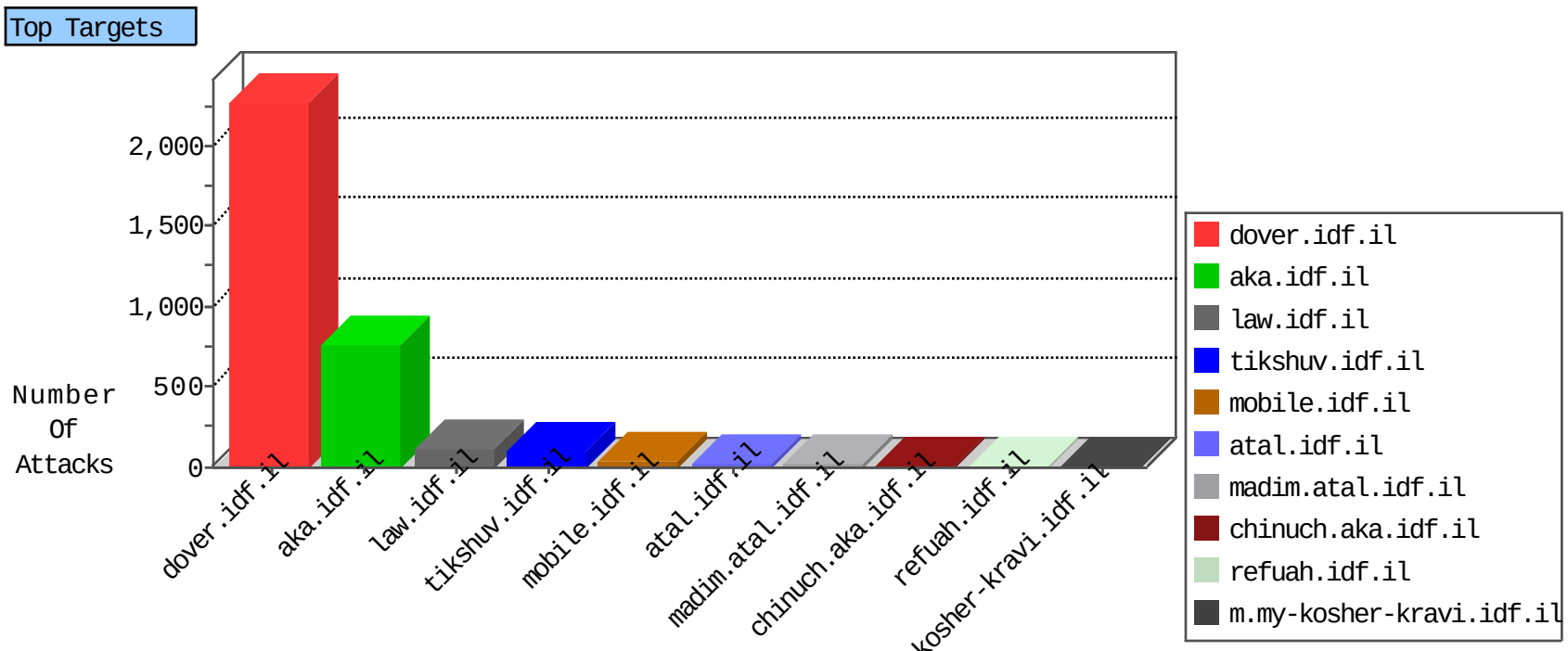
12-27-2015-23:04:03 to 12-28-2015-00:04:03

