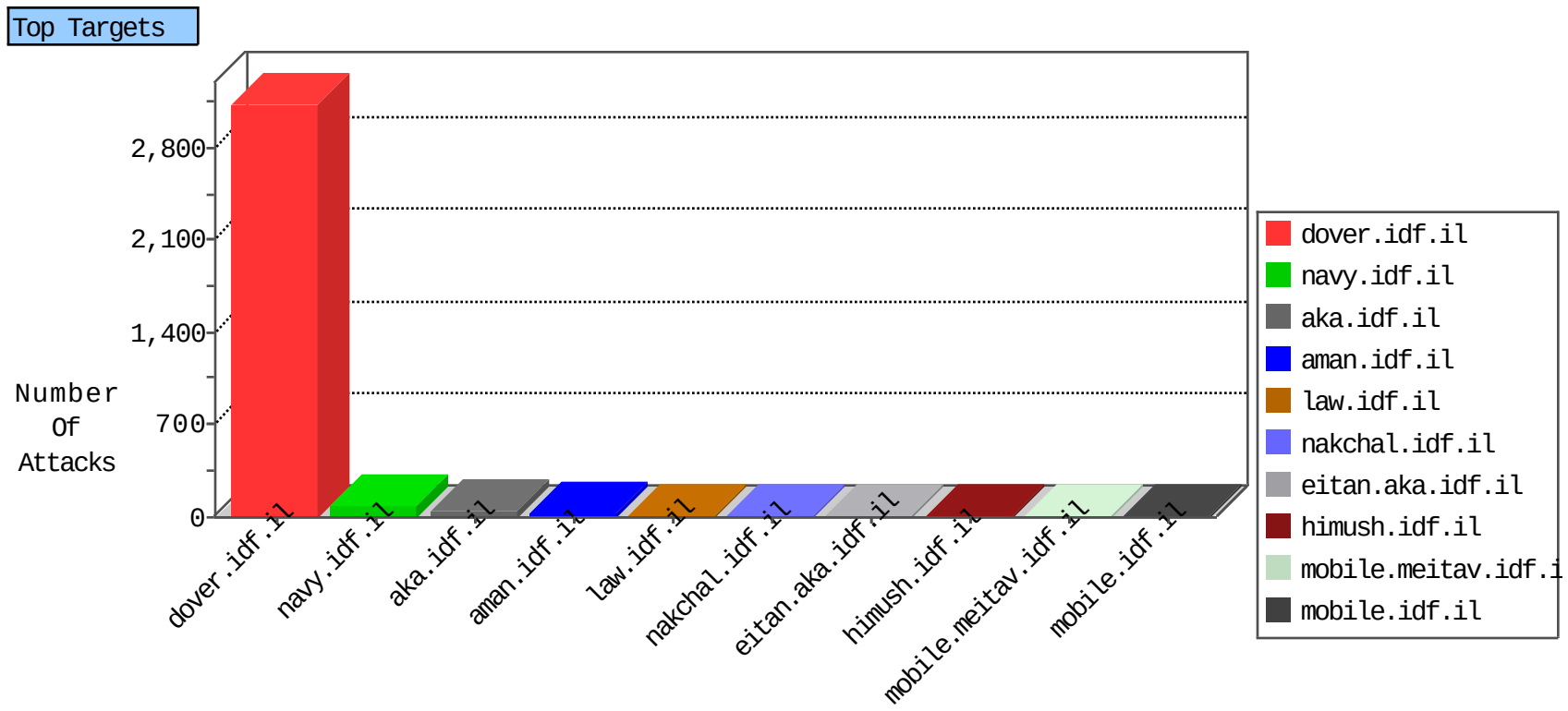
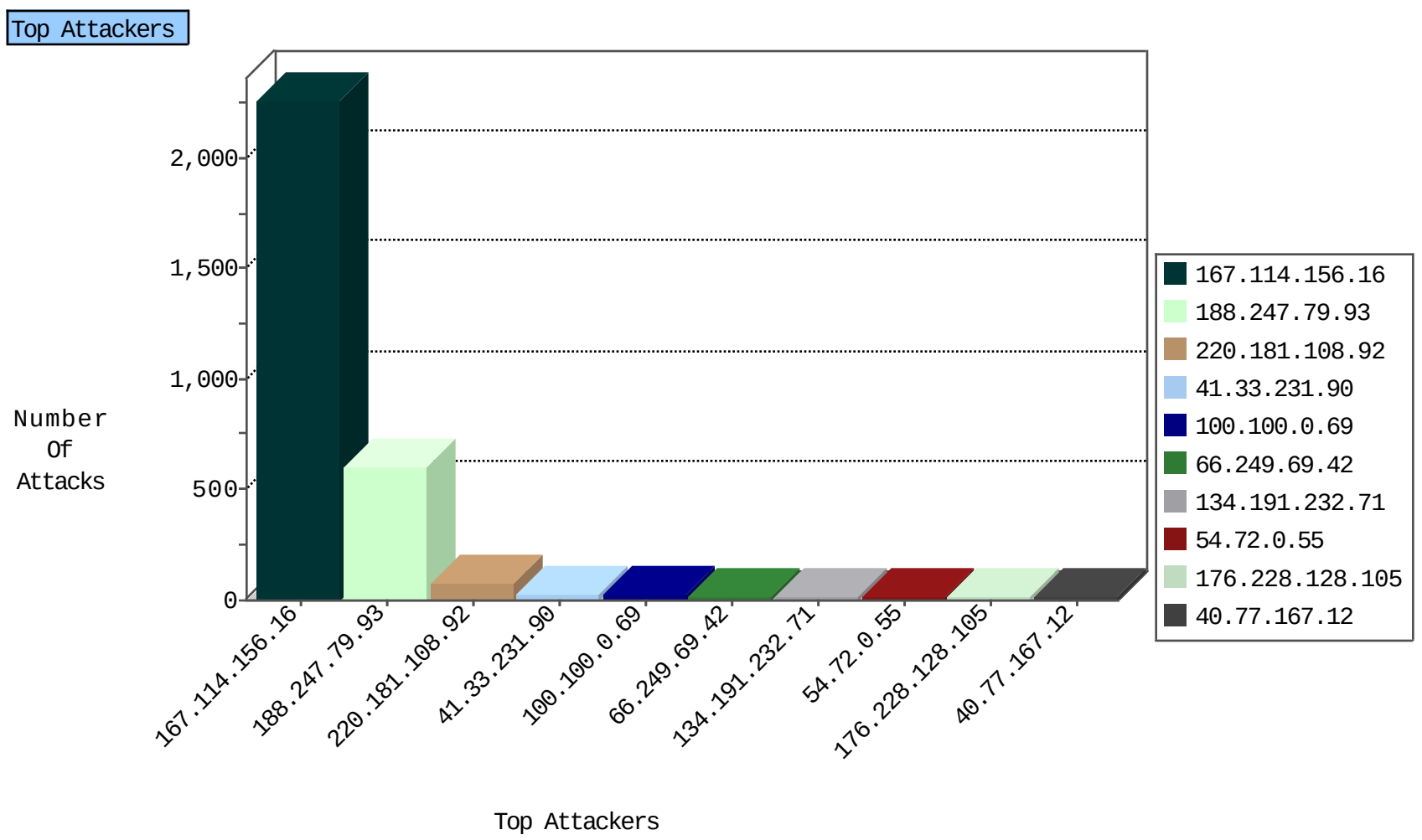
11-30-2015-03:04:03 to 11-30-2015-04:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-30-2015-03:04:03 to 11-30-2015-04:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.108.92	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	412225
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3368
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	109
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	3
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	2
195.154.211.30	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
159.148.186.196	Latvia	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
180.0.152.192	Japan	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.51.30	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
159.148.186.196	Latvia	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.150.230	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

