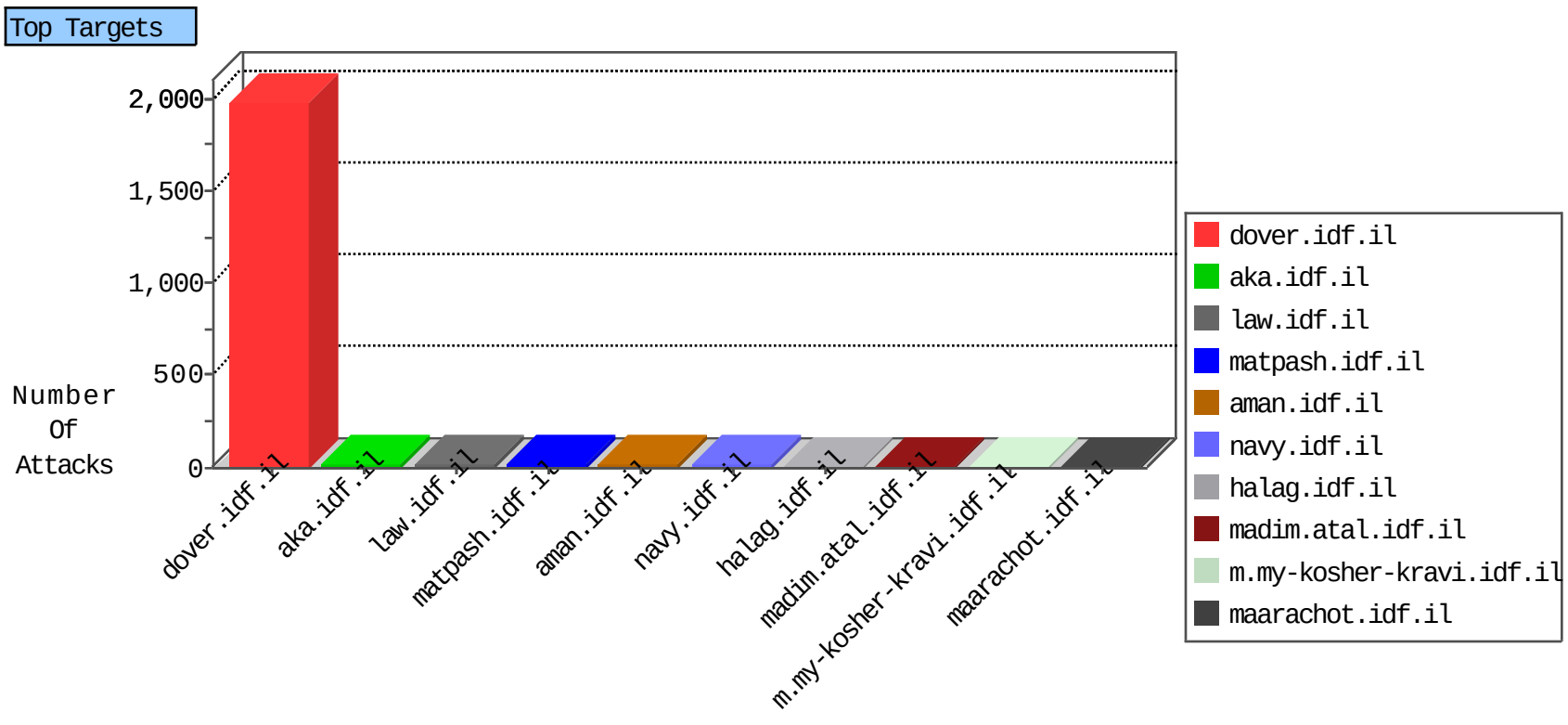
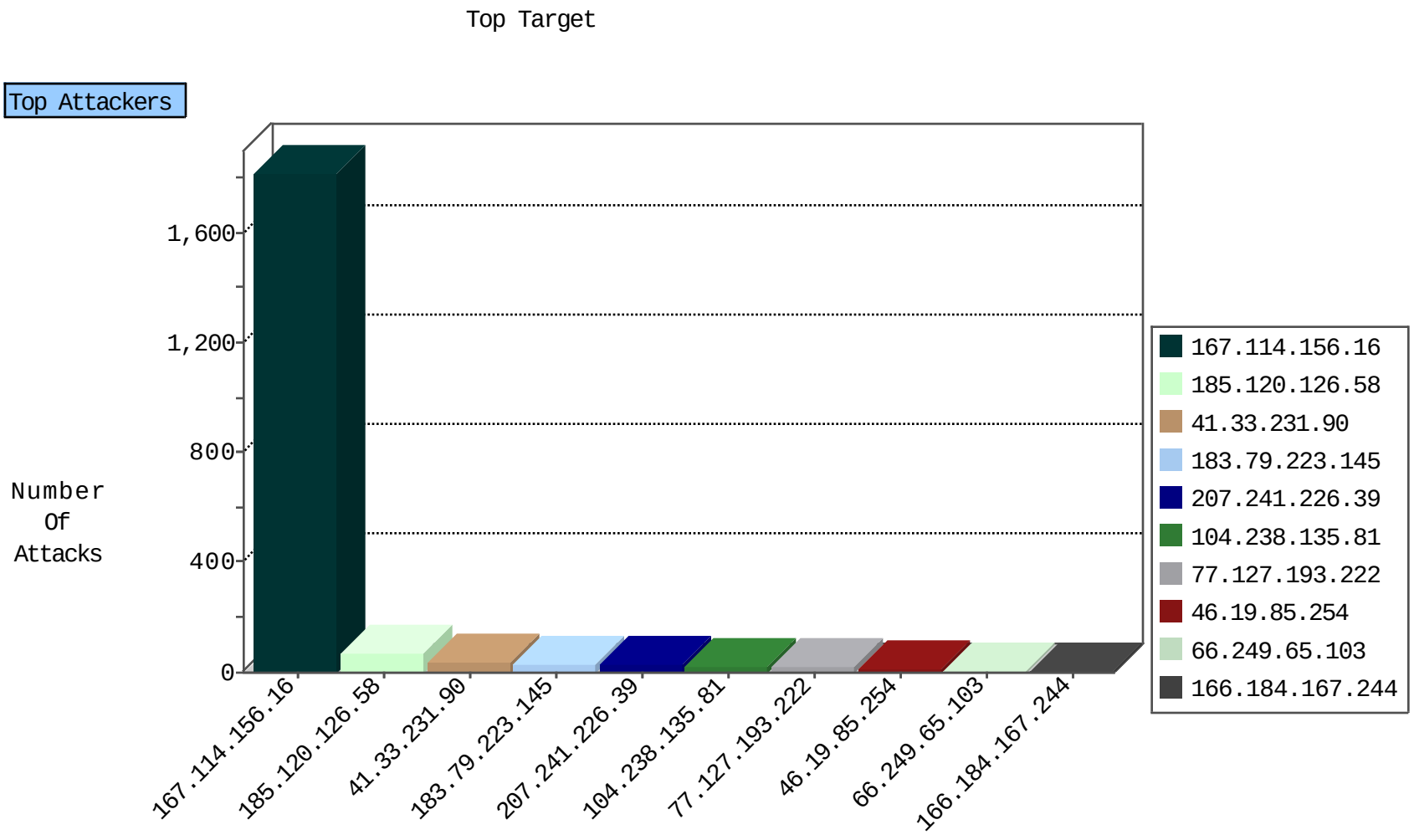
12-14-2015-03:04:04 to 12-14-2015-04:04:04

