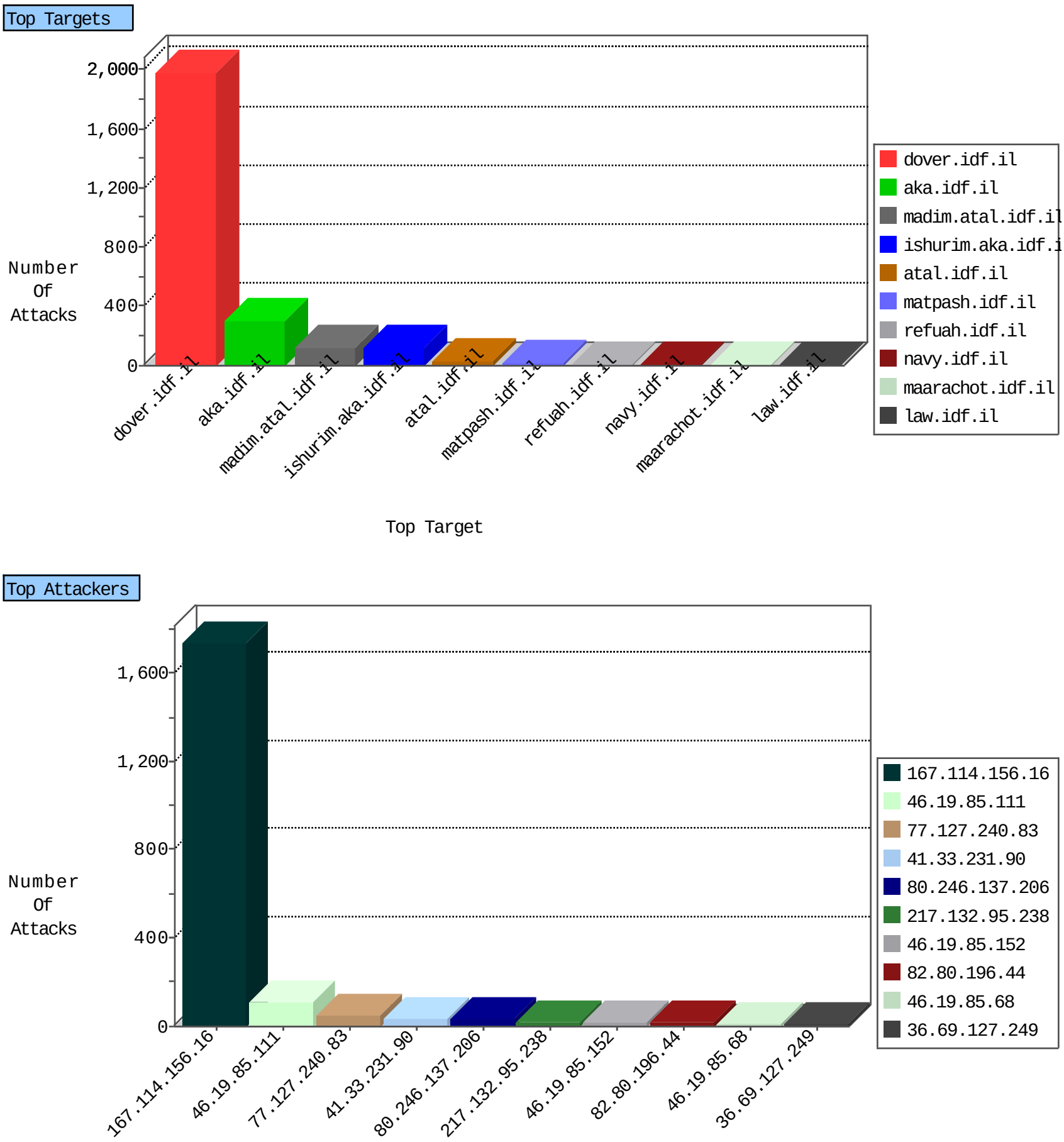
12-24-2015-12:04:02 to 12-24-2015-13:04:02

IDF Under Attack
Daily Report



12-24-2015-12:04:02 to 12-24-2015-13:04:02

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	3559
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	838
62.219.165.105	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

12-24-2015-12:04:02 to 12-24-2015-13:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.69.127.249	Indonesia	147.237.72.166	aka.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
36.69.127.249	Indonesia	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-24-2015-12:04:02 to 12-24-2015-13:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
36.69.127.249	147.237.72.166	Indonesia	aka.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	4
36.69.127.249	147.237.77.216	Indonesia	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	3
36.69.127.249	147.237.77.74	Indonesia	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	3
93.174.93.181	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
31.168.238.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.181	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.139.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.124.48.157	147.237.8.14	Japan	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
81.218.200.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.208	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.116.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.40	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.5.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.245.183.201	147.237.76.176	Japan	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
147.27.11.143	147.237.72.14	Greece	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
135.23.221.218	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.181	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
36.69.127.249	147.237.0.34	Indonesia	tikshuv.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	1
93.174.93.181	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
5.102.254.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.104.49.211	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
84.228.46.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.23.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.33.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.208	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.214.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.16.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
43.245.183.201	147.237.76.176	Japan	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.27.11.143	147.237.72.14	Greece	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
36.69.127.249	147.237.77.170	Indonesia	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	1
132.65.249.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-24-2015-12:04:02 to 12-24-2015-13:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.111	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	111
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
62.219.235.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.166.57.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.43.96.159	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.222	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
58.9.189.201	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.146.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.21	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.17.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.214.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.11.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.116.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.172.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.223.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.219.231.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.114.163.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.189.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.78	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.66.25.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.174.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.24.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.245.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.31.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.214.162	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.39.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.113.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

12-24-2015-12:04:02 to 12-24-2015-13:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.240.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
80.246.137.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
217.132.95.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
185.32.179.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
62.0.34.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.0.34.177	Block	7
80.246.138.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
149.78.197.227	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
109.253.198.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.150.215.254	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/113267.pdf	Block	3
2.54.33.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.5.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.181.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.142.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.173.157.38	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.179.150.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.254.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.58.178.56	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
93.173.244.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.166.186.224	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.118.78.57	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.143.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.144.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
79.177.201.43	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/938-he/refuah.aspx	Block	1
109.160.198.231	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	1
176.13.23.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.7.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
79.182.121.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
23.235.221.158	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
175.143.14.129	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
114.98.230.247	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/896-ar/idfg.aspx/trackback/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
193.34.56.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.10.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.151.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.129	United States	147.237.76.31	nakchal.idf.il	Multiple Malformed URL from 141.212.122.129	Block	1
79.177.201.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.73.146	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20422-he/idfgdover.aspx	Block	1
212.179.218.166	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
109.160.198.231	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/style/1.he/	Block	1
85.65.230.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.146.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.130.188	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
23.235.221.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1

12-24-2015-12:04:02 to 12-24-2015-13:04:02