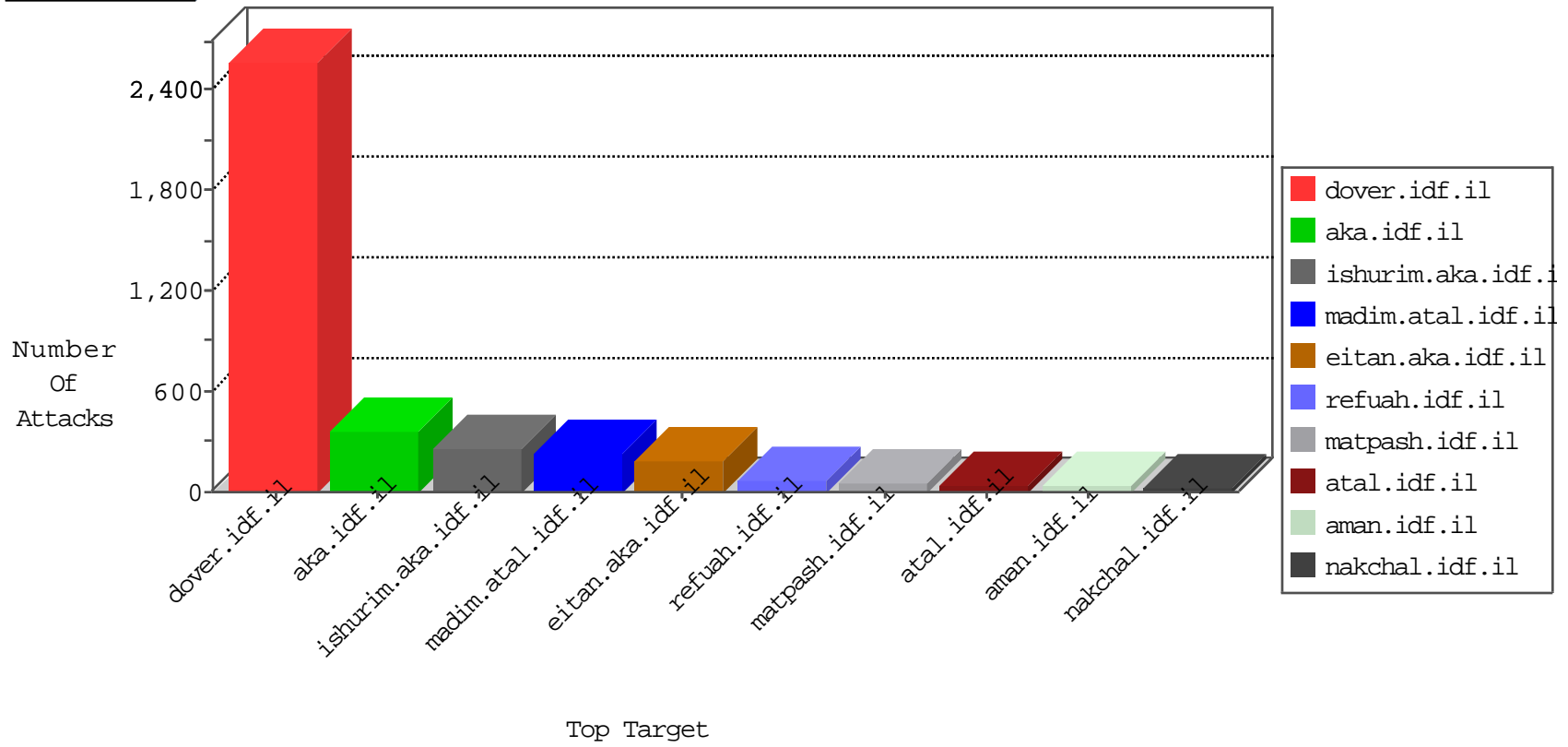


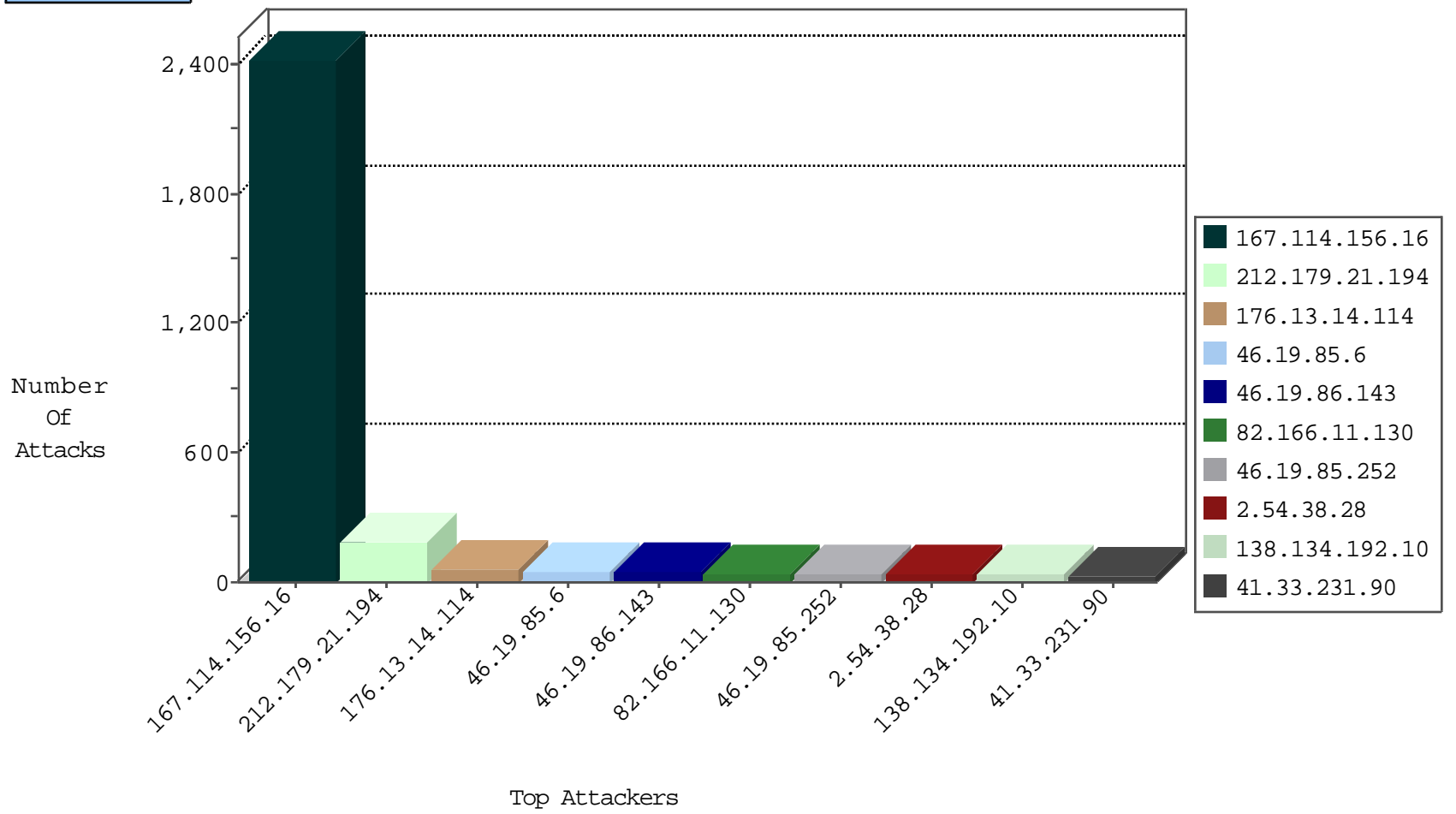
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3295
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
77.220.187.194	Russian Federation	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
118.193.23.46	China	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.45	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
208.69.30.69	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.59.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.22.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.116.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.176.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.200.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.55.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.79	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
40.115.58.160	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
218.38.12.218	147.237.76.177	Korea, Republic of	noore.idf.il	ET SCAN Potential SSH Scan	1
31.151.229.115	147.237.72.166	Netherlands	aka.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
2.52.56.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
119.73.228.130	147.237.0.33	Singapore	idf.il	ET SCAN NMAP -sS window 1024	1
109.65.103.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.8.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.37.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.252	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
176.12.150.129	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
185.120.126.77		147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
84.94.205.213	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	18
46.19.86.90	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
79.183.107.222	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
62.219.35.63	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.81.26.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.139	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
173.252.115.86	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.241.226.39	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	10
138.134.192.10	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
86.86.147.212	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
173.252.115.88	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
79.182.171.62	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
84.94.205.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
31.154.7.4	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	7
2.52.22.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.252	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.60.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.235.53.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.111.137.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.30.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.170.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.16.242	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.168.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.170.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.134	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
149.78.2.63	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.219	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.28.155.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.52.55.178	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.16.242	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
138.134.192.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.168.195.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.55.178	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.148.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence		monitor	4
31.168.195.70	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
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
176.13.14.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
82.166.11.130	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
2.54.38.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.12.150.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
138.134.192.10	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
147.235.8.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.52.54.21	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
194.90.240.37	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
212.235.98.139	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
5.28.165.135	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
46.19.86.36	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
77.126.61.19	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
80.246.137.215	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
77.125.7.21	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
84.109.126.202	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
46.19.86.78	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
40.77.167.98	United States	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
2.52.56.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.10.254	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
46.99.63.102	Albania	147.237.77.74	law.idf.il	PHP Attempt	Block	2
176.13.13.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
40.77.167.65	United States	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
176.13.14.114	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.14.114	Block	2
212.29.253.113	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1
46.19.86.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.107.26	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
109.64.25.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.101.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.90.239.2	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
93.172.7.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.6.53.179	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
176.13.10.254	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	1
46.121.64.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.112	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opmissingperson/opmissingperson.aspx	Block	1
82.166.11.130	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in All Sources from 82.166.11.130	Block	1
213.8.174.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.56.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
79.177.198.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
178.154.243.96	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
31.168.195.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1