.173.189.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
185.89.217.228		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
37.26.149.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.43	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
89.139.254.113	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
17.78.79.134	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
84.111.226.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.137.116	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.114.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
74.6.254.127	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
185.89.217.230		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
79.179.59.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.3.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.43	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.89.217.233		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
85.64.94.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.182.148.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.36.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.45.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
85.64.106.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.115.189.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
93.172.37.140	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
85.64.106.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.8.204.45	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
77.125.107.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
77.127.255.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.52.166.246	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	9
79.183.144.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.144.113	Block	5
46.19.85.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
212.199.232.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ishurim	Block	4
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.25.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
166.172.185.81	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.181.110	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/	Block	3
41.130.23.193	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1115-ar	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
5.29.253.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.144.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
2.54.155.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.226.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
87.68.76.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
212.76.122.17	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 212.76.122.17	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.253.150.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.166.246	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	2
194.90.88.105	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.90.236	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
37.26.147.208	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.126.62.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.153.109	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
85.64.106.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.242.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
198.20.226.241	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
46.19.86.41	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
176.13.12.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.209.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.145.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18035-he	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.154.86.181	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
94.23.6.148	France	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
2.52.21.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.78.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.117.128.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.232.194.23	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1