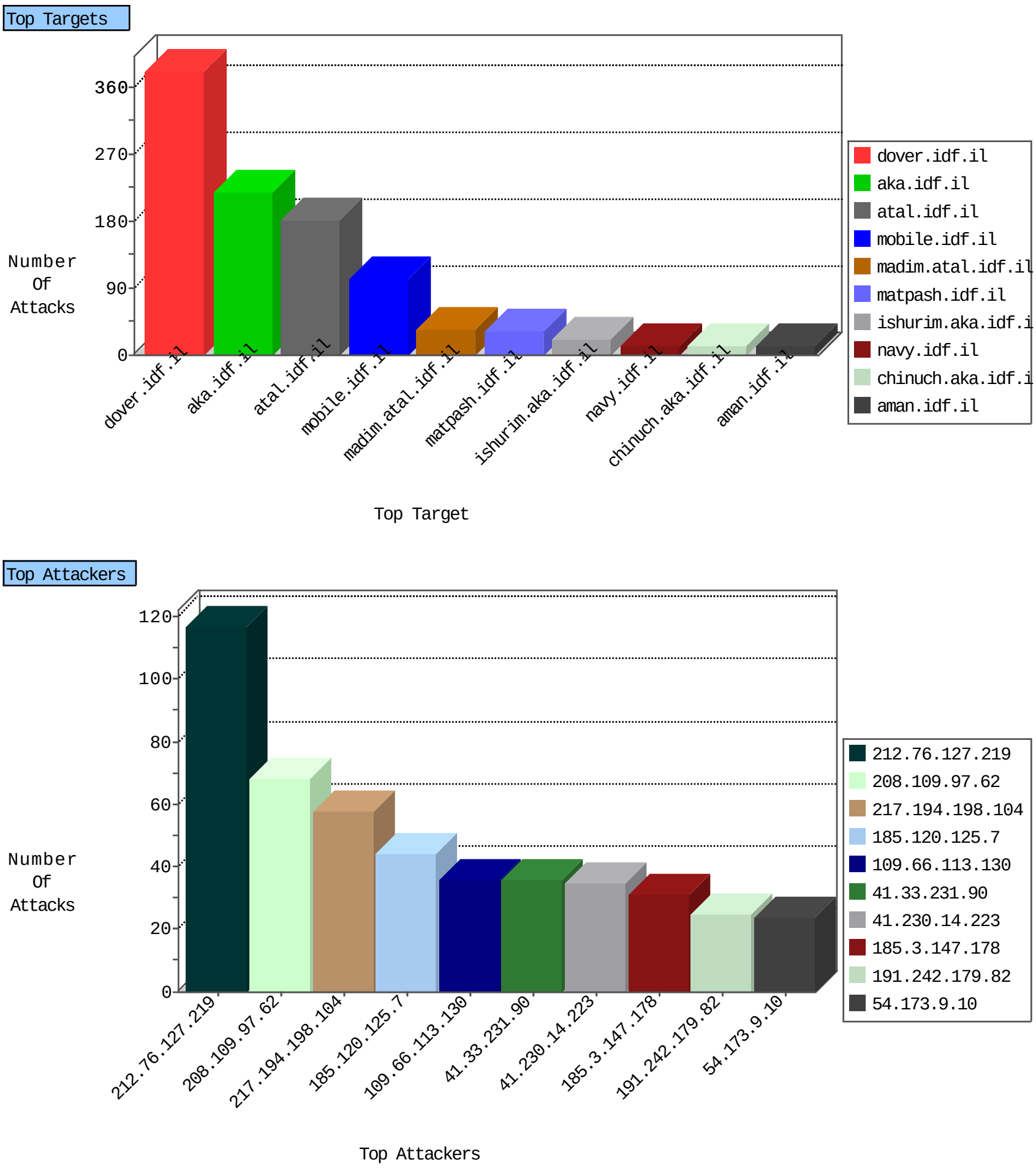
02-01-2016-00:04:01 to 02-01-2016-01:04:01

IDF Under Attack Daily Report



02-01-2016-00:04:01 to 02-01-2016-01:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.109.97.62	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1817
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	28
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	8
115.239.228.10	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2
184.26.161.65	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
192.99.39.151	Canada	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
74.91.28.58	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
142.54.160.213	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
74.91.28.58	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
184.26.161.65	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

02-01-2016-00:04:01 to 02-01-2016-01:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.119.118.213	Ukraine	147.237.76.147	chinuch.aka.idf.i	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

02-01-2016-00:04:01 to 02-01-2016-01:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
212.76.99.155	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
115.29.224.200	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
130.211.93.253	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.42	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
61.76.142.220	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.77.243	China	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.42	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.77.205	China	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.199.57.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.29.224.200	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.183.248.41	147.237.76.198	Korea, Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.183.248.41	147.237.76.147	Korea, Republic of	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.183.248.41	147.237.76.38	Korea, Republic of	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.183.248.41	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Potential SSH Scan	1
61.76.142.220	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Potential SSH Scan	1
125.27.37.60	147.237.76.34	Thailand	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.56.42	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.76.142.220	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.77.234	China	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.42	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.77.74	China	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.29.224.200	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.183.248.41	147.237.76.148	Korea, Republic of	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
210.183.248.41	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.183.248.41	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.183.248.41	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.76.142.220	147.237.76.148	Korea, Republic of	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

02-01-2016-00:04:01 to 02-01-2016-01:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	117
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.3.147.178	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
109.66.113.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.230.14.223	Tunisia	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	20
54.173.9.10	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.127.182.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
85.64.4.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
185.120.126.14		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
37.46.39.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.128.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.26.146.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.64.4.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.4.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.65.187.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.185.204	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.184	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.253.142.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
54.174.179.157	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.183.120.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.37.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.17.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.200.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.254	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.119.184.130	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.149.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.207.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
79.178.182.23	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.182.23	Block	11
109.66.113.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 217.194.198.104	Block	6
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 217.194.198.104	Block	6
109.253.223.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 217.194.198.104	Block	5
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 217.194.198.104	Block	5
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 217.194.198.104	Block	5
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 217.194.198.104	Block	4
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 217.194.198.104	Block	4
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 217.194.198.104	Block	4
54.173.9.10	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.173.9.10	Block	3
109.253.147.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 217.194.198.104	Block	3
2.54.63.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
80.178.16.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.66.99.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.207.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.194.198.104	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 217.194.198.104 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
46.19.85.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.5.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.180.111	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
188.143.232.35	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.35	Block	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 217.194.198.104	Block	2
80.246.136.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.46.39.9	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.63.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.65.128.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.190.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 217.194.198.104	Block	2
5.156.226.134	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
87.69.40.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1379-he/dover.aspx	Block	1
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/mobile/	Block	1
109.253.215.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding f×ƒÂ«××œ[[#3]][[#0]]am×’×¥zf×—Æ’â€¹Ã™Â oÂ£[[#0]]bÂšÂ¶i×¢â€¦ hrÂ§zâ€œ#pyt[[#18]]â€”â€°Â?Â¢6Ã?Ë†×‘	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.13.0.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
76.198.45.188	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
109.253.130.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.147.152.144	Croatia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
217.194.198.104	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
94.189.150.223		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Parameter Encoding from 217.194.198.104	None	1