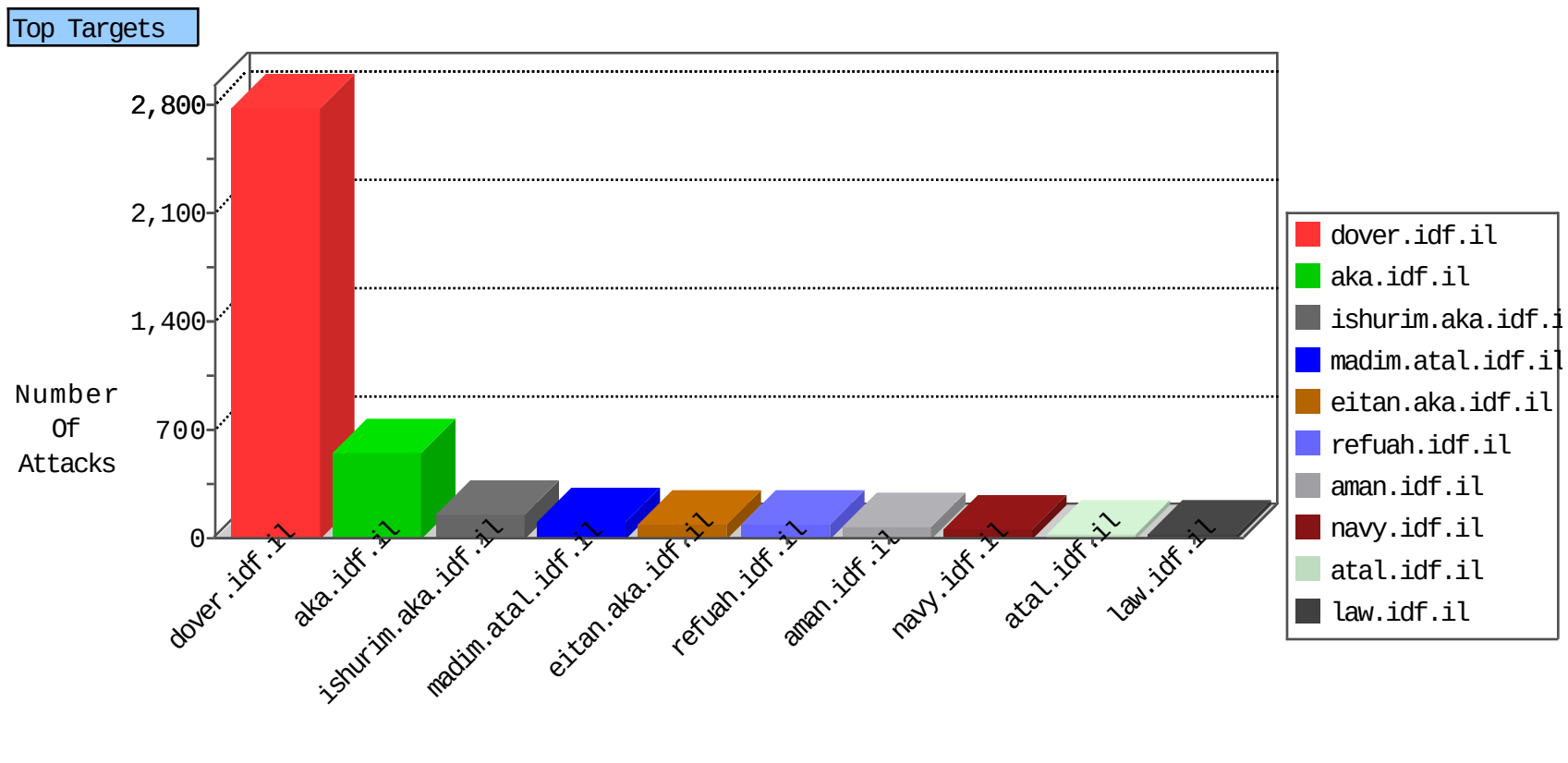
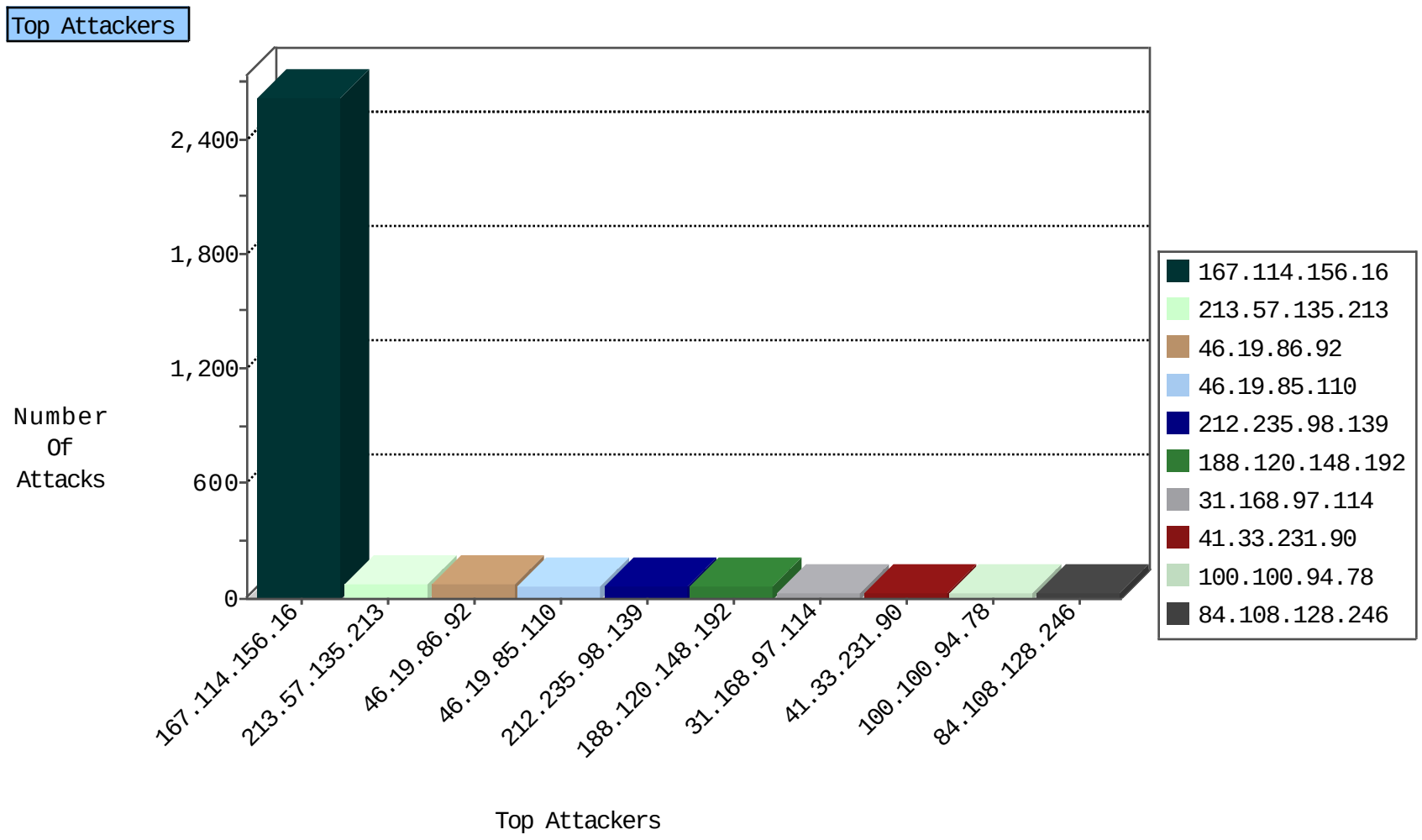
12-02-2015-15:04:00 to 12-02-2015-16:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-02-2015-15:04:00 to 12-02-2015-16:04:00

