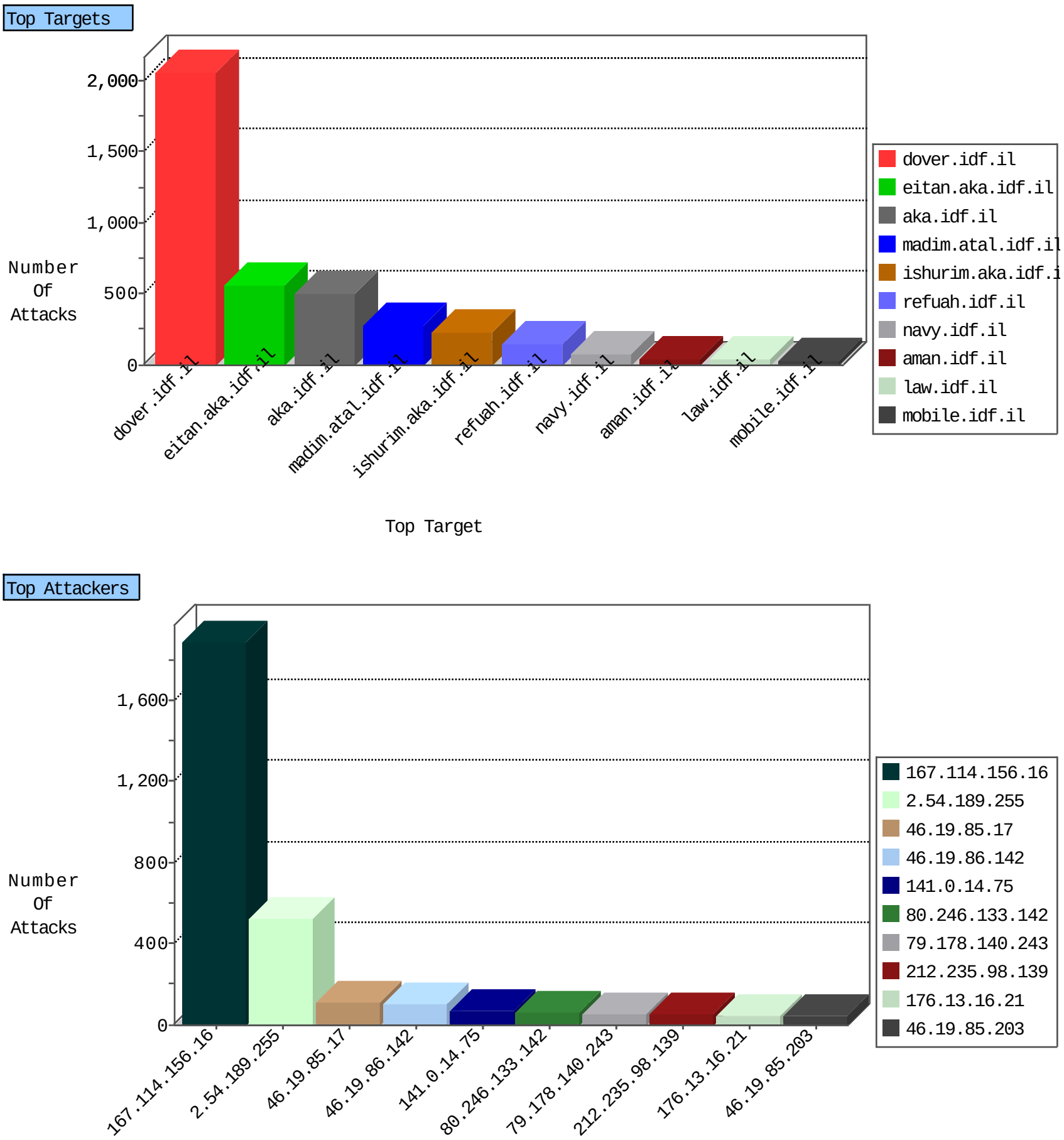
12-14-2015-11:04:04 to 12-14-2015-12:04:04

