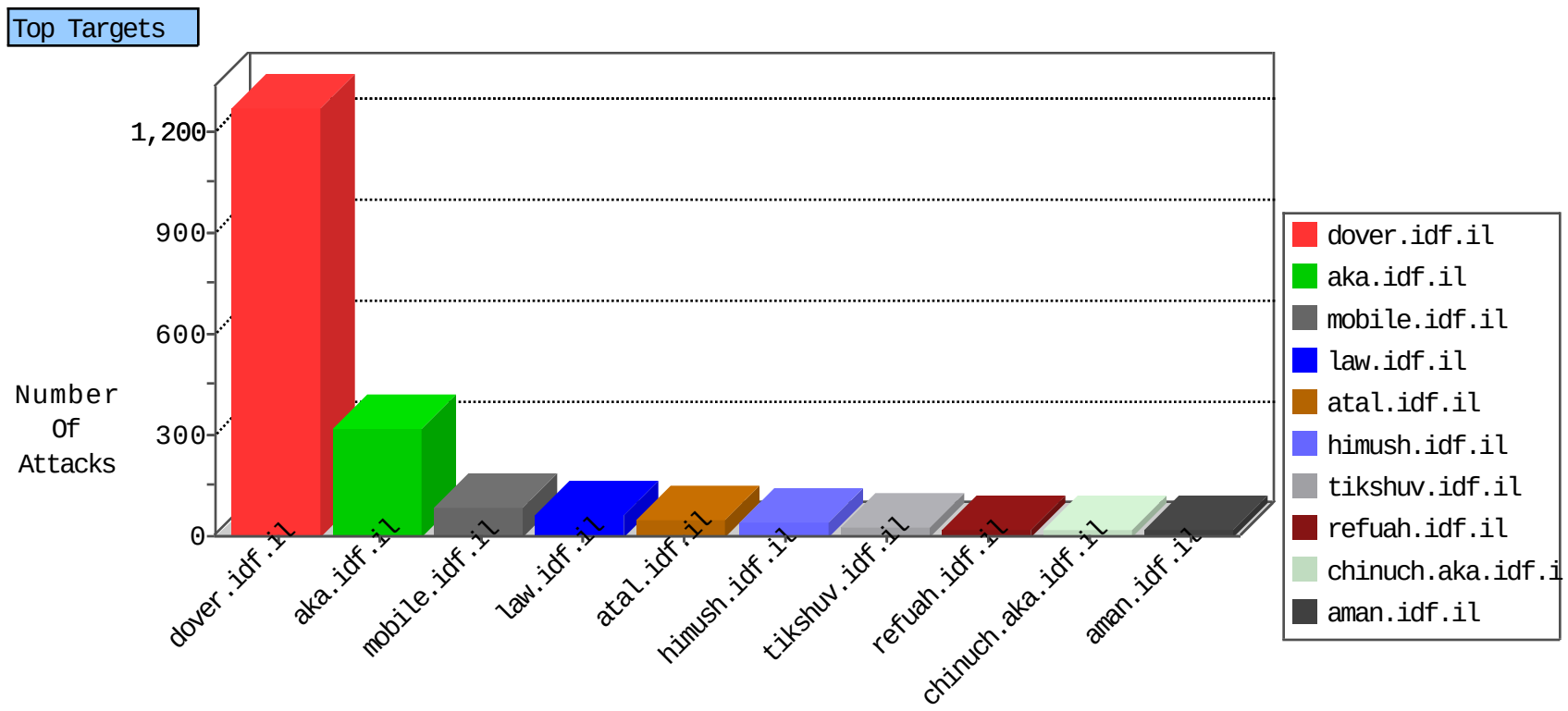
12-30-2015-23:04:02 to 12-31-2015-00:04:02

