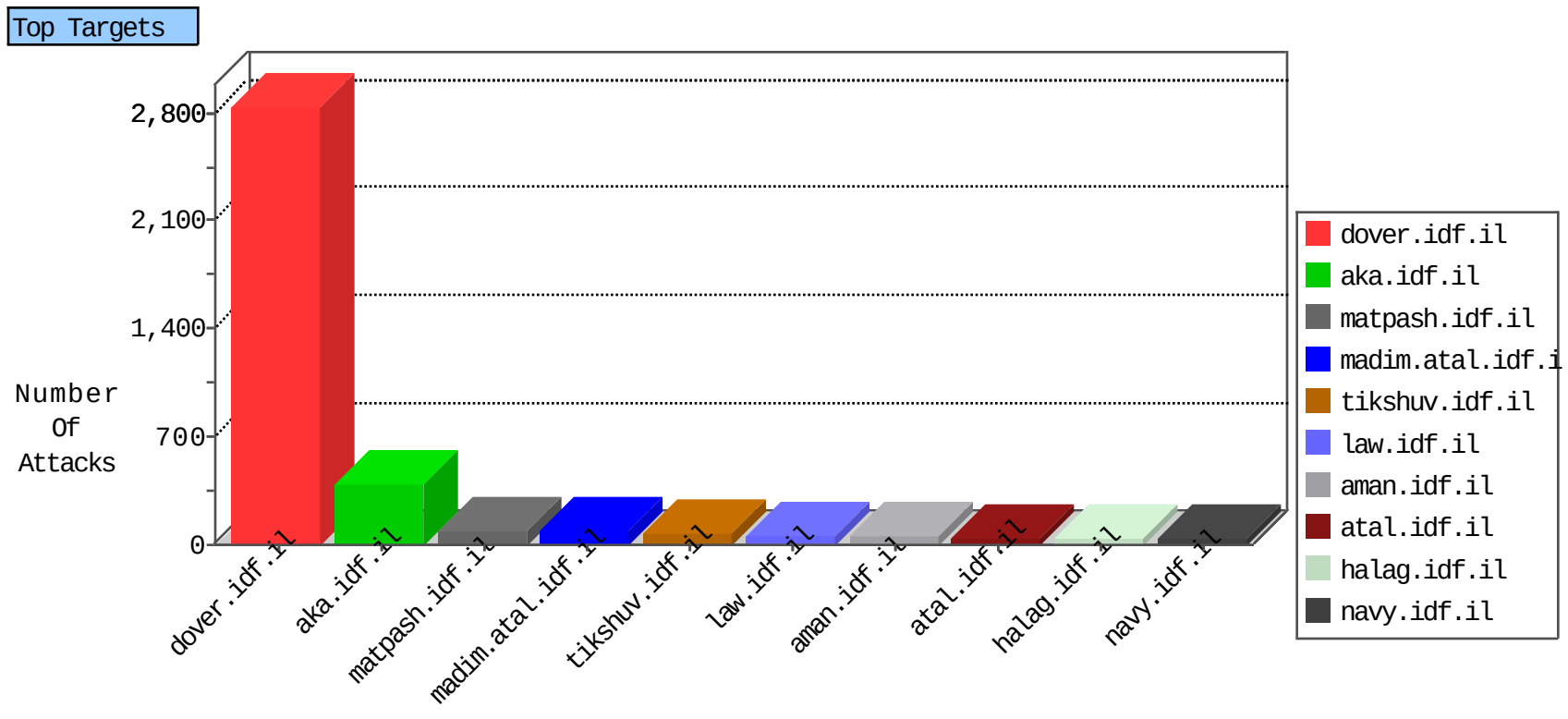
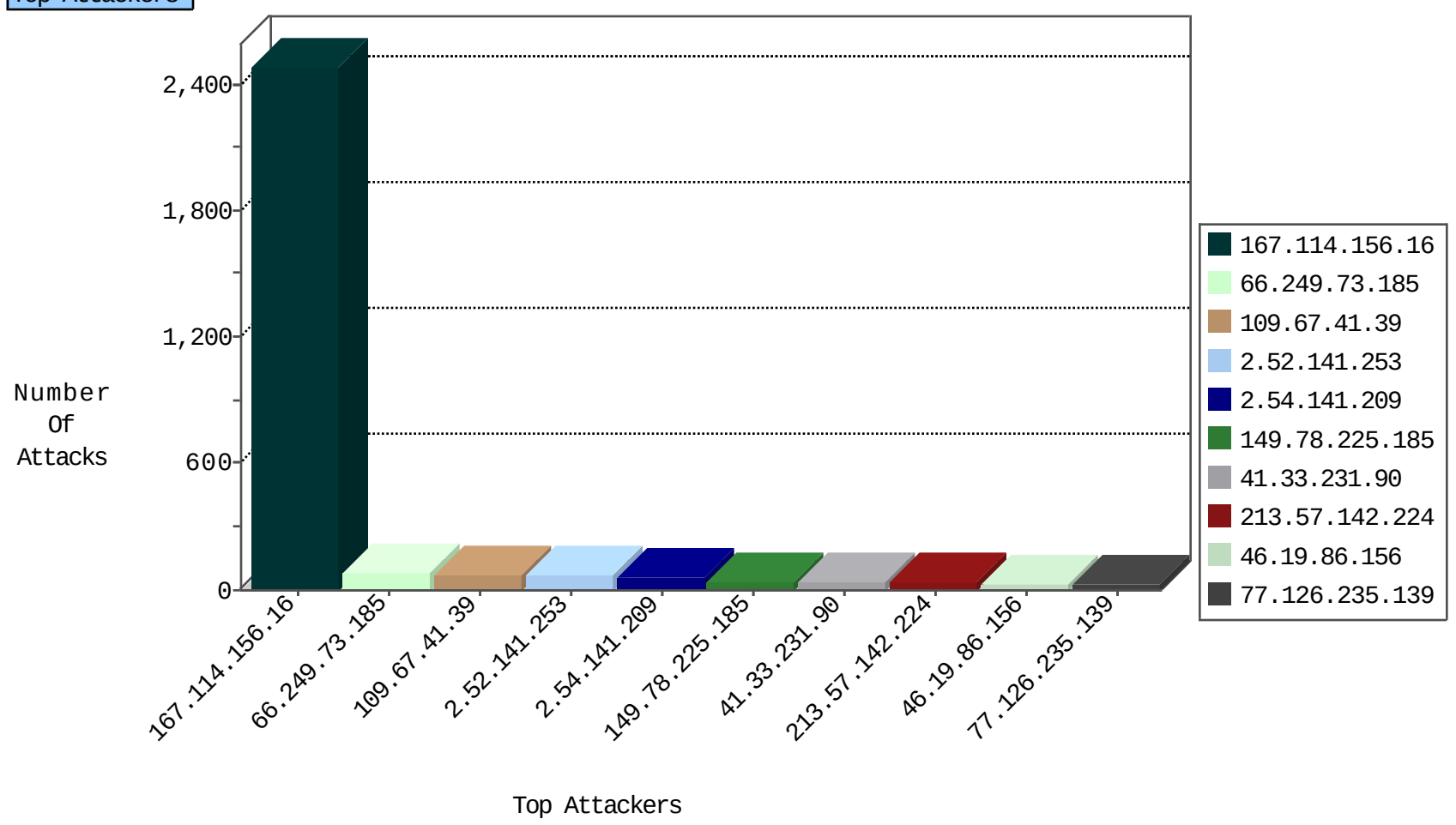
11-27-2015-23:04:02 to 11-28-2015-00:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-27-2015-23:04:02 to 11-28-2015-00:04:02

