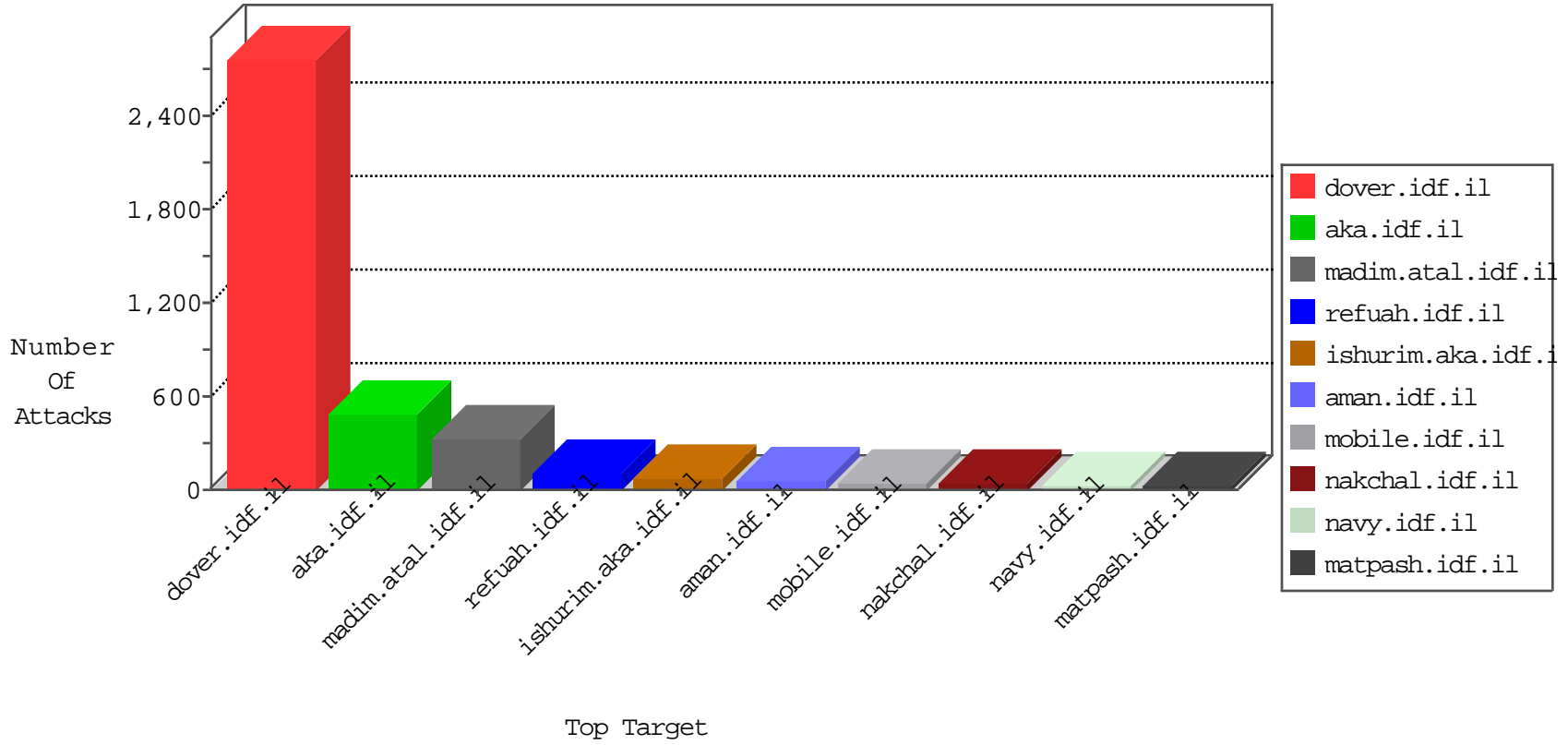


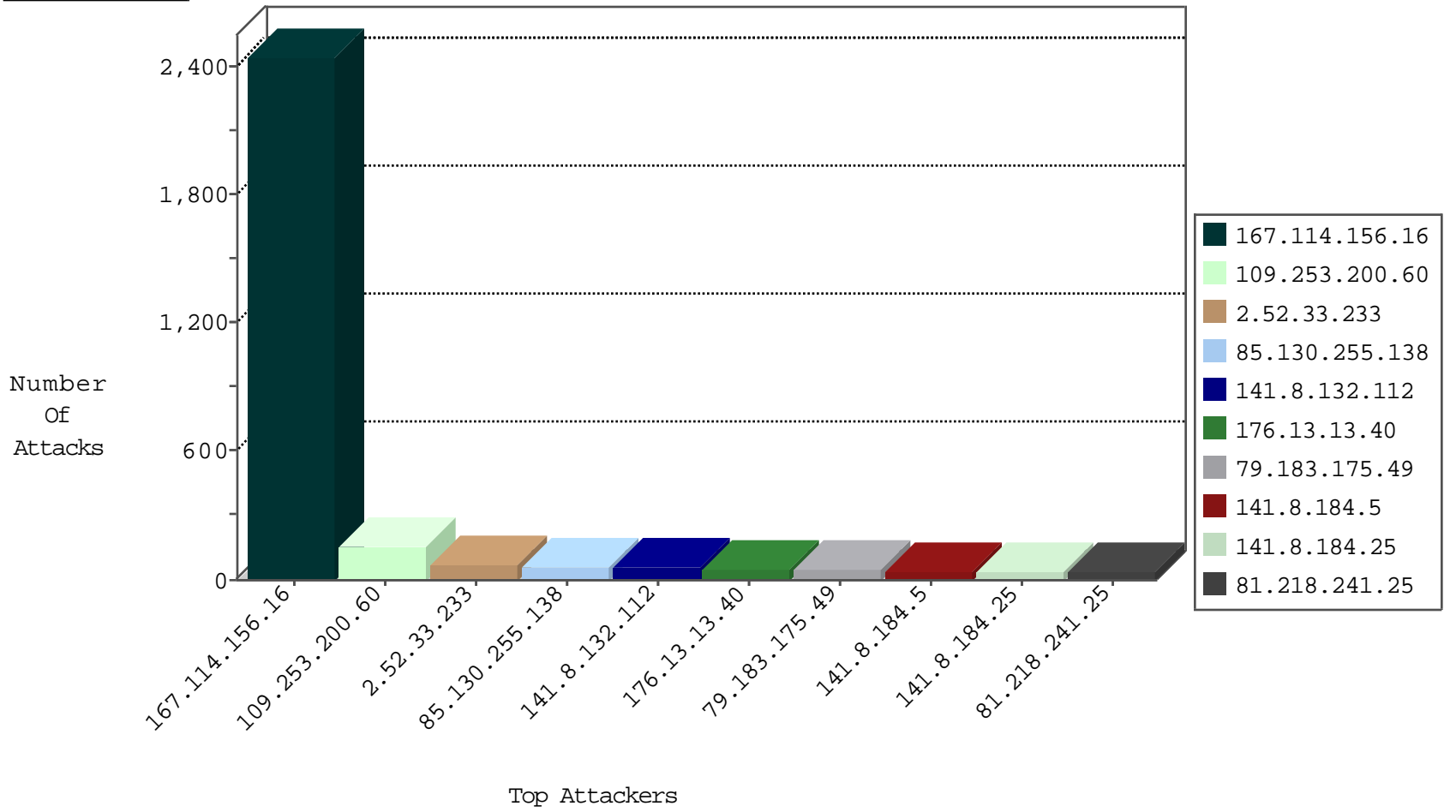
IDF Under Attack Daily Report



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	3137
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
79.178.99.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
213.8.204.81	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.52.58.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.54.29.111	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
185.130.5.224		147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.169	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
191.232.39.241	United States	147.237.72.166	aka.idf.i	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
200.98.137.169	Brazil	147.237.72.166	aka.idf.i	C041: HTTP: Access to - index.php?option=com_jce	Block	1

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	1
190.215.47.162	147.237.76.200	Chile	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
176.13.9.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.180.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.19.86.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.110.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
190.215.47.162	147.237.76.200	Chile	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
185.89.217.230	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.127.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.88.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.2	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.155	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
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
85.130.255.138	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
79.183.175.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
2.52.33.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
2.52.33.233	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.85.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.32.179.228	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.0.200.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.253.150.183	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.34.81	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
132.64.25.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.33.115	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.52.32.155	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.39.255	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.211	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
217.194.203.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.52.33.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.52.33.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
85.130.255.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.33.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.34.81	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.241.38.42	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.32.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.34.81	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.32.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.82	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.34.81	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
62.0.201.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
2.52.32.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.54.11.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
157.55.39.10	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.13.40	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
37.26.147.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
41.241.38.42	Sudan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.130.255.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.8.204.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.135.214	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.8.204.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
157.55.39.114	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.200.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
109.253.200.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	49
176.13.13.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
77.125.133.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
176.13.18.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.193.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
2.54.152.94	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	11
109.253.192.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
109.253.192.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	7
109.253.159.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.117.192.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	6
2.54.148.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.33.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.201.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.129.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.50.87.26	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.29.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.86.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
2.54.155.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.132.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
24.182.60.134	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.146.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.201.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/109210.pdf	Block	1
95.86.124.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.25.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.118.236.27	Bulgaria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
149.88.106.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.53	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
37.187.43.27	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.253.197.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
2.54.160.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.163.234.9	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Unknown Parameter on www.aka.idf.il/main/giyus/general.aspx parameter docI..	None	1
192.117.103.139	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.1.60	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
85.65.19.97	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.210.171.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.221.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.235.110.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.48.103	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1