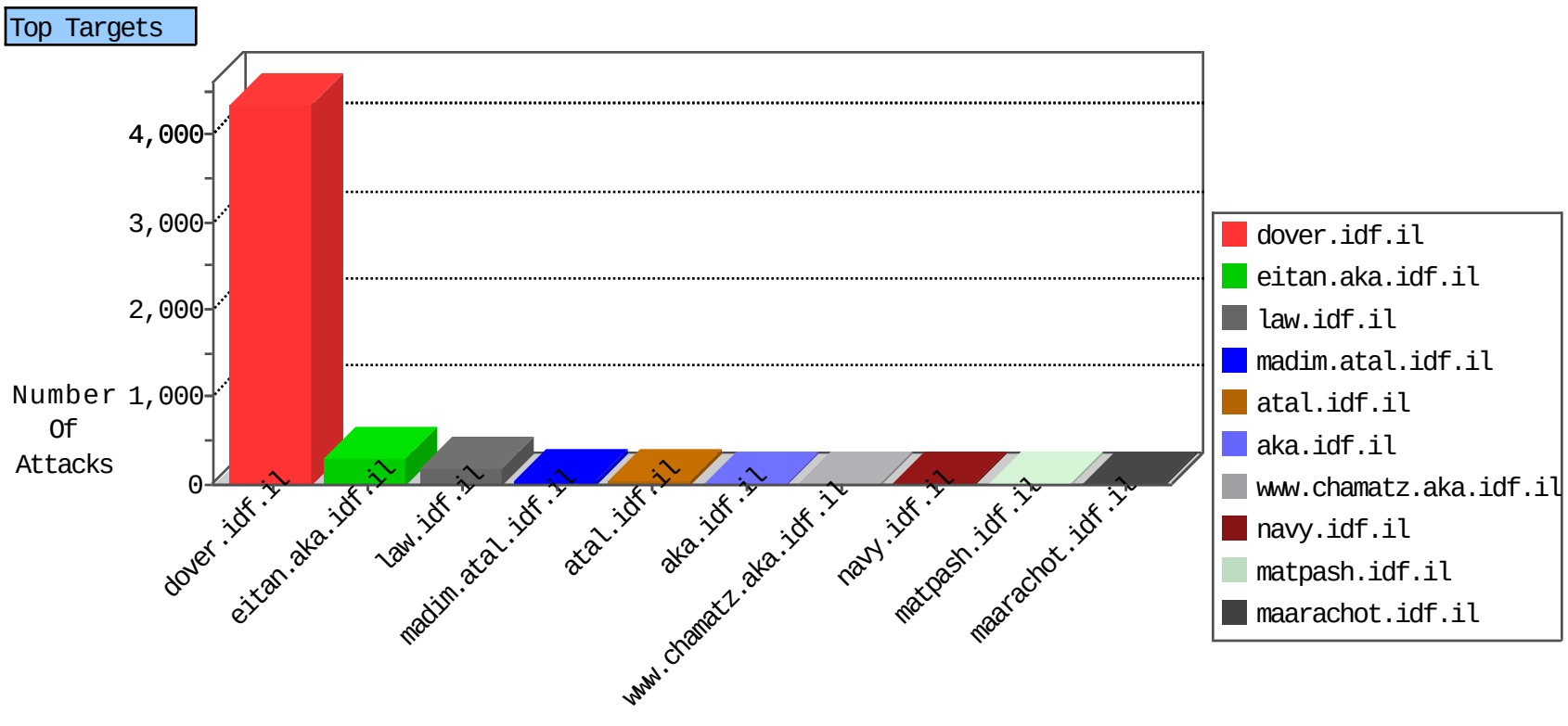
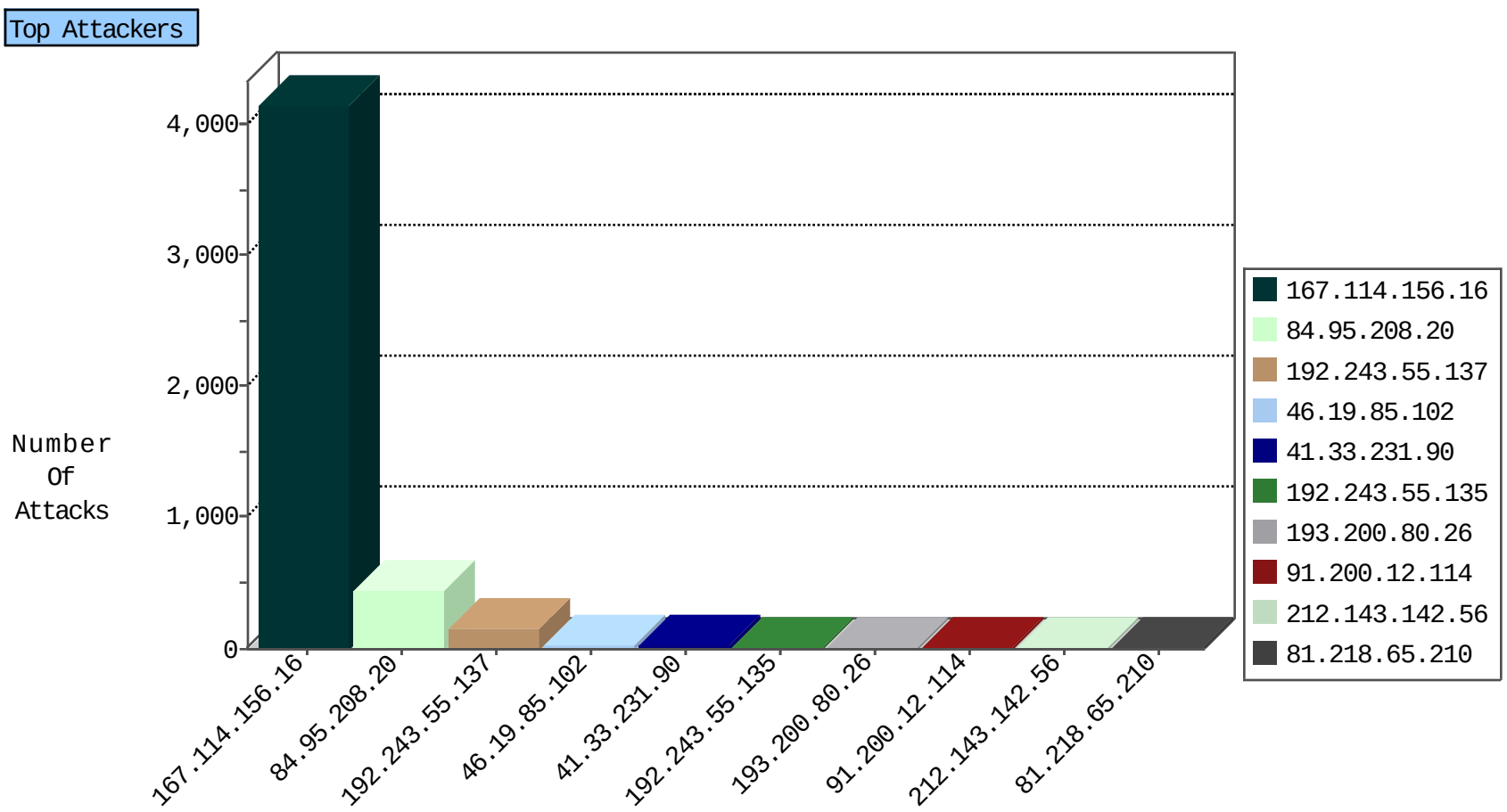
04-13-2016-03:04:03 to 04-13-2016-04:04:03