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	3735
66.249.66.125	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	993
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
200.29.186.163	Chile	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
37.61.151.183	Spain	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

11-27-2015-23:04:02 to 11-28-2015-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.63.88.184	Italy	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.245.62.10	Canada	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

11-27-2015-23:04:02 to 11-28-2015-00:04:02

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
66.249.75.44	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
75.179.3.87	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.76.198	Poland	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.3.66	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
185.106.94.91	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.76.177	Italy	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.93.153	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
83.110.227.35	147.237.76.30	United Arab Emirates	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.172.71.252	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.6.71.154	147.237.0.16	Poland	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.76.177	Italy	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
112.72.248.4	147.237.72.14	Korea, Republic of	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.153	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1

11-27-2015-23:04:02 to 11-28-2015-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
109.67.41.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
2.54.141.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
149.78.225.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
100.127.46.188		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.54.20.195	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.66.25		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
37.142.64.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
77.126.235.139	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	22
100.100.19.209		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
100.100.33.240		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
185.120.126.48		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	18
100.100.113.134		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
172.56.30.110	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
100.200.200.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
185.120.126.48		147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
100.100.16.142		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
213.57.142.224	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
100.100.90.33		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
213.57.142.224	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
100.100.90.33		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
199.30.24.183	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
100.100.33.240		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
109.64.197.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.126.235.139	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
213.57.128.210	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.65.215.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.142.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.142.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
65.49.14.154	Anonymous Proxy	147.237.77.216	dover.idf.il	drop		drop	6
87.69.56.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
82.80.58.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.102.254.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
100.100.90.33		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
89.139.26.180	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
94.230.86.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.110.209.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.58.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.3.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.72.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.57.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.217.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.141.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
109.67.41.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
2.54.141.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
79.182.170.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
149.78.225.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
93.173.177.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
149.88.101.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
201.148.104.107	Chile	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	3
5.153.225.110	United Kingdom	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	3
149.210.132.21	Netherlands	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
185.56.146.30	Netherlands	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 185.56.146.30	Block	3
94.23.121.14	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
74.220.207.153	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
199.175.51.66	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
91.146.107.207	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
185.56.146.30	Netherlands	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
129.7.107.7	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
89.221.250.23	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
174.127.116.185	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
103.247.0.7	Australia	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	3
185.56.146.30	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
37.122.209.14	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
50.87.161.155	United States	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
5.61.251.87	Netherlands	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	3
89.221.250.12	Sweden	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	3
84.22.107.124	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
103.227.176.6	Singapore	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
185.56.146.30	Netherlands	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
50.87.11.34	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
95.138.183.172	United Kingdom	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	3
217.167.147.156	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
173.254.85.31	United States	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
216.224.183.129	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
5.61.251.87	Netherlands	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	3
193.180.217.93	United States	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
149.210.201.208	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
198.20.228.139	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
185.56.146.30	Netherlands	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	3
216.119.129.194	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
78.47.17.5	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
197.85.184.79	South Africa	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
41.76.213.10	South Africa	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
188.165.150.69	France	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	3
149.210.157.227	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
185.24.99.199	United Kingdom	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	3
197.242.74.146	South Africa	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
75.98.175.88	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
176.13.0.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.210.201.208	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 149.210.201.208	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2

11-27-2015-23:04:02 to 11-28-2015-00:04:02