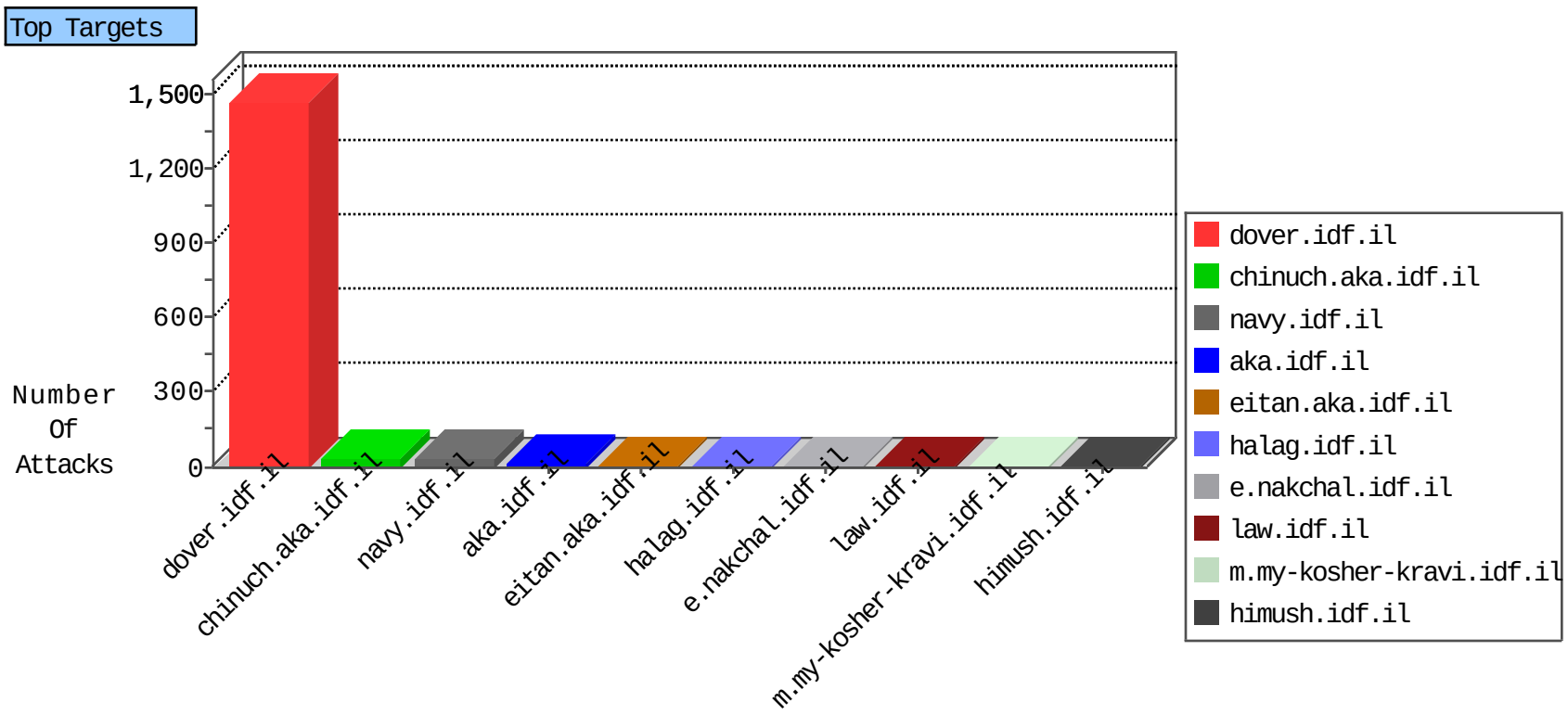
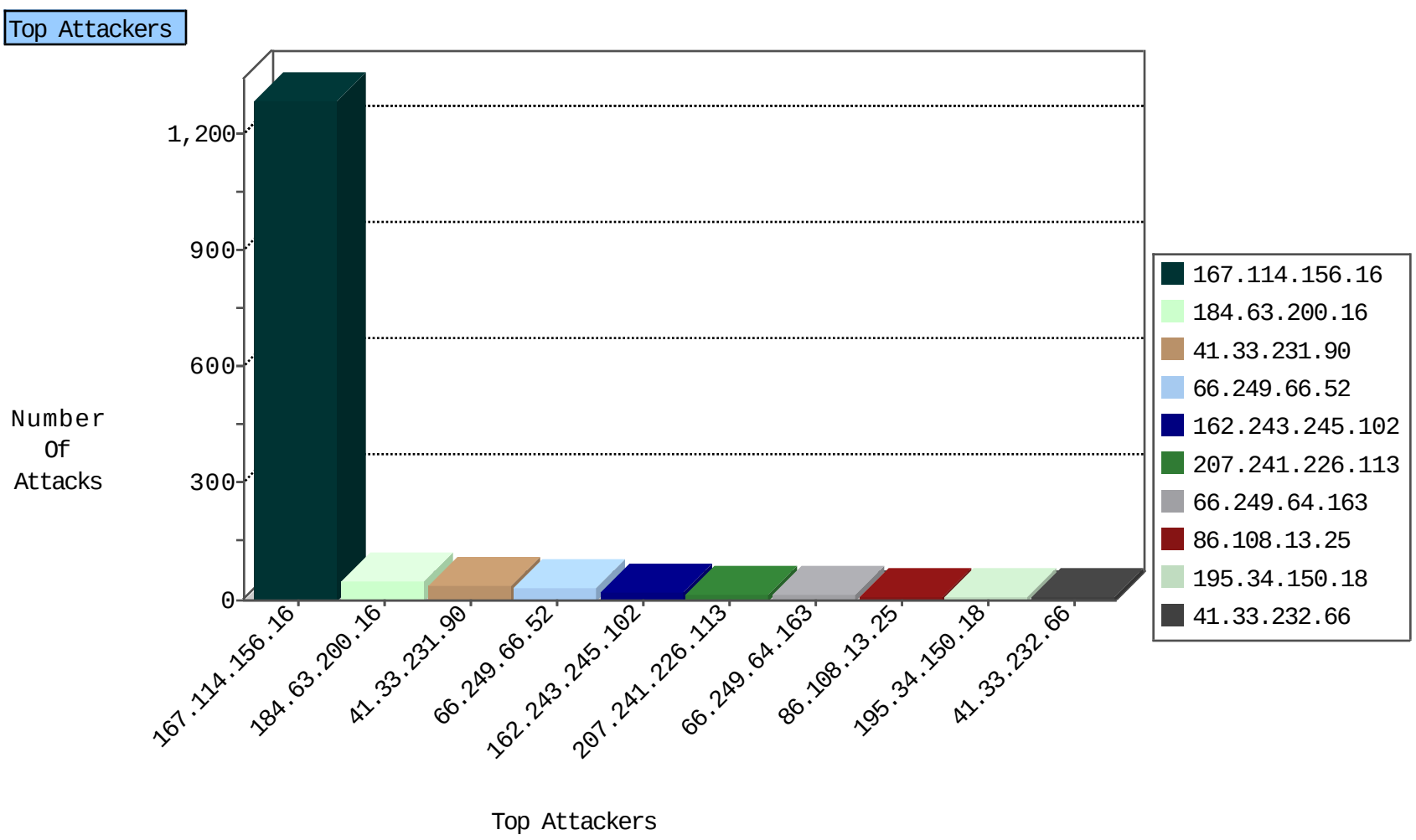
12-31-2015-04:04:07 to 12-31-2015-05:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-31-2015-04:04:07 to 12-31-2015-05:04:07

