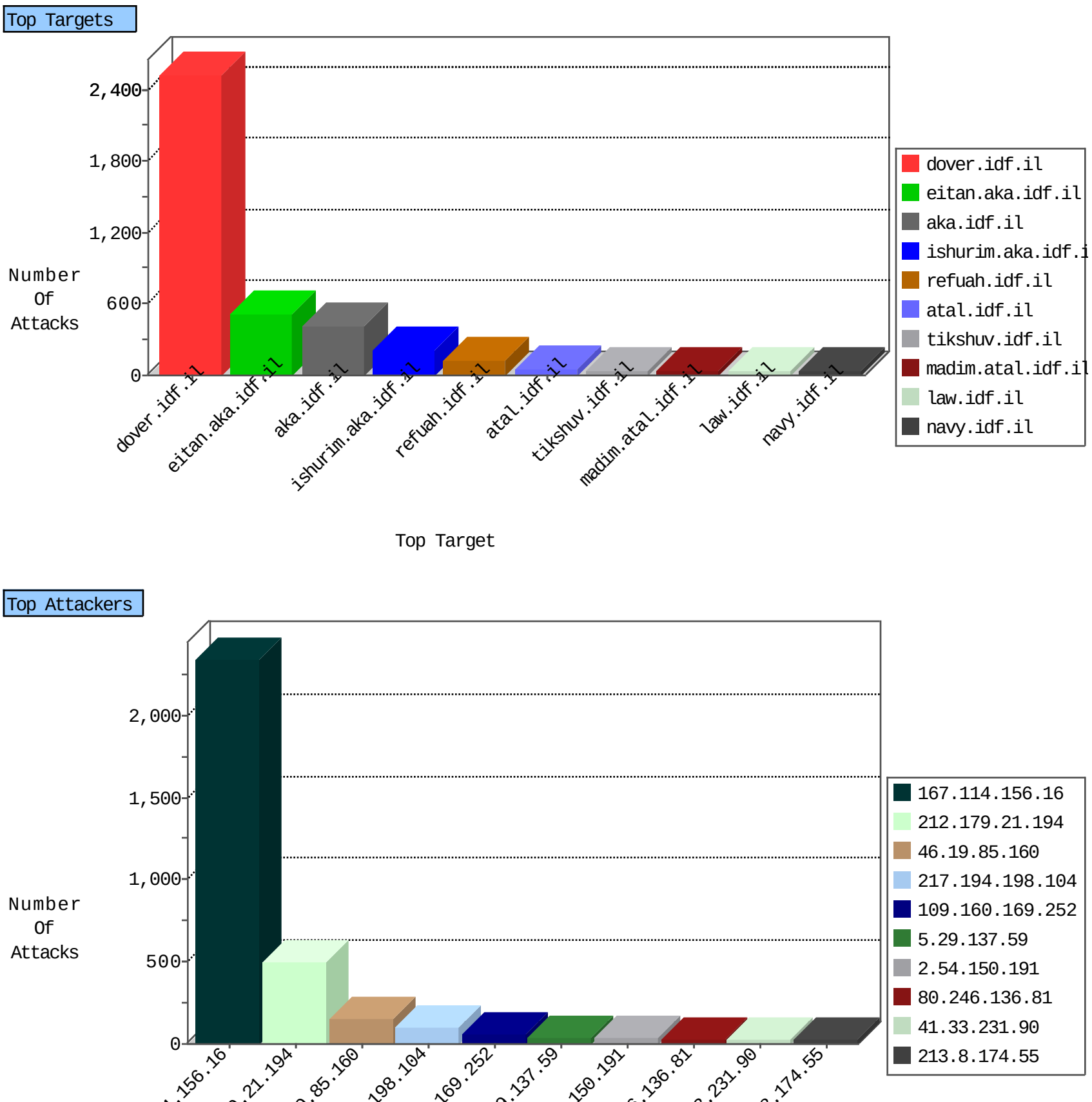
12-07-2015-10:04:00 to 12-07-2015-11:04:00

IDF Under Attack Daily Report



12-07-2015-10:04:00 to 12-07-2015-11:04:00

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	3319
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
194.90.151.18	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
37.26.149.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
167.88.7.237	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
167.88.7.251	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.239	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
167.88.7.233	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.241	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
185.35.62.249	Switzerland	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
167.88.7.237	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
167.88.7.246	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1

12-07-2015-10:04:00 to 12-07-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
69.12.70.34	United States	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
69.12.70.34	United States	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

12-07-2015-10:04:00 to 12-07-2015-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.126.116.147	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
96.94.72.226	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 2048	1
79.176.184.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.87.118.63	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
31.172.234.8	147.237.72.14	France	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
212.179.21.194	147.237.72.166	Israel	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
109.64.59.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
96.94.72.226	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -f -sS	1
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
31.172.234.8	147.237.77.61	France	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

12-07-2015-10:04:00 to 12-07-2015-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.160	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	151
217.194.198.104	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	100
109.160.169.252	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
40.77.167.33	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	21
109.160.169.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
37.26.149.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.160.169.252	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
80.246.133.30	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.30.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.29.137.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
213.57.143.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
195.200.205.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
80.246.136.81	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	10
46.19.86.246	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.246	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.29.137.59	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.150.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
84.108.25.127	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
213.8.174.55	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.150.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.150.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
138.134.102.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.150.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.116.130.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
213.8.174.55	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
46.121.157.214	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
46.19.85.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.136.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
213.8.174.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
217.194.195.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.137.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.162.134	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.174.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.116.241.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.137.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.131	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
2.54.150.191	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	6
5.29.137.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.150.191	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	6
5.29.137.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.194.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.161.150.6	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.35	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.136.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.6.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

12-07-2015-10:04:00 to 12-07-2015-11:04:00

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	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	485
176.12.150.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.18.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
213.8.204.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.204.41	Block	5
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
46.117.134.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.49.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.98.191	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
176.13.12.111	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
213.8.204.41	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	2
46.116.203.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.10.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.204.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	2
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
31.168.174.198	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	2
173.252.90.229	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.127.25.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
217.194.198.104	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/926-he/refuah.aspx	Block	2
2.52.44.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.95.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.132	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
80.246.139.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.13.110.116	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.89	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.9.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl60.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
69.171.230.100	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.22.134.97	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
109.253.34.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.226.90	France	147.237.72.166	aka.idf.il	Illegal HTTP Version HTTP/	Block	1
84.108.185.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
80.246.136.89	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.149.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.114.116	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.126.235.71	Macedonia, the Former Yugoslav Republic of	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
213.8.204.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.149.215.236	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
173.252.88.187	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.15.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.220.158.106	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.155	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/	Block	1
80.246.139.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.11.194	Israel	147.237.77.74	law.idf.il	Parameter Type Violation prefixText in www.law.idf.il/webservices/wscity.asmx/getcities	Block	1
173.252.90.90	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
69.171.230.105	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-07-2015-10:04:00 to 12-07-2015-11:04:00