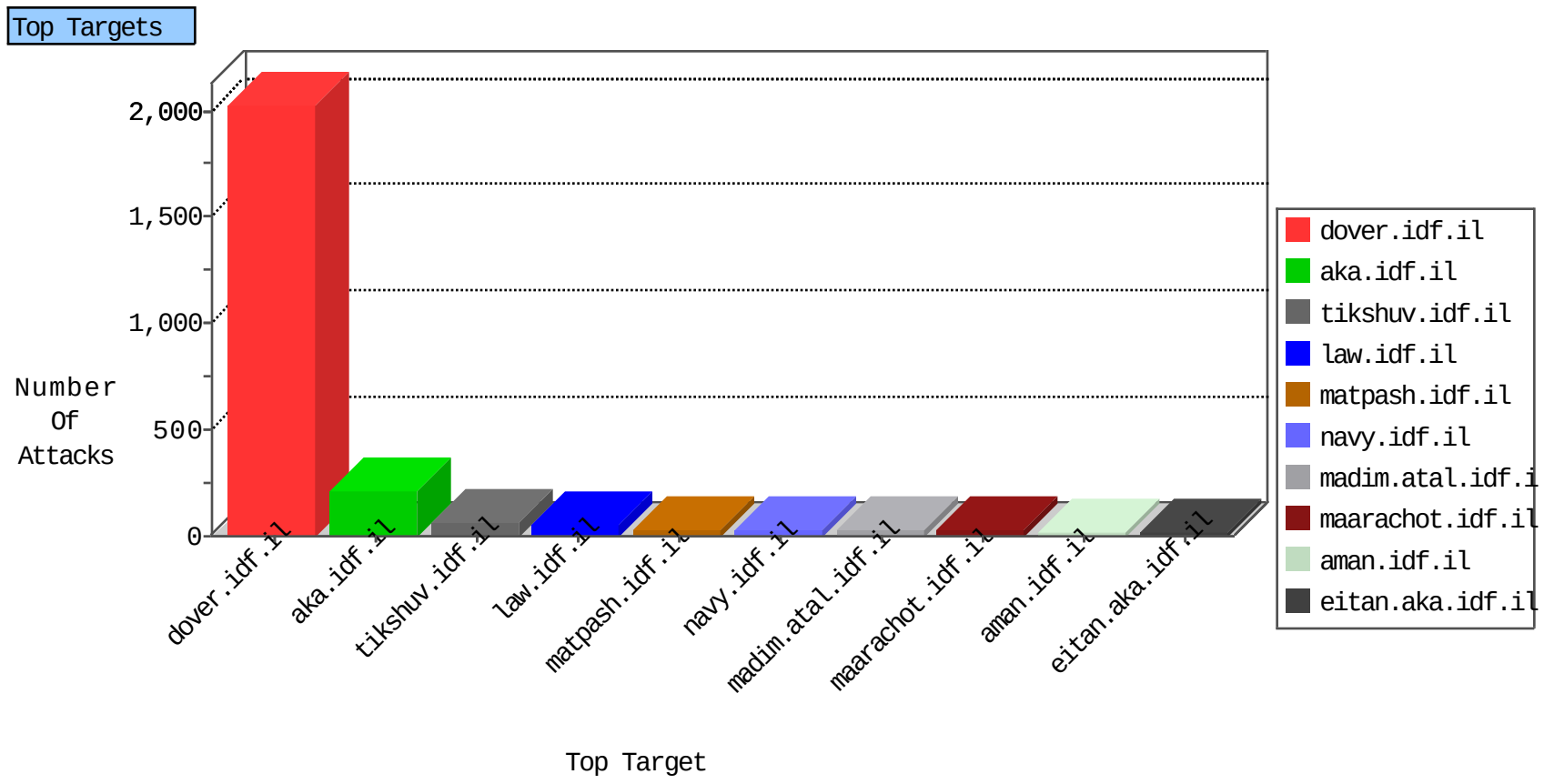
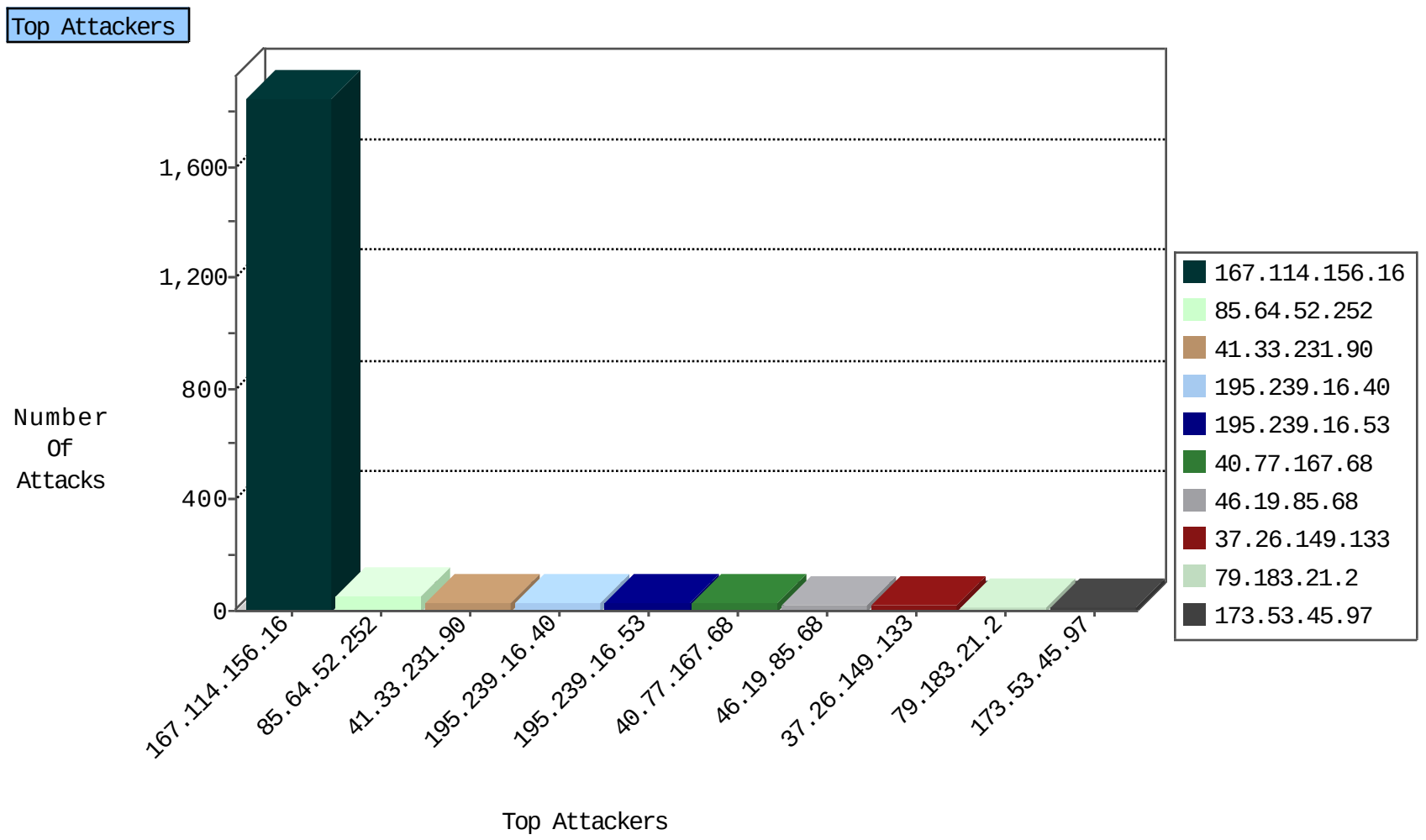
01-11-2016-23:04:09 to 01-12-2016-00:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-11-2016-23:04:09 to 01-12-2016-00:04:09