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	3478

12-02-2015-15:04:00 to 12-02-2015-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-02-2015-15:04:00 to 12-02-2015-16:04:00

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	2
95.86.92.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.178.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
218.24.113.2	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.46	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
91.218.246.103	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.139.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.205.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.46	147.237.76.201		e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.106.94.46	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1

12-02-2015-15:04:00 to 12-02-2015-16:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.110	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	66
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	65
46.19.86.92	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	46
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
31.168.97.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
100.100.90.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
213.57.135.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
213.57.135.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
84.108.128.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
79.179.20.85	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
62.219.130.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
84.143.137.176	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
46.19.85.133	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
100.100.94.78		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
213.57.135.213	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
213.57.135.213	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
100.100.94.78		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.78.18		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.92	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
100.100.47.166		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.121.24.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.4.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
199.203.196.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
94.230.86.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
149.88.158.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.12.144.30	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.52.155.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
176.12.140.236	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.223	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.92	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.95.211.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
188.120.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.168.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.62.61		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.58.171	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.92	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.166.116.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.58.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.166.86.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
196.217.162.80	Morocco	147.237.77.216	dover.idf.il	drop		drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.120.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
2.54.173.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
176.13.16.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	4
46.19.85.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
131.253.25.150	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/i/jot	Block	3
109.64.115.168	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.64.115.168	Block	3
79.176.72.166	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.54.186.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
197.37.49.160	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
197.37.49.160	Egypt	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 197.37.49.160	Block	3
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.111.122.71	Block	2
46.19.85.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.136.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.127.196.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 84.111.122.71	Block	2
132.68.80.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 84.111.122.71	Block	2
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 84.111.122.71	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
41.253.224.117	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
79.179.218.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 84.111.122.71	Block	2
31.154.92.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.32.71.18	Moldova, Republic of	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/homepage/	Block	2
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 84.111.122.71	Block	2
46.121.92.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.175.111.105	Bosnia and Herzegovina	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
2.54.171.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 84.111.122.71	Block	1
207.46.13.103	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rorapi/country	Block	1
2.52.31.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.122.71	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
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	1
89.138.177.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.126.147.218	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
31.168.97.114	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
5.28.156.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
211.181.236.140	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3058.jpg	Block	1
157.55.39.46	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.86.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.56.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_medium in www.aka.idf.il/main/home/default.aspx	None	1
2.54.45.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1