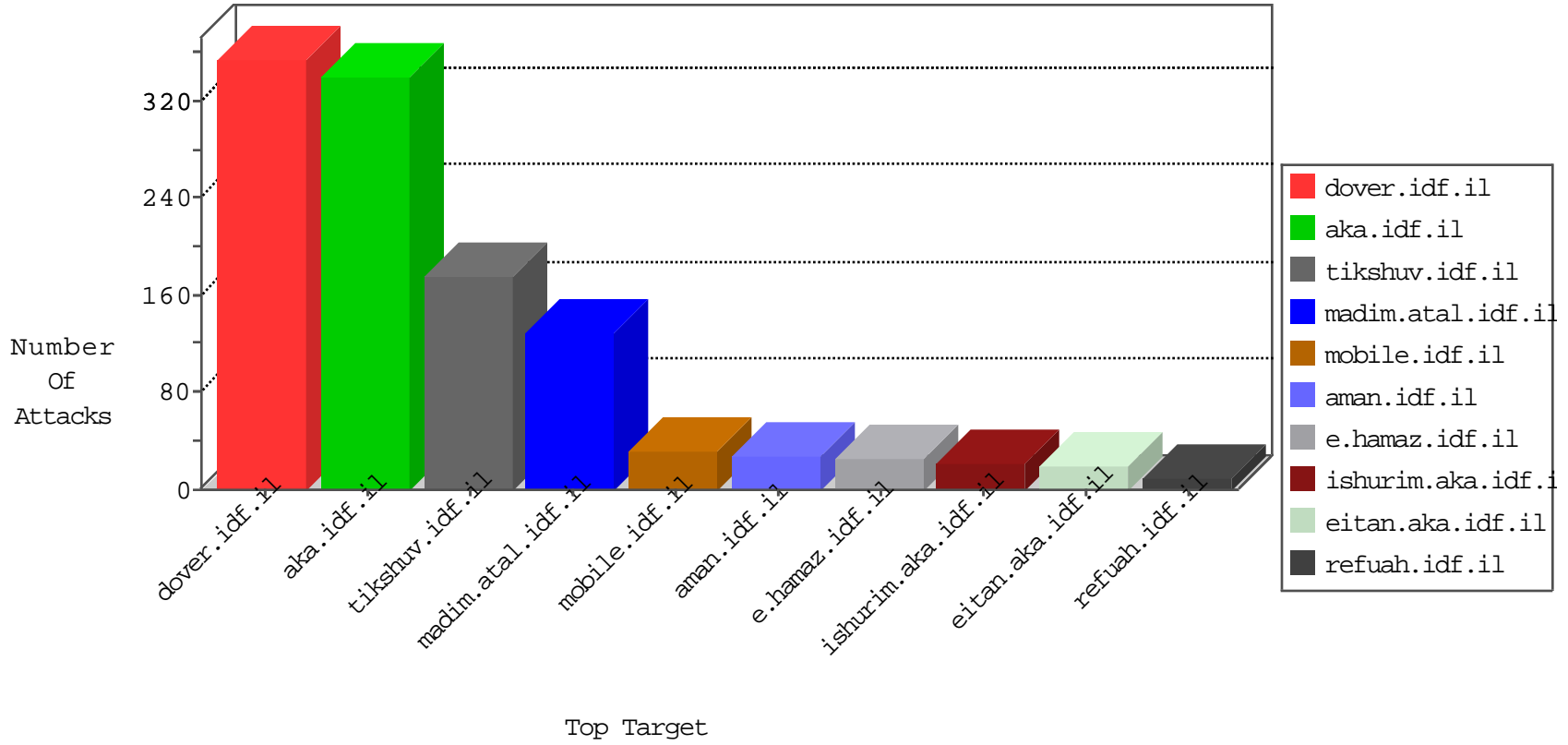


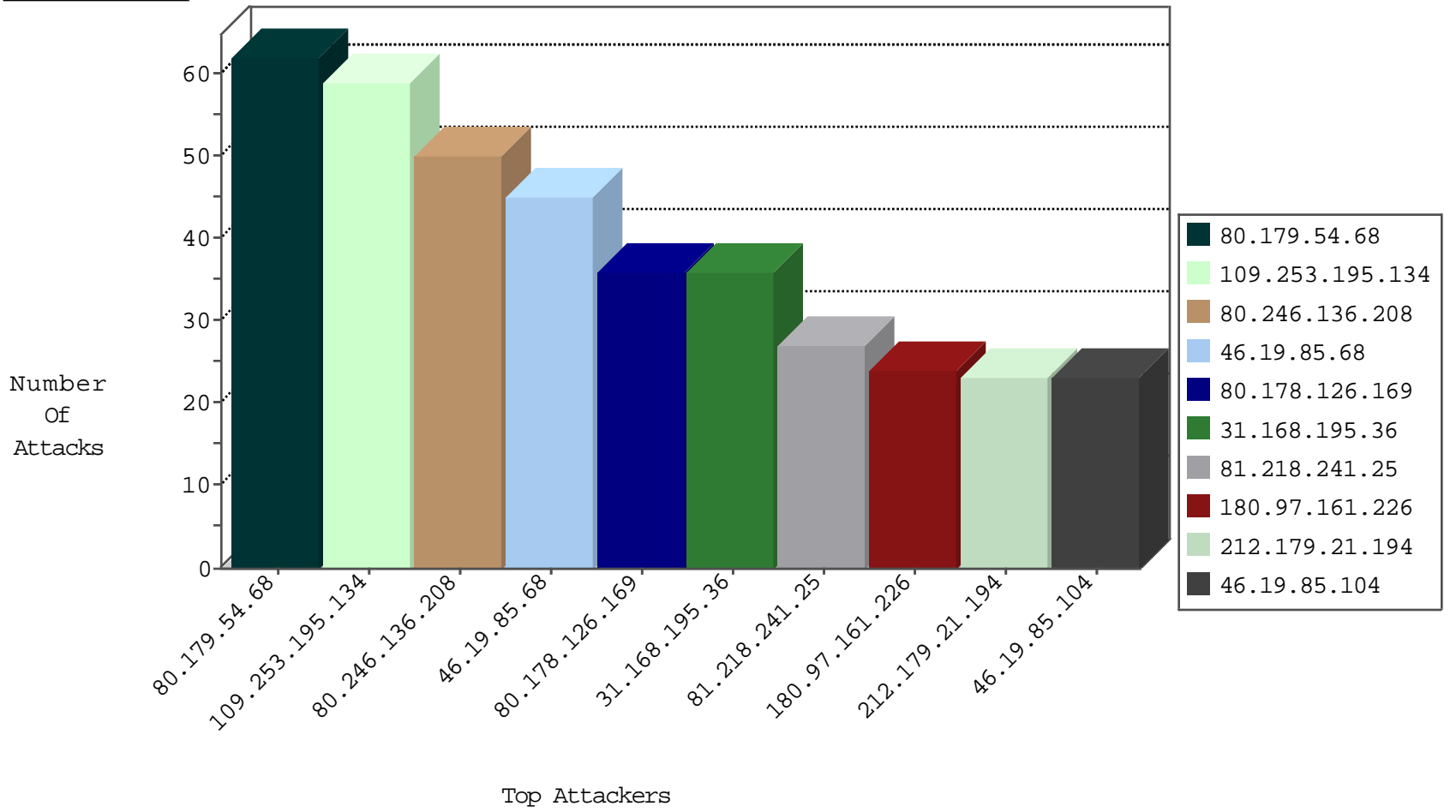
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	171
180.97.161.226	China	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	24
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	2
188.138.17.205	France	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.132	Netherlands	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.132	Netherlands	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
108.186.168.25	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
134.147.203.115	Germany	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.96.17	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.26.149.144	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.27.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.118	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.248.207.236	Jordan	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	3
82.193.127.15	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
2.52.169.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.198.186	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.5.87	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.181.63.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.161.0.57	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.178.239.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.153.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.72.135.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.135.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.186.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.126.209.216	147.237.77.216	Lebanon	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.114.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.234.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.29.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.75.214.5	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
212.179.244.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.215.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.171.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
132.68.146.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.98.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.70.86.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.116.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.178.126.169	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
31.168.195.36	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
80.179.54.68	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	31
80.179.54.68	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
46.19.85.68	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
46.19.85.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.149.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.122.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.53	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
110.171.182.73	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
158.58.172.238	Italy	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
158.58.172.238	Italy	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
176.13.15.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.165.179	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	7
46.19.85.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.165.179	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
93.172.153.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.132.100	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.163.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.240.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
212.179.21.194	Israel	147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.168	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.114.91.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.45.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.29.86.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.228.224.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.168.153.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.195.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
80.246.136.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
2.54.170.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
176.13.20.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.139.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
46.121.195.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.167.61	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.61	Block	3
118.173.164.100	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.111.108.69	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 84.111.108.69 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
79.176.203.173	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
93.173.98.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
212.179.21.194	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.89.217.231		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	2
37.26.147.205	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.108.69	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 84.111.108.69	Block	1
213.57.240.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.169.177	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.230.93.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
185.89.217.233		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.69.158.111	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
84.111.108.69	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.111.108.69	Block	1
46.19.85.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
156.196.25.62		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.26.146.143	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.186.56.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct113 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.111.108.69	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
87.71.6.125	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
72.9.148.10	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/kapatz/	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	1
87.69.158.111	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
37.26.148.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.70.66.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.108.69	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 84.111.108.69	Block	1
80.246.136.249	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
216.75.214.5	Europe	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.230.93.127	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.69.158.111	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.69.163	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
192.118.11.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12847-he/dover.aspx "• i ½	Block	1