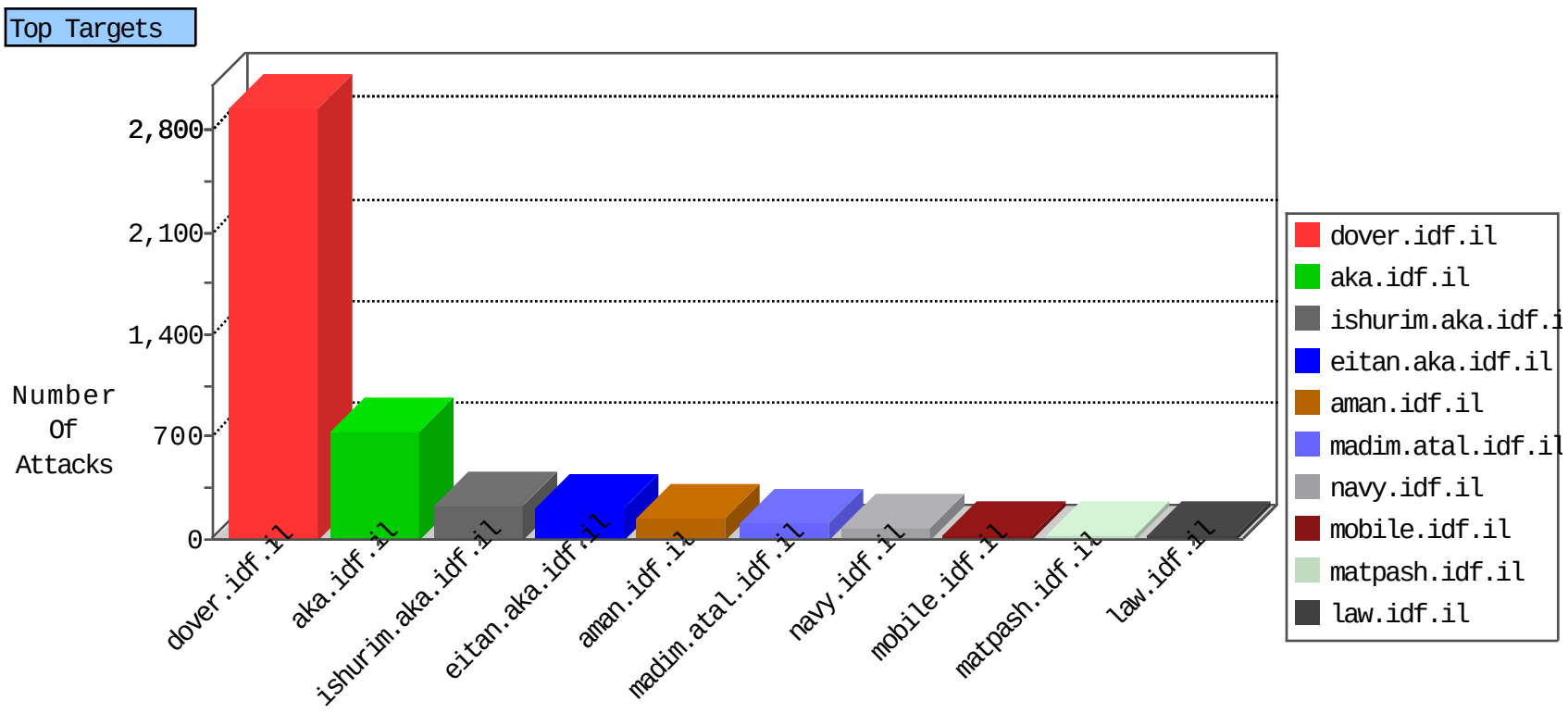
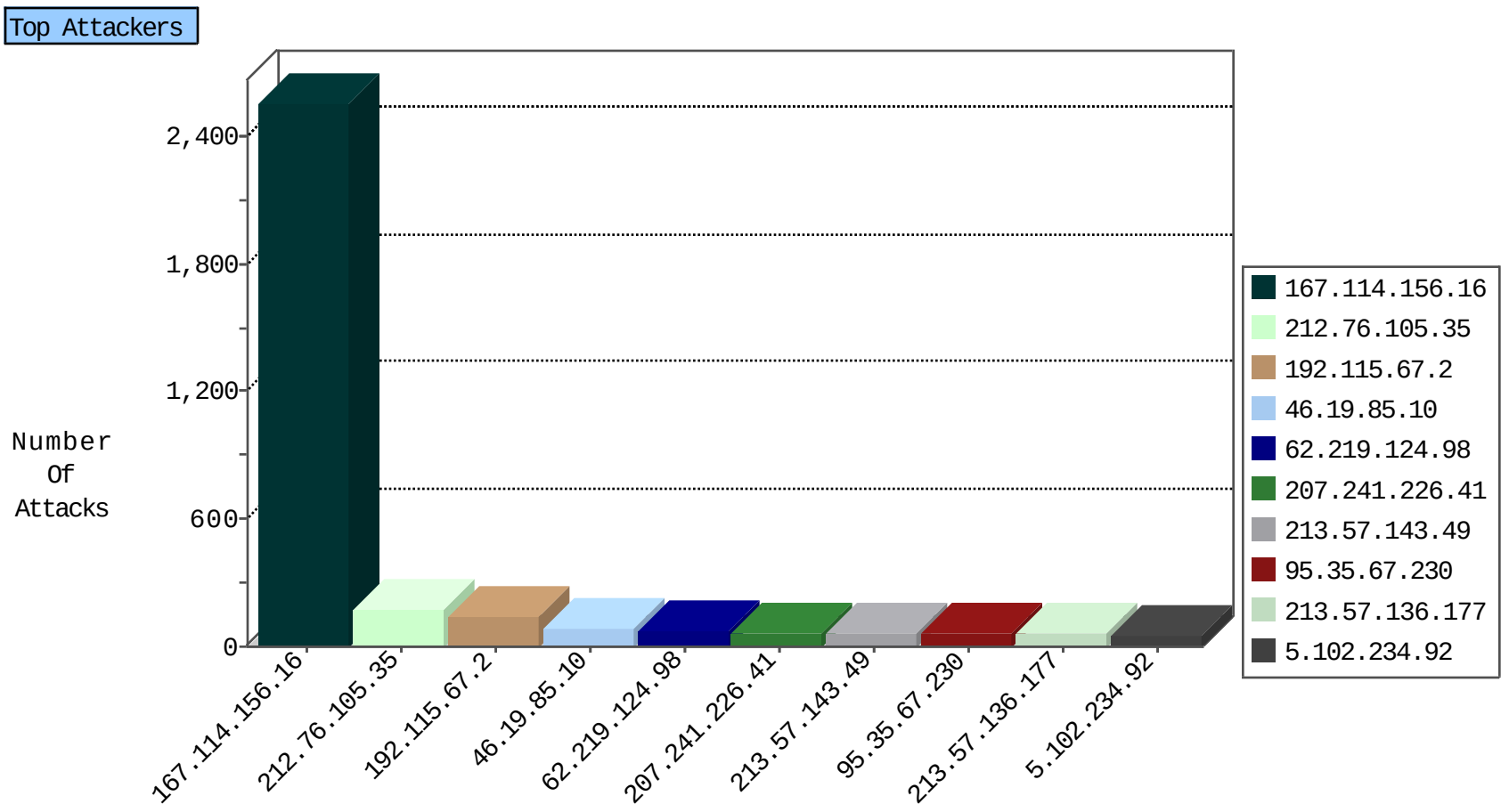
11-30-2015-20:04:01 to 11-30-2015-21:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-30-2015-20:04:01 to 11-30-2015-21:04:01