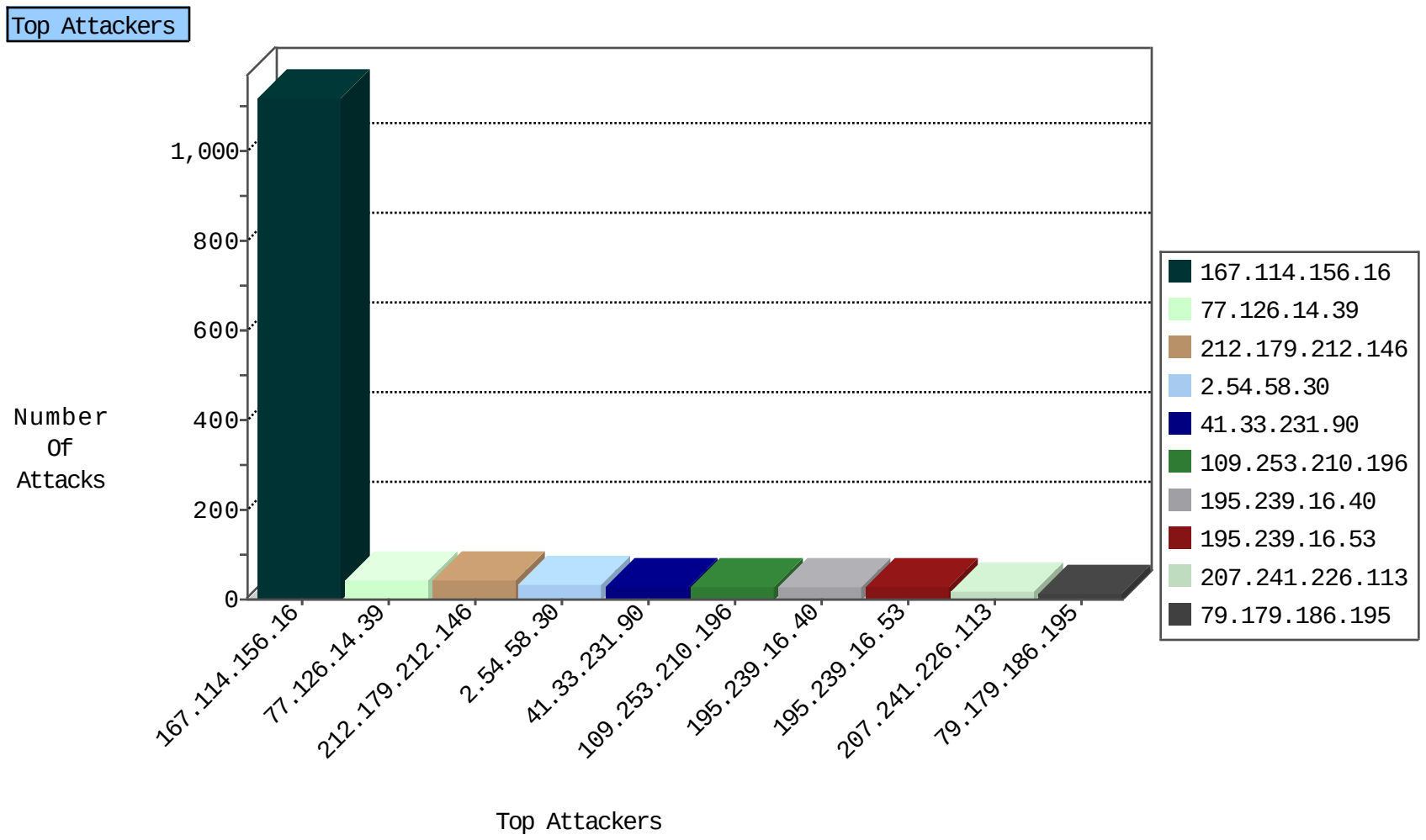
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-30-2015-23:04:02 to 12-31-2015-00:04:02

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	3038
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1910

12-30-2015-23:04:02 to 12-31-2015-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

12-30-2015-23:04:02 to 12-31-2015-00:04:02

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
119.184.254.215	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.165.173.83	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potenti Scan or Infection	1
82.117.208.243	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
2.61.157.29	147.237.8.27	Russian Federation	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.44.18	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
220.231.195.122	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN NMAP -sS window 4096	1
192.186.95.178	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -sS window 3072	1
95.165.173.83	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.198	Turkey	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.10.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.58.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 3072	1
220.231.195.122	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN NMAP -sS window 3072	1
192.186.95.178	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -sS window 4096	1

12-30-2015-23:04:02 to 12-31-2015-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
109.253.210.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
207.241.226.113	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
212.179.212.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.174.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.121.106.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
2.54.58.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.179.212.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
31.154.25.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.179.212.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.103	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.10.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.3.146.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.179.212.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.32.179.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.22.129.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.39.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.146.211	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.182.35.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.134.127	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.247.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.58.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.58.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.120.206.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.58.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.244	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.58.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.57.134.127	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.229	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.154.25.42	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	4
93.172.140.198	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.57.132.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.102.254.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.120.206.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.87.128.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.178.214.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.222.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-30-2015-23:04:02 to 12-31-2015-00:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.186.195	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.179.186.195	Block	14
109.253.210.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
79.181.134.32	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
66.249.66.61	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 77.126.14.39	Block	4
141.8.142.82	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 77.126.14.39	Block	4
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 77.126.14.39	Block	4
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 77.126.14.39	Block	4
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 77.126.14.39	Block	4
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 77.126.14.39	Block	3
2.54.174.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
5.29.17.20	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
114.97.48.57	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 114.97.48.57	Block	3
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.10.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
217.132.0.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.173.255.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.114.72	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.206.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 77.126.14.39	Block	2
46.19.86.194	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
217.132.15.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 77.126.14.39	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
217.132.57.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 77.126.14.39	Block	2
109.67.33.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 77.126.14.39	Block	2
46.120.206.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.108.64.218	Israel	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.251.182.114	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.251.182.114	Block	2
84.109.17.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.76.15.155	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin7.	Block	1
2.54.135.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.139.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.226.27.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.126.14.39	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 77.126.14.39	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
46.19.85.244	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
85.250.242.34	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.35.62.11	Switzerland	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
5.29.142.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.139.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
114.97.48.57	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1567-he/cogat.aspx/trackback/	Block	1

12-30-2015-23:04:02 to 12-31-2015-00:04:02