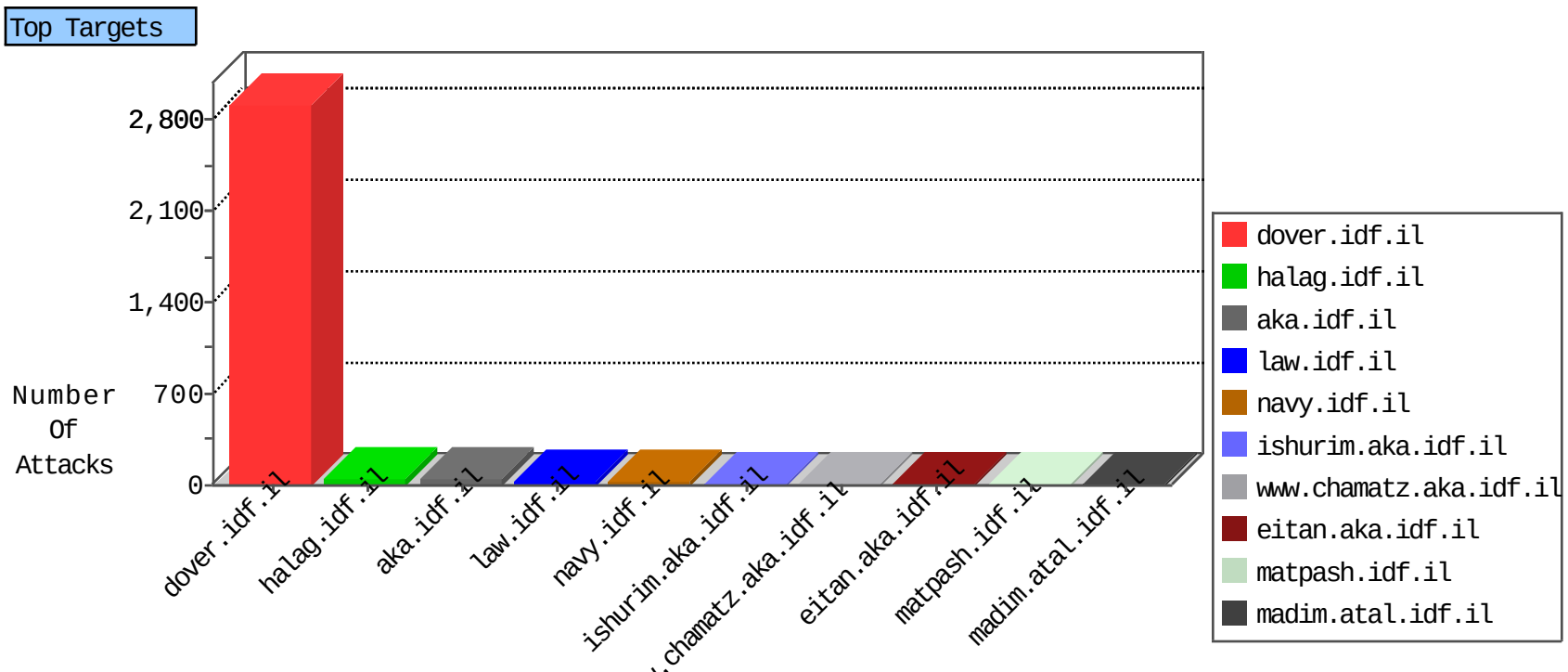
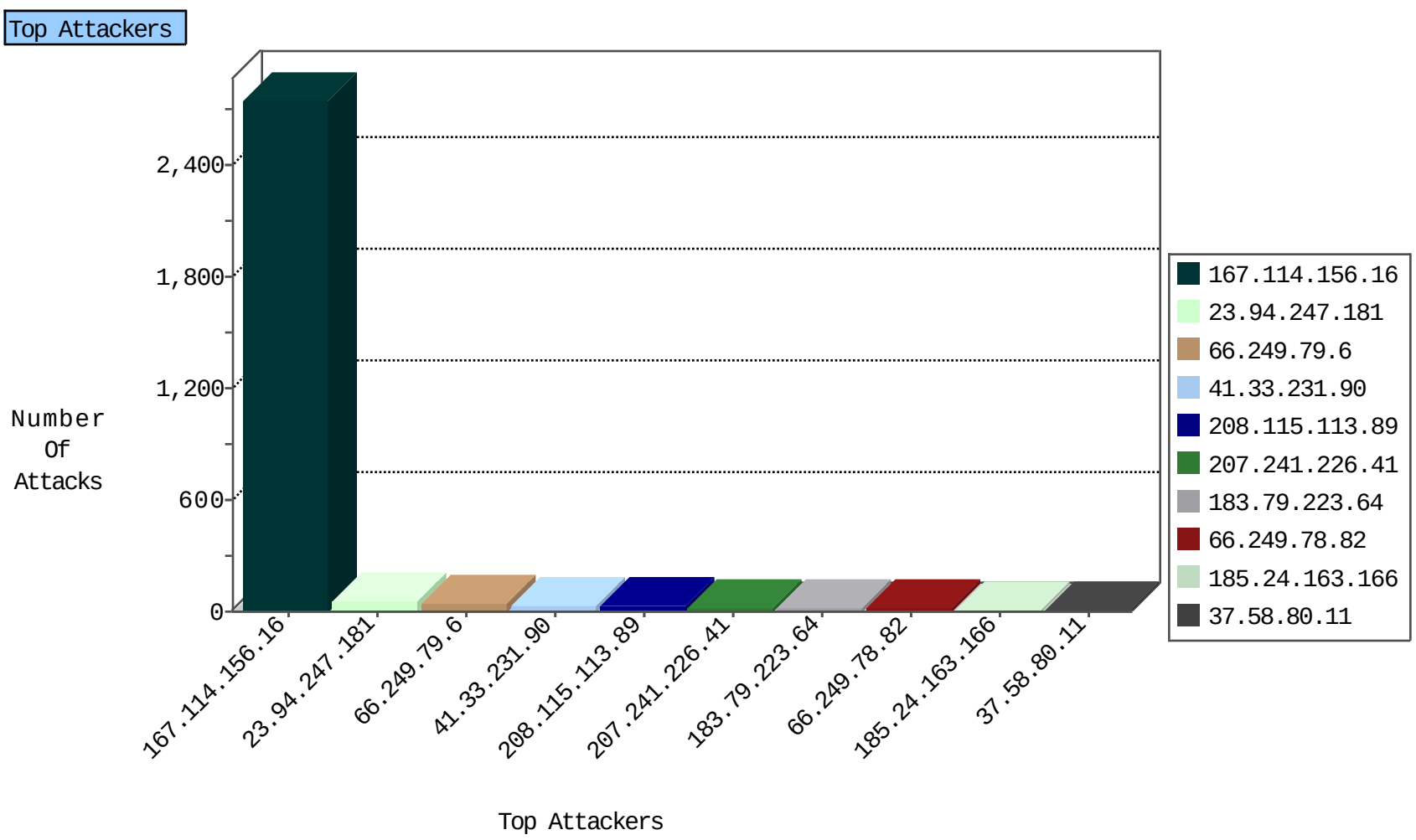
12-09-2015-02:04:05 to 12-09-2015-03:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-09-2015-02:04:05 to 12-09-2015-03:04:05