11-30-2015-03:04:03 to 11-30-2015-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.191.177	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.194.47	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.211.30	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.120	Italy	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-30-2015-03:04:03 to 11-30-2015-04:04:03

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	4
195.154.194.47	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
195.154.191.177	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
169.54.91.220	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
115.194.20.11	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.112.79.250	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
114.112.79.250	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
195.154.211.30	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	1
80.82.70.230	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
64.166.50.150	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.106.94.16	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
169.54.91.220	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.91.220	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
114.112.79.250	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
114.112.79.250	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
114.112.79.250	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
195.154.194.47	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	1
75.82.48.43	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.151.55.35	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.16	147.237.77.19		law-forum.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.16	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1

11-30-2015-03:04:03 to 11-30-2015-04:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	210
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	112
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	99
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	drop		drop	76
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.228.128.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
40.77.167.12	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.54.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.3.125	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
177.85.102.169	Brazil	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
23.235.221.158	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
85.214.147.14	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
213.57.128.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
40.77.167.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
65.55.210.146	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
40.77.167.14	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.67.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.64	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
177.85.102.169	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.195	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.110	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.138.1.218	Germany	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.107	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.196	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.120	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.228.188.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.89	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

11-30-2015-03:04:03 to 11-30-2015-04:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.32.230.183	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
124.217.229.60	Malaysia	147.237.77.74	law.idf.il	PHP Attempt	Block	3
175.107.146.153	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
104.152.108.121	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
95.142.159.11	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
162.254.250.31	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
192.163.195.188	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
162.247.78.111	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
162.144.209.193	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
54.206.58.76	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
71.46.208.79	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
149.210.131.9	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
162.144.209.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
54.206.58.76	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
37.142.68.59	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	2
95.86.102.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
71.46.208.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
149.210.131.9	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
104.152.108.121	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
46.32.230.183	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
124.217.229.60	Malaysia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2
175.107.146.153	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
162.254.250.31	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
95.142.159.11	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
162.247.78.111	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
162.144.209.193	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
104.152.108.121	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
54.206.58.76	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
71.46.208.79	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
149.210.131.9	Netherlands	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
95.142.159.11	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
46.32.230.183	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
162.254.250.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
192.163.195.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	2
175.107.146.153	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
37.142.68.59	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	2
162.247.78.111	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/index.php	Block	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
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.94.29.40		147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
95.142.159.11	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-admin/admin-ajax.php	Block	1
162.254.250.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-admin/admin-ajax.php	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1236-he/refuah.aspx	Block	1
192.163.195.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-admin/admin-ajax.php	Block	1
107.158.100.141	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
162.247.78.111	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-admin/admin-ajax.php	Block	1

11-30-2015-03:04:03 to 11-30-2015-04:04:03