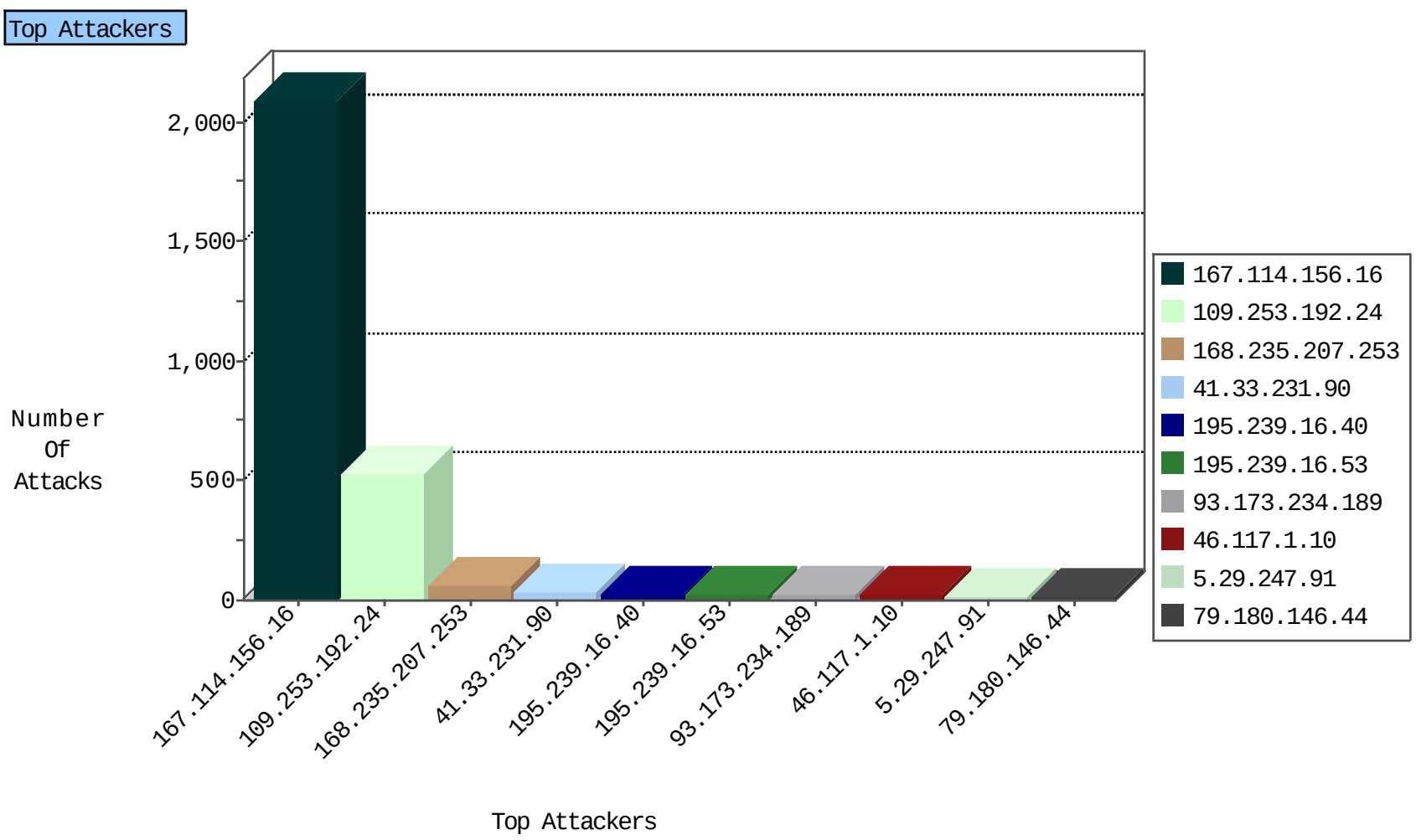
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-27-2015-23:04:03 to 12-28-2015-00:04:03

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	DOS-Tool-SwitchbladG	dest-reset	3319
79.178.151.17	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
168.235.207.253	United States	147.237.77.74	law.idf.il	Frk_Purple_Con_Limit_Http	drop	3
79.178.151.17	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
213.193.29.145	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
168.235.207.253	United States	147.237.77.74	law.idf.il	Frk_Under_Attack_Con_Http	drop	1
185.106.120.54		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-27-2015-23:04:03 to 12-28-2015-00:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.105.17.34	France	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
62.163.78.143	Netherlands	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1

12-27-2015-23:04:03 to 12-28-2015-00:04:03

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
151.217.178.88	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.219.238.10	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.76.201	France	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
68.168.137.2	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.161.237.210	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
151.217.178.88	147.237.77.179		e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
98.119.105.221	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1
79.114.23.96	147.237.72.14	Romania	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
68.168.137.2	147.237.72.166	Canada	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.77.235		sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-27-2015-23:04:03 to 12-28-2015-00:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.192.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	527
168.235.207.253	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
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
5.29.94.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
37.26.149.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.146.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.173.234.189	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
93.173.234.189	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	10
185.32.179.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
100.127.247.7		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
81.158.185.133	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.29.247.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
213.57.130.109	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
109.66.154.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.99.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.161.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.1.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
172.56.34.102	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.168.164.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.154.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.4.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.121.244.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.181.4.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.29.247.91	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	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
213.8.204.45	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.76.103.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
94.230.86.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.117.1.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
176.12.146.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
206.190.141.236	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
188.120.148.179	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.117.1.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.183.116.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.180.54.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.54.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.41.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.210.186.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.117.1.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.238	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	10
2.52.179.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
87.69.178.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.120	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	6
84.111.154.74	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	5
208.115.113.92	United States	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	5
84.111.168.157	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	5
84.94.41.85	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	5
84.108.234.183	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	4
79.179.131.45	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	4
40.77.167.50	United States	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	4
213.8.204.30	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	4
84.228.235.93	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	4
109.253.219.242	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.120.190.186	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	3
80.246.133.99	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.26.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.25.107	United States	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	3
23.254.243.147	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
79.181.130.30	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
79.180.146.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.57.90	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.170	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.28	United States	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
79.177.158.110	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
192.222.146.53	Canada	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
5.29.170.51	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.4	United States	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
79.181.61.59	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
79.182.133.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
41.203.18.61	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.64.81.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.103.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.160	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/servlet/satellite	Block	1
185.27.105.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.133.140.38	Hungary	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.185.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.85	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.51.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.151.60.230	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
109.253.145.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.52.96	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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

12-27-2015-23:04:03 to 12-28-2015-00:04:03