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	3340
192.115.67.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	648
79.178.108.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
146.185.57.7	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
93.174.93.151	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
38.229.1.13	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
114.80.122.91	China	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

11-30-2015-20:04:01 to 11-30-2015-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.245.88.217	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.245.88.135	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

11-30-2015-20:04:01 to 11-30-2015-21:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.245.88.217	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
192.114.105.254	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
109.64.213.176	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
2.52.6.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.150.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
159.122.238.133	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -f -sS	1
79.183.25.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.12.127.94	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.119.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.12.127.94	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.219.114.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.12.127.94	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.116.140.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.155	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.147.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.40.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
2.52.132.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.238.133	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
84.108.65.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.139.55.122	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.181.142.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.12.127.94	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.176.213.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.12.127.94	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.120.114.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.12.127.94	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
110.77.239.94	147.237.0.16	Thailand	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
31.6.71.154	147.237.77.121	Poland	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
95.144.187.141	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
2.54.40.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.245.88.135	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	1

11-30-2015-20:04:01 to 11-30-2015-21:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.115.67.2	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	70
62.219.124.98	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
5.102.234.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
95.35.67.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.57.143.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
213.57.143.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
213.57.136.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
213.57.136.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
212.76.105.35	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.30.59		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
95.35.67.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
2.54.46.4	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	18
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
79.178.108.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.106.226.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
176.106.226.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
212.34.11.110	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.93.234	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.219.233.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
72.37.140.47	Italy	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
79.182.227.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.182.227.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.85.123	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
100.100.34.212		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
79.176.58.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.169.157	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.46.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.54.46.4	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.102.254.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.46.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.46.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.120.125.48		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.228	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.23.158		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
100.100.100.31		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
192.117.182.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.58.75.46	Netherlands	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
46.19.85.179	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.2.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.236.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.30.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.184.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
157.55.39.174	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
93.173.168.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.151.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

11-30-2015-20:04:01 to 11-30-2015-21:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.76.105.35	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
207.241.226.41	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	65
94.230.86.222	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 94.230.86.222	Block	30
79.182.227.56	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
212.34.11.110	Jordan	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	6
212.34.11.110	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.11.110	Block	5
37.142.171.134	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	4
78.46.7.81	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
200.98.246.226	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
54.66.144.179	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
109.169.50.31	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.54.134.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
162.247.78.230	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
84.110.80.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
41.78.6.166	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.54.17.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.11.187.2	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
80.246.137.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.78.43.160	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	3
83.170.118.9	United Kingdom	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
209.175.158.221	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
50.87.45.170	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
83.170.118.9	United Kingdom	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 83.170.118.9	Block	3
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.13.23.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/pays	Block	2
162.247.78.230	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
85.250.73.5	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	2
41.78.6.166	South Africa	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
212.34.11.110	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.11.110	Block	2
209.175.158.221	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
79.182.227.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
50.87.45.170	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
78.46.7.81	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.46.7.81	Block	2
79.183.219.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.4.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
212.11.187.2	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
46.120.227.134	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
84.108.191.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.10.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.111.28.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
83.170.118.9	United Kingdom	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	2
209.175.158.221	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
200.98.246.226	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
54.66.144.179	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
85.65.161.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.169.50.31	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2

11-30-2015-20:04:01 to 11-30-2015-21:04:01