IDF Under Attack
Daily Report



12-14-2015-11:04:04 to 12-14-2015-12:04:04

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	3465
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
141.0.14.75	Europe	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
79.179.6.184	Israel	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	2
66.240.236.119	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
141.0.14.75	Europe	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1

12-14-2015-11:04:04 to 12-14-2015-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.131.59	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	7
64.251.25.176	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
94.102.153.58	United Kingdom	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-14-2015-11:04:04 to 12-14-2015-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.153.58	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	4
64.251.25.176	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
46.19.85.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.138.233.215	147.237.77.216	Greece	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.222.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.37.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.83.135.131	147.237.8.46	Georgia	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
79.177.13.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.226.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.100.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
60.4.60.20	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.47.52.157	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 2048	1
58.253.96.122	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
109.186.39.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.102.171.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.83.135.131	147.237.8.50	Georgia	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.8.24	Georgia	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.108.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.64.214.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
115.47.52.157	147.237.72.217	China	e.idf.il	ET SCAN NMAP -f -sS	1
46.120.28.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.111.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-14-2015-11:04:04 to 12-14-2015-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.189.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	474
46.19.85.17	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	108
141.0.14.75	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	68
80.246.133.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	52
46.19.85.203	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.143.44.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	24
109.186.64.119	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	18
2.54.24.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.177.211.100	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.80.59.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.9.118	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
192.114.3.241	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	11
212.235.52.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.145.1	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.80	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
80.246.133.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
109.67.111.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.22.134.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.52.146.24	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.29.47.189	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.107	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.102.9.10	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.52.146.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.26.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
2.54.30.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.27.116	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.35.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.98.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.223.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.143.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.162.103	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.9.35	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	5
109.64.25.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.37	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
149.88.25.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.55.253	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	4
2.52.176.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
146.185.56.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.54.35.228	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.181.32.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.8.204.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

12-14-2015-11:04:04 to 12-14-2015-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
79.178.140.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.54.189.255	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.189.255	Block	49
176.13.16.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
37.26.148.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
203.86.236.20	Hong Kong	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 203.86.236.20	Block	13
77.126.85.101	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.85.101	Block	9
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.26.149.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.20.67	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	6
176.12.148.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.168.1.202	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.168.1.202	Block	4
203.86.236.20	Hong Kong	147.237.77.74	law.idf.il	PHP Attempt	Block	4
212.199.107.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
2.52.169.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/1088-he/meretz.aspx	Block	3
203.86.236.20	Hong Kong	147.237.77.74	law.idf.il	Multiple CVE-2008-7212: Mambo 4.6.3 Path Disclosure Vulnerability(+) from 203.86.236.20	Block	3
213.8.204.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/fachar	Block	3
212.235.13.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
84.108.37.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.24.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.9.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
212.199.224.24	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
2.54.189.255	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	2
2.54.24.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.64.25.67	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
84.108.70.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
203.86.236.20	Hong Kong	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/fckeditor/editor/filemanager/connectors/asp/connector.asp	Block	1
46.19.86.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.54.167	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.136.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.144.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
85.64.150.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.24.145	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.i	Multiple Malformed URL from 84.228.101.57	Block	1
79.177.22.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.5.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.64.119	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.i	Illegal Byte Code Character in Header Name [[#7]][[#14]]MÂ£Ã?Â, }dÃ§Â¯d[[#31]]4Â”Ã”=Ã¾wÃ¤Â³[[#28]]Ã¹[[#12]]ÂŒÂ‰_Ã¥b6%EÂ€ =[[#17]]Ã¥T[[#20]]Â?oÂ¯ ÃœXÃˆBÂ?Ãœ[[#29]][[#18]]Â´[[#30]]Â’Â²{Ã¤Â?	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
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
37.142.64.92	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/6_s3_	Block	1
82.80.59.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
203.86.236.20	Hong Kong	147.237.77.74	law.idf.il	CVE-2008-7212: Mambo 4.6.3 Path Disclosure Vulnerability	Block	1

12-14-2015-11:04:04 to 12-14-2015-12:04:04