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	3135
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
185.40.4.205		147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	2
185.40.4.205		147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	2
115.239.228.10	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.40.4.205		147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
23.95.248.111	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
185.40.4.205		147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
89.248.168.218	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
23.95.248.111	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

01-11-2016-23:04:09 to 01-12-2016-00:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.214.46	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
177.47.187.20	Brazil	147.237.77.170	maarachot.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	1

01-11-2016-23:04:09 to 01-12-2016-00:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
177.47.187.20	147.237.77.170	Brazil	maarachot.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
173.53.45.97	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
173.53.45.97	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.94	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.53.45.97	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
173.53.45.97	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
193.169.86.5	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Potential SSH Scan	1
158.255.6.220	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
173.53.45.97	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
108.61.119.41	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
173.53.45.97	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
173.53.45.97	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
173.53.45.97	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
222.186.34.94	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.53.45.97	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.94	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.53.45.97	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
193.169.86.5	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
158.255.6.220	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
193.169.86.5	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
158.255.6.220	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
173.53.45.97	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
108.61.119.41	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
173.53.45.97	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
173.53.45.97	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 4096	1

01-11-2016-23:04:09 to 01-12-2016-00:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
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
40.77.167.68	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
79.176.16.14	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.68	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.21.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.68	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.90.210.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	6
217.194.199.151	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.209.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.153.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
128.0.201.60	Cyprus	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.149.234	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.129.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.21.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.121.63.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.11.130	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.65.3.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.253.146.153	Israel	147.237.77.170	maarachot.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
109.64.48.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.185.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.66.199.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.198.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.191.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.107.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.108.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.198.160	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
82.81.28.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.134.199	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.11.130	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

01-11-2016-23:04:09 to 01-12-2016-00:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.52.252	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.52.252	Block	54
2.54.132.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.199.57.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.154.227.118	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
37.26.149.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.7.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.183.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
40.77.167.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
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	2
77.126.255.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.165.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
177.47.187.20	Brazil	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.64.217.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
177.47.187.20	Brazil	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/index.php	Block	1
2.54.46.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/general.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/	Block	1
46.19.86.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.154.131	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
80.230.92.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
12.251.180.146	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
177.47.187.20	Brazil	147.237.77.170	maarachot.idf.il	Directory Traversal (In Cookies/Parameters Value)	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
223.240.127.54	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 223.240.127.54	Block	1
164.138.115.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.121.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
46.116.194.134	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	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
185.101.107.189		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.69.7.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
37.142.64.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.16.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.237.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
207.46.13.116	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/home/default.aspx	Block	1
149.78.198.160	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
195.154.194.111	France	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
27.25.7.81	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/3916.pdf/trackback/	Block	1
177.47.187.20	Brazil	147.237.77.170	maarachot.idf.il	Multiple Directory Traversal - 8(+) from 177.47.187.20	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
173.252.89.56	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.219.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-11-2016-23:04:09 to 01-12-2016-00:04:09