IDF Under Attack
Daily Report





04-13-2016-03:04:03 to 04-13-2016-04:04:03

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	Block_Ip_Web_In	drop	4129
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
184.105.247.254	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.31	Switzerland	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.99	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
38.229.33.47	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.90	United States	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.202	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
179.43.144.31	Switzerland	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.31	Switzerland	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
62.138.3.98	Germany	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1

04-13-2016-03:04:03 to 04-13-2016-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.200.80.26	United Kingdom	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
61.135.189.98	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-13-2016-03:04:03 to 04-13-2016-04:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.200.80.26	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
59.45.79.103	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
27.3.46.115	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.240.250.154	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
103.56.157.116	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -sS window 4096	1
103.56.157.116	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -f -sS	1
88.204.187.90	147.237.77.179	Kazakstan	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.103	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
162.39.113.86	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
113.240.250.154	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
103.56.157.116	147.237.76.86	Vietnam	navy.idf.il	ET SCAN NMAP -sS window 2048	1
88.204.187.90	147.237.77.179	Kazakstan	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.103	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1

04-13-2016-03:04:03 to 04-13-2016-04:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	43
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	26
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	10
37.46.41.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.64.198	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.29	United Kingdom	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
2.55.30.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.29	United Kingdom	147.237.0.33	idf.il	drop		drop	2
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
128.232.110.29	United Kingdom	147.237.76.34	yohalan.idf.il	drop		drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.39.222.159	Netherlands	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
171.64.222.195	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.202	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
211.36.143.26	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
90.158.39.41	Turkey	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.46.41.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.162.205.5	Germany	147.237.0.33	idf.il	drop		drop	1
137.116.71.170	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.150	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
61.135.189.98	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.55.30.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
159.226.95.66	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.126.113.80	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
90.158.39.41	Turkey	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.192	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
90.158.39.41	Turkey	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.193	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-13-2016-03:04:03 to 04-13-2016-04:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	100
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	32
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	15
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	5
91.200.12.114	Ukraine	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	4
91.200.12.114	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	3
101.167.226.87	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
91.200.12.114	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.114	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
101.167.226.88	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
91.200.12.114	Ukraine	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/wp-login.php	Block	2
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.25.134	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.25.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
208.109.252.167	United States	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
101.167.226.85	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
219.74.166.247	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
150.70.173.8	Japan	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
91.200.12.114	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
5.39.222.159	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
208.109.252.167	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/phpcms/languages/en/admin.lang.php	Block	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot	Block	1
203.127.58.231	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.47.233.68	France	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.15/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	Block	1
208.109.252.167	United States	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
91.200.12.114	Ukraine	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/wp-login.php	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
219.74.148.111	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-13-2016-03:04:03 to 04-13-2016-04:04:03