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	3491
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1516
66.249.64.195	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	228

12-09-2015-02:04:05 to 12-09-2015-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.106.94.2		147.237.77.226	www.chamatz.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
167.114.229.247	Canada	147.237.77.179	e.mazi.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
185.106.94.2		147.237.77.226	www.chamatz.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

12-09-2015-02:04:05 to 12-09-2015-03:04:05

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
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.9	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
185.24.163.166	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
153.201.174.35	147.237.0.16	Japan	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
185.24.163.166	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.24.163.166	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
185.24.163.166	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.24.163.166	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.24.163.166	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
153.201.174.35	147.237.8.24	Japan	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
153.201.174.35	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
153.201.174.35	147.237.0.15	Japan	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.106.94.2	147.237.77.226		www.chamatz.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
185.24.163.166	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
185.24.163.166	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential SSH Scan	1
185.24.163.166	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
153.201.174.35	147.237.77.216	Japan	dover.idf.il	ET SCAN Potential SSH Scan	1
153.201.174.35	147.237.0.35	Japan	akaws.idf.il	ET SCAN Potential SSH Scan	1

12-09-2015-02:04:05 to 12-09-2015-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
207.241.226.41	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	11
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
64.183.7.42	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.239.5.117	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.179.13.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.115.113.89	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	3
77.127.85.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
119.94.12.176	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.72.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.58.80.11	Netherlands	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.179	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
5.29.127.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
37.58.80.11	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.185	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.146.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.196.104.39	China	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
167.114.229.247	Canada	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.58.80.11	Netherlands	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.179	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.127.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.22.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
197.157.244.240	Somalia	147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	1
37.58.80.11	Netherlands	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.186	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.39.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.196.104.39	China	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.28.159.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.178	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.144.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.58.80.11	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.180	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.254.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.67.6.58	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.183.7.42	United States	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
197.157.244.240	Somalia	147.237.0.33	idf.il	drop	SAM rule	drop	1
141.212.121.186	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

12-09-2015-02:04:05 to 12-09-2015-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.94.247.181	United States	147.237.77.216	dover.idf.il	Too Many of the Same Response Code (404) in Session from 23.94.247.181	Block	48
183.79.223.64	Japan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.79.223.64	Block	17
107.167.112.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	7
207.241.226.41	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	6
207.241.226.41	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	5
141.0.8.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	4
157.55.2.170	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
79.176.179.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
46.19.86.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.28.187.118	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.28.187.118	Block	2
192.200.210.195	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
197.35.255.36	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
87.106.22.163	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/admin	Block	1
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/57978.pdf.2005	Block	1
150.70.173.50	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
45.55.197.238		147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
88.236.5.49	Turkey	147.237.77.170	maarachot.idf.il	Multiple Directory Traversal - 1(+) from 88.236.5.49	Block	1
207.241.226.41	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/piwik.php	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/112930.pdf	Block	1
129.114.58.106	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/piwik.php	Block	1
104.236.91.134		147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
197.35.255.36	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
87.106.22.163	Germany	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19369-he/idfgdover.aspx	Block	1
45.55.250.50		147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
88.236.5.49	Turkey	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-content/themes/mtheme-unus/css/css.php	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/default.asp	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	1
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
45.55.94.36		147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
104.236.113.144		147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
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	1
87.106.22.163	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/admin	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8656-he/dover.aspx	Block	1
159.203.133.140	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
45.55.254.68		147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
104.131.9.106	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
5.28.187.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/318812435/recoverpassword.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.200.210.195	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.200.210.195	Block	1
141.212.121.176	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
45.55.132.215		147.237.0.34	tikshuv.idf.il	Unauthorized Method HEAD for 147.237.0.34/	Block	1
104.236.251.80		147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
88.236.5.49	Turkey	147.237.77.170	maarachot.idf.il	Directory Traversal (In Cookies/Parameters Value)	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8833-he/refuah.aspx	Block	1
183.79.221.60	Japan	147.237.76.200	eitan.aka.idf.il	Abnormally Long Request request version	Block	1

12-09-2015-02:04:05 to 12-09-2015-03:04:05