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	3803
180.97.106.161	China	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
213.177.27.210	Romania	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.36	China	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
180.97.106.162	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
180.97.106.162	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
180.97.106.161	China	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
184.63.200.16	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
180.97.106.36	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1

12-31-2015-04:04:07 to 12-31-2015-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-31-2015-04:04:07 to 12-31-2015-05:04:07

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
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.15	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 3072	1
118.68.29.67	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.114	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
82.211.60.107	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
45.34.163.42	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.15	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
118.68.29.67	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 3072	1
118.68.29.67	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -f -sS	1
82.211.60.107	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
82.211.60.107	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
189.198.118.62	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.34.163.42	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
183.61.109.189	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

12-31-2015-04:04:07 to 12-31-2015-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
184.63.200.16	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	49
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
207.241.226.113	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
162.243.245.102	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
86.108.13.25	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
157.55.39.19	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
207.46.13.91	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.200	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.30.16.178	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
128.232.110.28	United Kingdom	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
67.82.229.201	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
128.232.110.28	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.66.148.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.66.148.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.16.178	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
213.57.132.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
67.45.114.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.186.248.49	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.112	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.178.116.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.154.56.44	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.76	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.185.184.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.14	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.243	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
62.210.37.82	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
180.97.106.36	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.111.52.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.227.118	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
67.227.163.231	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.86	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.166.170.3	Lithuania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
74.82.47.16	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
194.150.168.79	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
71.233.128.220	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.112	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
195.28.180.101	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
180.97.106.162	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1

12-31-2015-04:04:07 to 12-31-2015-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.52	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	31
162.243.245.102	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.245.102	Block	4
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/4636.jpg	Block	2
37.142.242.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	2
66.249.66.55	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.149.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.178	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.116.25.197	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.116.25.197	Block	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.116.25.197	Romania	147.237.77.216	dover.idf.il	PHP Attempt	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
109.66.144.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.123.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
162.243.245.102	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
79.116.25.197	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
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	1
2.54.147.65	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
109.66.148.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	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
180.76.15.25	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
98.193.54.186	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
5.29.103.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
128.232.110.29	United Kingdom	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
74.82.47.2	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
64.113.32.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
180.76.15.153	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.170.1.51	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1

12-31-2015-04:04:07 to 12-31-2015-05:04:07