IDF Under Attack Daily Report





12-14-2015-03:04:04 to 12-14-2015-04:04:04

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	3685
58.229.254.149	Korea, Republic of	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.231.222.40	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2

12-14-2015-03:04:04 to 12-14-2015-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-14-2015-03:04:04 to 12-14-2015-04:04:04

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
104.238.135.81	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	2
46.200.212.254	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1
46.200.212.254	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
23.249.175.114	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
104.238.135.81	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
23.249.175.114	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
104.238.135.81	147.237.72.14		dover.idf.il(old)	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
104.238.135.81	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -f -sS	1
104.238.135.81	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.77.243		mobile.idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	1
82.211.60.82	147.237.77.121	Germany	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.135.81	147.237.77.178		e.matpash.idf.il	ET SCAN Potential SSH Scan	1
46.200.212.254	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.200.212.254	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.189	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
23.249.175.114	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
185.106.94.46	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.135.81	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
104.238.135.81	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
172.91.90.247	147.237.76.31		nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.238.135.81	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.77.234		halag.idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.238.135.81	147.237.77.212		e.dover.idf.il	ET SCAN Potential SSH Scan	1

12-14-2015-03:04:04 to 12-14-2015-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
77.127.193.222	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
66.249.65.103	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
77.127.193.222	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
213.57.129.15	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.254	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
166.184.167.244	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
70.208.64.51	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.47.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
166.184.167.244	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
213.57.212.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.163.234.8	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
213.57.212.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
128.199.87.148	Singapore	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.70	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.136.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.47.234.59	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
167.88.10.198	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.166.170.3	Lithuania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.96	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.201.154.140	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
213.57.212.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.199.87.148	Singapore	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.234.157.254	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
52.53.253.135	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.97	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.199.87.148	Singapore	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.212.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.127.193.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	alert	1
166.184.167.244	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
130.207.203.56	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
93.110.35.189	Iran, Islamic Republic of	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
71.88.0.118	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
54.183.240.200	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.97	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.199.87.148	Singapore	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.212.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

12-14-2015-03:04:04 to 12-14-2015-04:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.79.223.145	Japan	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.79.223.145	Block	26
207.241.226.39	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	23
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
141.8.142.29	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.228.37.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
199.115.117.117	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/_asterisk	Block	1
141.212.122.97	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /x	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
207.241.226.39	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/templates/news/piwik.php	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.125	Block	1
109.64.194.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71864-he/maarachot.aspx	Block	1
176.12.137.65	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding 9VhKxIfvybw$l@T:wUS%tOfJ72X(5I.:{^X4h]V)N0?*-eV8 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/6255.jpg	Block	1
109.163.234.2	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15490-he/dover.aspx	Block	1
176.12.137.65	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.137.65	None	1
107.178.195.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
213.57.145.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.1.214.180	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/5/3895.pdf/	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/11591.jpg	Block	1
207.46.13.187	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19036-en/dover.aspx <a href=	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
199.115.117.117	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/_asterisk	Block	1
141.212.122.97	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /x	Block	1
85.64.244.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.241.226.39	United States	147.237.76.30	himush.idf.il	PHP Attempt	Block	1
198.90.112.27	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1

12-14-2015-03:04:04 to 12-14-2015-04:04:04